UNIVERSIDAD NACIONAL DEL SANTA

FACULTAD DE EDUCACIÓN Y HUMANIDADES

ESCUELA PROFESIONAL DE DERECHO Y CIENCIAS POLÍTICAS

"EL PHISHING COMO CONDUCTA DELICTIVA NO REGULADA EN EL ORDENAMIENTO JURIDICO PERUANO. PROPUESTA DE INCORPORACIÓN DEL ARTÍCULO 7-A EN LA LEY DE DELITOS INFORMÁTICOS 30096"

TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE ABOGADO

PRESENTADO POR:

- Bach.: CARITO NATIVIDAD HIDALGO CORONEL
- Bach.: GERSON STEVE SOLANO VIDAL

ASESOR:

- ABOG. MARIA CARMEN PEÑA RODRIGUEZ

CHIMBOTE – PERÚ

2021

HOJA DE AVAL DEL ASESOR

La presente tesis 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", ha sido elaborada según el Reglamento General de grados y Títulos, aprobado por Resolución N° 492-2017-R-UNS, del 03 de julio del 2017, para obtener el título profesional de Abogado, mediante la modalidad de tesis, por tal motivo firmo el presente trabajo en calidad de asesor, designado mediante Resolución Decanal N° 231-2019-UNS-DFEH, de fecha 30 de octubre del 2019.

.....

Abogada María Peña Rodríguez

Asesora de Tesis

HOJA DE CONFORMIDAD DEL JURADO EVALUADOR

Culminada la sustentación de tesis intitulada "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". Se considera aprobado al bachiller GERSON STEVE SOLANO VIDAL, con código 0201235037 y aprobada a la bachiller CARITO NATIVIDAD HIDALGO CORONEL con código 0201235028.

Revisado y aprobado por el jurado evaluador designado mediante resolución N° 229-2021-UNS-CFEH, de fecha 13 de agosto del 2021.

.....

MS. EDUARDO MONTENEGRO VIVAR

PRESIDENTE

.....

M. ROSA LUZ CASTRO CÁRDENAS

SECRETARIO

.....

ABG. MARÍA PEÑA RODRÍGUEZ

INTEGRANTE

UNIVERSIDAD NACIONAL DEL SANTA
FACULTAD DE EDUCACIÓN Y HUMANIDADES

ACTA DE CALIFICACIÓN DE LA SUSTENTACIÓN DE TESIS

En el distrito de Nuevo Chimbote, en el Aula Virtual mediante plataforma de Video conferencia Zoom, siendo las veintiún horas con quince minutos del día cuatro de diciembre del año dos mil veintiuno, se reunió el Jurado Evaluador presidido por: MS. EDUARDO MONTENEGRO VIVAR, teniendo como integrantes a: la Ms. ROSA LUZ CASTRO CÁRDENAS, y ABOGADA MARÍA PEÑA RODRÍGUEZ, para la sustentación de Tesis, a fin de optar el Título de ABOGADO, al Bachiller en Derecho y Ciencias Políticas: **GERSON STEVE SOLANO VIDAL,** quien expuso y sustentó el trabajo intitulado:

"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"

Terminada la sustentación, el graduado respondió las preguntas formuladas por los miembros del Jurado.

El Jurado después de deliberar sobre aspectos relacionados con el trabajo, contenido y sustentación del mismo y con las sugerencias pertinentes declara: .....APROBADO POR UNANIMIDAD.....; según el Art. 39° del Reglamento General para obtener de Grados y Títulos de la UNS (Resolución No. 492-2017-CU-R-UNS de 03.07.2017).

Siendo las once horas del mismo día se da por terminado el acto de sustentación.

Nuevo Chimbote, 04 de diciembre de 2021

.....
MS. EDUARDO MONTENEGRO VIVAR
PRESIDENTE

.....
M. ROSA LUZ CASTRO CÁRDENAS
SECRETARIO

.....
ABG. MARÍA PEÑA RODRÍGUEZ
INTEGRANTE

UNIVERSIDAD NACIONAL DEL SANTA
FACULTAD DE EDUCACIÓN Y HUMANIDADES

ACTA DE CALIFICACIÓN DE LA SUSTENTACIÓN DE TESIS

En el distrito de Nuevo Chimbote, en el Aula Virtual mediante plataforma de Video conferencia Zoom, siendo las veintiún horas con quince minutos del día cuatro de diciembre del año dos mil veintiuno, se reunió el Jurado Evaluador presidido por: MS. EDUARDO MONTENEGRO VIVAR, teniendo como integrantes a: la Ms. ROSA LUZ CASTRO CÁRDENAS, y ABOGADA MARÍA PEÑA RODRÍGUEZ, para la sustentación de Tesis, a fin de optar el Título de ABOGADA, a la Bachiller en Derecho y Ciencias Políticas: **CARITO NATIVIDAD HIDALGO CORONEL,** quien expuso y sustentó el trabajo intitulado:

"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"

Terminada la sustentación, la graduada respondió las preguntas formuladas por los miembros del Jurado.

El Jurado después de deliberar sobre aspectos relacionados con el trabajo, contenido y sustentación del mismo y con las sugerencias pertinentes declara: .....APROBADA POR UNANIMIDAD.....; según el Art. 39° del Reglamento General para obtener de Grados y Títulos de la UNS (Resolución No. 492-2017-CU-R-UNS de 03.07.2017).

Siendo las once horas del mismo día se da por terminado el acto de sustentación.

Nuevo Chimbote, 04 de diciembre de 2021

.....
MS. EDUARDO MONTENEGRO VIVAR
PRESIDENTE

.....
M. ROSA LUZ CASTRO CÁRDENAS
SECRETARIO

.....
ABG. MARÍA PEÑA RODRÍGUEZ
INTEGRANTE

DEDICATORIA

A DIOS, padre, por brindarnos salud, sabiduría y por permitirnos terminar nuestros estudios superiores de manera satisfactoria. Por iluminar nuestro camino y bendecirnos cada día de nuestra vida. Asimismo, por hacer realidad nuestros sueños.

A mis padres Pedro Hidalgo Castro y Maximina Coronel Valderrama les agradezco por su apoyo, protección y amor incondicional, que durante todo el transcurso de mi vida me han venido brindando.

Dedico esta tesis a mi madre Flor Aguirre Vidal, por su esfuerzo y apoyo incondicional en lo moral y económico, por enseñarme a ser perseverante, por confiar en mí y apoyarme a lo largo de todos estos años de formación universitaria.

Los autores.

AGRADECIMIENTO

A nuestros padres, por permitirnos e incentivarnos a estudiar una carrera profesional, por su amor, esfuerzo, comprensión e inculcarnos valores.

A nuestra asesora de tesis, Abog. María Carmen Peña Rodriguez, por su disposición y entusiasmo para poner en practica este trabajo, asi como compartir sus conocimientos, su tiempo y dedicación con nosotros, por apoyarnos en todo momento, y recordarnos que debemos esforzarnos cada vez más.

A nuestra casa de estudios Universidad Nacional del Santa, especialmente a la Escuela Académico de Derecho y Ciencias Políticas, pues nos formó durante seis años en conocimiento, experiencia y valores.

Los autores.

PRESENTACIÓN

Señores miembros del jurado:

En cumplimiento de las disposiciones legales vigentes en el Reglamento General de Grados y Títulos aprobado por Resolución N° 492-2017-CU-R-UNS del 03 de julio del 2017 de la Universidad Nacional del Santa y las disposiciones normativas contenidas en el Currículo de la Escuela Profesional de Derecho y Ciencias Políticas adscrita a la Facultad de Educación y Humanidades, presentamos a vuestra disposición la tesis titulada: «EL PHISHING COMO CONDUCTA DELICTIVA NO REGULADA EN EL ORDENAMIENTO JURIDICO PERUANO. PROPUESTA DE INCORPORACIÓN DEL ARTÍCULO 7-A EN LA LEY DE DELITOS INFORMÁTICOS 30096», con fin de optar el título profesional de Abogado.

La presente investigación atiende una demanda social de cada vez mayor relevancia en la realidad peruana, pues el avance de la tecnología permite que también las técnicas empleadas por sujetos inescrupulosos sean más sofisticadas, lo que pone en riesgo a una gran parte de la población, pues en la actualidad el uso de las tecnologías de información se ha vuelto indispensable, más si se tiene en cuenta el estado de emergencia a raíz de la pandemia por COVID-19, lo que ha generado que se multiplique la cantidad de tiempo que las personas pasan navegando por internet, quedando expuestos a la cibercriminalidad.

Es así que esta investigación es el resultado del análisis del ordenamiento jurídico nacional y comparado, principios y del respaldo de las legislaciones comparadas que han sabido incorporar tipos penales más precisos para la protección de la sociedad frente a la cibercriminalidad, de manera que las nuevas modalidades delictivas que aparecen con el tiempo no queden impunes.

ÍNDICE

RESUMEN

La presente investigación tiene por objetivo dar a conocer el problema existente en torno a la deficiente regulación jurídica que se ha hecho sobre los delitos informáticos en nuestro ordenamiento jurídico, específicamente en el caso del *phishing*, conducta que tiene algunas modalidades que no son posibles de ser tipificadas en ninguno de los tipos penales previstos en la Ley de Delitos Informáticos; ello genera que exista impunidad en estas conductas, pues se dificulta la acción del Ministerio Público como ente persecutor del delito; el tipo de investigación es descriptiva y aplicada. Asimismo se han empleado el método científico y método jurídico de tal manera que hemos elaborado una propuesta de Ley, a fin de regular de manera específica el *phishing* en un tipo penal que englobe todas las modalidades de ejecución de esta conducta ilícita.

Los autores

ABSTRACT

The objective of this research is to make known the existing problem around the deficient legal regulation that has been made on computer crimes in our legal system, specifically in the case of phishing, conduct that has some modalities that are not possible to be typified in none of the criminal types provided for in the Computer Crimes Law; this generates impunity in these conducts, since the action of the Public Ministry as a criminal prosecutor is difficult; the type of research is descriptive and applied. Likewise, the scientific method and legal method have been used in such a way that we have prepared a proposal for a Law, in order to specifically regulate phishing in a criminal type that encompasses all the modalities of execution of this illegal conduct.

The authors

I. INTRODUCCIÓN

1.1.PLANTEAMIENTO DEL PROBLEMA

1.1.1. DESCRIPCIÓN DE LA REALIDAD PROBLEMÁTICA

Con el avance de la tecnología y especialmente desde que surgió la pandemia por COVID-19, la presencia de los medios tecnológicos en la vida cotidiana ha visto un abrupto incremento, siendo indispensable actualmente para el desarrollo normal de ciertas actividades, como es en el caso del sector educación, el sector laboral y más evidente en el sector comercial. Según un reporte de la Cámara Peruana de Comercio Electrónico, en el año 2020 se ha visto un incremento del 50% del volumen total de *ecommerce* en el Perú, y se ha registrado un 400% de crecimiento en el número de empresas involucradas en el *ecommerce*. “Frente a un contexto, donde la mayoría de industrias han registrado contracciones, el *ecommerce* ha tenido un crecimiento del 50% en términos dolarizados, según consultas a diversos medios de pagos.” (CAPECE, 2021, p. 14)

Estos cambios en nuestros hábitos han traído como consecuencia también un incremento en el número de ataques y modalidades de ciberdelincuencia. Siendo el phishing una de las modalidades de ciberataque que más incidencia tiene en el mundo. Así lo ha reconocido la empresa MICROSOFT en su reporte de defensa digital del año 2020 donde se sostiene:

> El phishing por correo electrónico en el contexto empresarial sigue creciendo y se ha convertido en un vector dominante. Básicamente, el phishing ocurre cuando las personas u organizaciones reciben un correo electrónico

> fraudulento que los anima a hacer clic en un enlace, que le da al ciberdelincuente acceso a un dispositivo o información personal. (p. 14)

El Perú no es una excepción a los avances de la ciberdelincuencia, así tenemos que, a nivel de fiscalía, se ha registrado desde hace años un incremento sustancial en el número de denuncias registradas por delitos informáticos:

> Al mes de noviembre del año 2019, se registró un total de 6,906 delitos informáticos, cifra mayor en un 79.33% a los delitos registrados en el mismo período del año 2018 que fueron de 3,851 delitos; asimismo, al mes de noviembre del 2019 se puede observar que el tipo de delito con mayor incidencia se presenta en los delitos informáticos contra el patrimonio con un 38.24%. (MINISTERIO PÚBLICO, 2019, p. 59)

Asimismo, en el anuario estadístico del Ministerio Público para el año 2020 se ha registrado la incidencia de los delitos informáticos de la siguiente manera:

> Durante el año 2020, se registraron un total de 8,674 delitos informáticos – Ley N°30096, donde el mayor porcentaje se concentra en delitos informáticos contra el patrimonio con 54.65% (4,741 delitos). (MINISTERIO PÚBLICO, 2020, p. 50)

Pero, aunque los ciberataques van incrementando y surgen nuevas modalidades delictivas, nuestro ordenamiento jurídico se ha visto estancado pues, aunque existe una Ley de Delitos Informáticos (Ley 30096), ésta no se ha visto actualizada desde que en febrero del 2014 se promulgara la Ley 30171 que modificó

algunos artículos de la Ley 30096. Y esta pasividad en nuestros legisladores frente a la problemática de los delitos informáticos, genera que las nuevas conductas delictivas sean difíciles o imposibles de tipificar en los delitos existentes, máxime si se tiene en cuenta que de acuerdo al principio de legalidad, no se puede sancionar a nadie por un acto que no estaba tipificado como delito al momento de la comisión del hecho.

1.1.2. OBJETO DE LA INVESTIGACIÓN

El objeto de la presente investigación versa sobre la regulación del phishing como conducta penalmente relevante en el ordenamiento jurídico peruano.

1.1.3. ANTECEDENTES DEL PROBLEMA

El tema objeto de investigación aun cuando es novedoso ya se ha tratado en revistas jurídicas, tesis e investigaciones a nivel internacional, nacional y hasta local.

a) A nivel internacional.

En el ámbito internacional podemos encontrar la tesis de pregrado, en la Universidad Central de Ecuador, realizada por Herrera Calderón (2016) titulada “El phishing como delito informático y su falta de tipificación en el Código Orgánico Integral Penal”, entre sus principales conclusiones advierte que:

> El Phishing es un delito informático muy peligroso el cual genera alarma en la sociedad debido a que violenta el derecho a la intimidad y el derecho a la propiedad, derechos que están protegidos constitucional, penal y civilmente.

> (…) El Convenio de Cibercriminalidad de Budapest, es el único acuerdo internacional que cubre todas las áreas relevantes de la legislación sobre ciberdelincuencia, tiene como finalidad la seguridad de la información, tratando delitos contra la alteración de datos, el atentado contra la integridad, contra la confidencialidad de los sistemas, redes informáticas. propone una prioritaria política criminal contra la ciberdelincuencia. (p.115)

Asimismo, en la tesis de posgrado para el grado de Magister, sustentada en la Universidad Regional Autónoma de los Andes, titulada El delito Informático de Phishing, el autor Valle Matute (2013) reconoce que:

> Los sujetos o personas que realizan 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. Del análisis realizado a los diferentes tipos de delitos informáticos, el phishing es una actividad es sumamente lucrativa, y en la gran mayoría de legislaciones internacionales se la considera ilegal. (p.125)

En tal sentido, ambos autores identifican en el phishing una conducta delictiva sumamente peligrosa, cuya tipificación en los ordenamientos jurídicos de cada país es de suma importancia, y, además, identifican con acierto, que el phishing vulnera más que solo el patrimonio de la víctima. Es destacable en estos trabajos, que, en el país vecino de Ecuador a nivel de investigaciones, ya se viene alertando

sobre la necesidad de incluir de manera específica el phishing como delito en su Código Penal; y no podría ser de otra manera, el phishing es una conducta que se realiza de manera masiva. El anonimato y posibilidades de aplicación a escala internacional que caracterizan esta conducta hacen que su tipificación en el ordenamiento jurídico de cada país sea una necesidad imperativa.

Por otro lado, en la Universidad Autónoma de México, en la tesis de pregrado titulada Estudio del impacto de la ingeniería social - phishing, sustentada por Gonzáles Juárez y Peña Enriquez (2012), se califica al phishing como un delito de gran presencia en la sociedad:

> Phishing es el principal delito de estafa a través de la red en la actualidad, esta se realiza al momento de obtener información de algún usuario y suplantar su identidad en diversos medios como son entidades bancarias en línea, servicios de pagos a través de la red, acceder a diversos tipos de redes sociales, etc. (p.109)

Los autores de esta tesis reconocen con acierto que el phishing se ha masificado en la actualidad, siendo el principal delito a cometido a través de las redes, esto debido en parte a la poca intervención necesaria de parte del phisher en algunas de las modalidades. En efecto, los ataques si bien son cada vez más sofisticados, pueden ser difundidos con mayor facilidad, y una mayor cantidad de posibles víctimas son expuestas a los enlaces fraudulentos; esto es una consecuencia inevitable del auge de las redes sociales y el acceso cada vez más fácil a equipos celulares por parte de la población en general, y si a esto le sumamos la evolución de las actividades que se pueden realizar desde un equipo celular –como el acceso a

la banca móvil-, el phishing se vuelve un fenómeno social muy peligroso si no se tipifica adecuadamente.

b) A nivel nacional.

Hancco Zapana (2017) en su tesis titulada: "La tipificación del bien jurídico protegido en la estructura del tipo penal informático como causas de su deficiente regulación en la Ley 30096, Perú – 2017", sustentada en la Universidad Nacional San Agustín para obtener el título profesional de abogado, tuvo como objetivo principal analizar la tipificación del bien jurídico protegido en la estructura del tipo penal informático como causas de su deficiente regulación en la Ley 30096, Ley de Delitos Informáticos.

Dicho estudio tuvo entre sus conclusiones que: primero, los tipos penales sancionados en la Ley 30096 resultan innecesarios siempre que existen tipos penales más amplios y genéricos para tutelar los bienes jurídicos protegidos con la Ley 30096 algo que como tesistas encontramos cuestionable, pues la existencia de tipos penales específicos no puede ser desmerecida de manera tajante; otra de sus conclusiones resaltantes indica que la técnica legislativa empleada para la redacción de los tipos penales regulados en la Ley 30096 es defectuosa, lo que origina una incorrecta tipificación del bien jurídico protegido, el trabajo de investigación descrito reconoce que la forma en que se encuentran redactados los tipos penales de la ley mencionada dificulta su aplicación en un caso concreto, y en el mismo sentido los tesistas pregonamos la necesidad de implementar un tipo penal mucho más específico a fin de corregir la incertidumbre actual en cuanto a la configuración de

los ilícitos penales informáticos; y finalmente, el trabajo de investigación considera que los tipos penales incluidos en la Ley 30096 presentan incoherencia entre la gravedad del injusto y la determinación de la pena, precisando que la norma penal materia de análisis encierra todas las conductas que pudieran afectar un sistema informático, lo que a entender nuestro, es el origen de los problemas de aplicación de los tipos penales informáticos.

Pardo Vargas (2018) en su tesis denominada: "Tratamiento jurídico penal de los delitos informáticos contra el patrimonio, Distrito Judicial de Lima, 2018", presentada en la Universidad Cesar Vallejo – Lima, para obtener el grado de maestro en derecho penal y procesal penal, planteó como objetivo principal analizar el tratamiento jurídico penal de los delitos informáticos contra el patrimonio, Distrito Judicial de Lima, 2018 y entre sus objetivos específicos se analizó el tratamiento jurídico penal de los delitos informáticos contra el patrimonio en su modalidad de fraude.

Mediante el análisis de la realidad jurídica de otros países, a la que tuvo acceso mediante encuestas a expertos de cada país, el investigador concluyó que ninguno de los delitos informáticos contra el patrimonio sancionados en la ley 30096 se encuentra correctamente tipificado, y específicamente en el caso del fraude informático, su deficiencia radica en la amplitud de las conductas que se pretende regular, lo que las vuelve inexactas y poco precisas.

Por nuestra parte, los tesistas consideramos acertado este razonamiento, pues hemos identificado como uno de los principales problemas de la ley 30096 que pretende agrupar diversas conductas ilícitas en un mismo tipo penal, el cual sin

embargo resulta vago y redundante; mientras que, por otro lado, conductas específicas y plenamente identificables como el phishing no pueden encuadrarse en ninguno de los tipos penales introducidos por dicha ley.

También Vega Aguilar (2010) en su tesis denominada "Los delitos informáticos en el Código Penal" presentada en la Universidad Católica de Santa María para obtener el grado de Magister en Derecho Penal aborda como problema principal las razones por las que los delitos informáticos no son denunciados e investigados en sede fiscal y judicial pese a que se encuentran tipificados en el Código Penal vigente, teniendo como objetivo principal demostrar que el problema de los delitos informáticos se debe a que su tipificación en el Código Penal vigente, es deficiente e inoperante frente a los ilícitos que originan el avance tecnológico.

c) A nivel local

Zorrilla Tocto (2018) en su tesis denominada: "Inconsistencias y ambigüedades en la ley de delitos informáticos Ley Nº 30096 y su modificatoria Ley Nº 30171, que imposibilitan su eficaz cumplimiento", presentada en la Universidad Nacional de Ancash Santiago Antúnez de Mayolo – Huaraz, para obtener el título profesional de abogado, identifica que:

> En el Perú no existe una ley que determine específicamente tipos penales que definan los delitos que se presentan con mayor frecuencia en las redes sociales, lo que es necesario para sancionar correctamente estas modalidades delictivas que afectan una sociedad completa. (p. 98)

Esta posición es compartida en cierta medida por los tesistas, pues a lo largo del presente trabajo se realizará un análisis exhaustivo de los tipos penales que, si bien podrían guardar relación con la conducta del phishing, no la regulan correctamente, esto por razones de deficiencias en la técnica legislativa empleada en la Ley, entre otros problemas.

A lo largo de la investigación sustentaremos la necesidad de tipificar de manera específica esta conducta, pues no se adecúa a otros tipos penales, y es diferenciable por la forma en que se ejecuta, los bienes jurídicos que afecta y la participación de cada uno de los intervinientes en la conducta.

1.2.ENUNCIADO DE PROBLEMA

¿Cuáles son los fundamentos jurídicos para tipificar el phishing en el ordenamiento jurídico peruano y evitar su impunidad como conducta delictiva?

1.3.LOS OBJETIVOS DE LA INVESTIGACIÓN

1.1.1. OBJETIVO GENERAL

a. Desarrollar los fundamentos jurídicos para tipificar el phishing en el ordenamiento jurídico peruano y evitar su impunidad como conducta delictiva.

1.1.2. OBJETIVOS ESPECÍFICOS

a. Determinar la relación que existe entre los tipos penales previstos en el Código Penal y la impunidad del phishing.

b. Determinar la relación que existe entre los tipos penales previstos en la Ley de Delitos Informáticos y la impunidad del phishing.

c. Verificar el resultado de las investigaciones fiscales por denuncias de phishing en el Distrito Fiscal del Santa.

d. Proponer la incorporación del phishing como un tipo penal independiente en la Ley de Delitos Informáticos30096.

1.4.FORMULACIÓN DE LA HIPÓTESIS

Dado que es necesario tipificar el phishing en el ordenamiento jurídico peruano para evitar la impunidad de la conducta, es probable que los fundamentos jurídicos que lo justifiquen sean el principio de legalidad y el principio de lesividad.

1.5.VARIABLES

a. Variable Cualitativa 1: La tipificación del phishing en el ordenamiento jurídico peruano.

b. Variable Cualitativa 2: La impunidad del phishing.

Variable	Dimensión	Indicadores	ÍTEMS
V.C.1. Tipificación del phishing en el ordenamiento jurídico peruano	Phishing	Bien jurídico vulnerado	*a. Patrimonio* *b. Fe pública* *c. Intimidad*
	Tipos penales	Código Penal	*a. Hurto* *b. Estafa* *c. Falsedad genérica*
		Ley de Delitos Informáticos	*a. Interceptación de datos informáticos* *b. Fraude informático* *c. Suplantación de identidad*
V.C.2 La impunidad del phishing	Investigaciones Penales	Estado final de las investigaciones fiscales	*a. Archivo* *b. Sobreseimiento* *c. Sentencia absolutoria* *d. Sentencia condenatoria*

1.6.JUSTIFICACIÓN DE LA INVESTIGACIÓN

La presente investigación versa sobre un problema que cada día alcanza una mayor acogida en la realidad peruana, dado que el uso del internet ha pasado de ser un simple instrumento para relacionarse entre personas, a ser utilizado en la realización de diversas transacciones comerciales como financieras, instrumento que viene desplazando a los procedimientos ordinarios y rutinarios, por cuanto su fácil acceso y la menor inversión de tiempo que demanda, han hecho que tenga una gran acogida en la sociedad.

Empero, el internet también se ha vuelto en centro de atención de ciertas personas inescrupulosas, para el despliegue de sus conductas delictivas en el ámbito cibernético, y es por ello, que el Estado, a través del Derecho Penal, ha implementado la ley de delitos informáticos, con la finalidad de castigar aquellas conductas delictivas cometidas en el ámbito de la informática, sin embargo, en dicha ley, no se regulan adecuadamente, por cuanto, las conductas sancionadas en los tipos penales informáticos son muy genéricos e imprecisos, y al no establecer conductas específicas, permiten la impunidad en la gran cantidad de casos, como lo es el caso del phishing, una conducta delictiva que con el transcurrir del tiempo viene siendo ampliamente usada por los comúnmente conocidos en el ámbito informático, como delincuentes de guante virtual, sin embargo, su conducta al no encontrarse regulada en nuestro ordenamiento actual, ha traído como consecuencia la desprotección de los bienes jurídicos afectados con la perpetración del phishing.

De lo explicado en el párrafo anterior se evidencia un vacío en la regulación del phishing como un delito informático, por ello resulta importante evaluar, a través de la

presente investigación, la necesidad de regular dicha conducta como un delito informático. En ese sentido, si incorporamos al phishing como una conducta delictiva prevista en la Ley de delitos Informáticos, tendría cabida una sanción penal y así evitaría la impunidad de dichas conductas.

La presente investigación y su propuesta legislativa busca beneficiar, por un lado, a la población, quienes al realizar constantemente transacciones vía web, están expuestas a ser víctimas del actuar delictivo de los phishers, quienes buscan obtener información confidencial de su víctima para posteriormente hacer uso de ella, en ese sentido, si se regulara dicha conducta, la población podría ver satisfecho su deseo de castigo a dichos delincuentes mediante la imposición de una sanción penal, así también, poder verse resarcidos de los daños ocasionados a sus bienes jurídicos, solicitando una reparación por ello.

Por otro lado, también se beneficiaría con este proyecto el Ministerio Público, por cuanto podría activar su facultad persecutora del delito, y así poder encuadrar dichas conductas en un tipo penal específico y no aventurarse a encuadrarlo en algún otro delito establecido en la ley de delitos informáticos, y no estar con la incertidumbre de que en juicio no se llegue a sancionar por existir un vacío legal, sin embargo, con la incorporación de este delito, el fiscal podrá, con todos los elementos de convicción reunidos, tener la certeza de que en juicio sí se sancionaría dicha conducta.

Por último, el Poder Judicial también se vería beneficiado, por cuanto podría imponer una sanción penal al phisher y de esta forma generar en la población la idea de que el Estado se preocupa por sancionar a quienes cometen conductas delictivas y finalmente reducir los índices de criminalidad cibernética. Pues al no sancionarse

dichas conductas, estaríamos contribuyendo a la impunidad y que aumenten los índices de criminalidad.

Finalmente, a modo de resumen, se precisa que para justificar la presente investigación nos realizamos los siguientes cuestionamientos referidos al trabajo: ¿Por qué?, ¿Para qué? Y ¿Quiénes serían los beneficiados?

Conforme se ha sustentado, el phishing es una conducta cada vez más común, las víctimas de esta modalidad delictiva se incrementan exponencialmente con los años, y eso sin contar los casos en los que la víctima ni siquiera ha podido denunciar por falta de información. Así pues, el phishing se trata de un fenómeno de la realidad social, el mismo que genera un alto grado de reproche en la población, pues las víctimas se ven despojadas de fuertes sumas de dinero y ven imposible la recuperación del mismo debido al alto grado de complejidad del delito y las pocas perspectivas de identificación del autor y su posterior sanción; ante esto, el Derecho Penal no puede hacer caso omiso.

Se hace evidente entonces el por qué de la necesidad de regulación de este delito: porque el Derecho Penal debe sancionar las conductas abiertamente delictivas, y, merced al principio de legalidad, para sancionar una conducta, ésta debe estar previamente tipificada, pues como reza la conocida frase *nulla crime, nulla poena, sine lege*.

La consecuencia inevitable de la regulación de una conducta como delito es que su posibilidad de sanción. La regulación del phishing como delito permitiría a los operadores de justicia (jueces, fiscales) la persecución penal de una conducta que afecta a una gran parte de la población, y en consecuencia permitiría que se apliquen

sanciones a quienes cometen dichos ilícitos. Así, la regulación de este delito serviría para que se evite la impunidad de conductas ilícitas y consecuentemente reducir los índices de criminalidad en relación a delitos informáticos.

El presente trabajo de investigación busca regular la conducta delictiva conocida como phishing la cual afecta a muchas personas quienes se ven víctimas de los ciberdelincuentes, los cuales amparados en el anonimato de su actividad y la poca respuesta por parte de los operadores de justicia, cometen sus crímenes con impunidad.

En ese sentido, los beneficiarios principales serán las personas que con posterioridad a la regulación se conviertan en víctimas de estos ciberdelincuentes, pues tendrán un asidero legal para que se procese y sancione a las personas que cometieron el delito en su agravio; asimismo, la población en general se beneficiaría, pues como se sabe, la pena tiene un efecto disuasorio en los delincuentes, quienes tendrán que decidir si arriesgarse a cometer un nuevo delito sabiendo que existe la posibilidad de ir a la cárcel por ello.

El proponer un proyecto ley, en beneficio de los ciudadanos peruanos, que se encuentren inmersos en los supuestos de la presente investigación servirá como aporte jurídico de solución a esta situación de impunidad en que se encuentra dicha conducta delictiva.

1.7. ESTRUCTURA DEL TRABAJO

La presente tesis describe la siguiente estructura: el Marco Teórico, que está conformado por tres capítulos: CAPÍTULO I, denominado: *"El phishing como comportamiento penalmente relevante",* en el que cual damos a conocer lo referente a

la problemática planteada, sobre la historia, modalidades y fases del phishing, a fin de tener un entendimiento de la complejidad de la conducta objeto de investigación; CAPÍTULO II, denominado: *"El phishing en el ordenamiento jurídico peruano",* en el que se analiza la actual regulación que se hace en nuestro ordenamiento sobre los delitos informáticos, asimismo se evalúan las razones por las que el phishing no se puede subsumir en los tipos penales que existen a la fecha en nuestro Código Penal y la Ley de Delitos Informáticos . CAPÍTULO III, denominado :*"Los fundamentos jurídicos para la tipificación del phishing",* este último capítulo se puntualiza en las bases de nuestro ordenamiento jurídico, que obligan a una regulación estricta de las conductas que pueden ser sancionadas como delito; asimismo, daremos a conocer nuestra propuesta de solución bajo la forma de un proyecto de ley que regule el phishing como un tipo penal específico y autónomo.

Una vez concluido el marco teórico, se describen los Materiales y Métodos, aquí se explica los métodos empleados, las técnicas e instrumentos para recolectar datos y los procedimientos para analizarlos, luego detallamos los resultados, la discusión las conclusiones, las recomendaciones y finalmente las referencias bibliográficas.

1.8.BREVE REFERENCIA DE LOS MÉTODOS EMPLEADOS, DEL TIPO DE INVESTIGACIÓN, Y EL DISEÑO DE INVESTIGACIÓN

El presente trabajo de investigación, según su aplicabilidad es de tipo básica, y su diseño de teoría fundamentada y propositivo, porque se producirá una explicación general a partir del problema identificado de la falta de tipificación del phishing, y para llegar a dicha teoría se analizará la perspectiva de distintos participantes, de manera

que se elaborará una teoría al respecto, la cual será plasmada en un proyecto de ley que permita regular adecuadamente el phishing.

En esta investigación se utilizó, Métodos Científicos y Métodos propios de la Investigación Jurídica; dentro del primero en mención se aplicó el Método inductivo, pues a través del análisis de las investigaciones fiscales del distrito fiscal del Santa en materia de phishing se llegó a la conclusión de que la falta de tipificación de dicha conducta incide en su impunidad.

Así también el Método comparativo, el cual permitió establecer las semejanzas y diferencias que presentan los ordenamientos jurídicos de otros países con el nuestro en la regulación de los delitos informáticos, y específicamente del phishing. Respecto al segundo tipo de método mencionado, se empleó el Método Hemenéutico que contribuyó a la correcta interpretación de la casuística y legislación nacional e internacional estudiada en la presente investigación.

Por otro lado, el método dogmático también fue usado, pues se recurrió a las fuentes formales, como es la legislación nacional y del derecho comparado. Asimismo se empleó el método histórico, al analizar la evolución histórica de la regulación de los delitos informáticos en el país.

También el método literal permitió analizar el contenido de algunos de los tipos penales relevantes para el presente trabajo, mientras que el método de la ratio legis fue empleado para analizar los tipos penales de la Ley de delitos informáticos.

Y finalmente, se usó el método sistemático como método de interpretación de otros tipos penales en los que podría encuadrarse el phishing.

1.9.BREVE DESCRIPCIÓN DE LA BIBLIOGRAFÍA EMPLEADA

Para la presente investigación se ha consultado doctrina nacional e internacional, asi como autores que brindan distintas opiniones sobre la forma en que debe tratarse la regulación del phishing en un ordenamiento jurídico.

Asi también, se han consultado libros virtuales, noticias locales, nacionales e internacionales, revistas jurídicas, páginas online autorizadas; de donde se recogió la información relevante para el desarrollo del presente informe.

II. MARCO TEÓRICO, CASUÍSTICA Y LEGISLACIÓN

CAPITULO I: EL PHISHING COMO COMPORTAMIENTO PENALMENTE RELEVANTE

1.1. ANÁLISIS HISTÓRICO DE LA EVOLUCIÓN DEL PHISHING COMO CONDUCTA DELICTIVA

Actualmente, el consenso es que los primeros casos de Phishing tuvieron lugar en la década de los 90, estos actos fueron llevados a cabo por un grupo de hackers que se hacían llamar “The Warez Community”. Este grupo comenzó creando programas generadores de números de tarjeta de crédito para crear cuentas en AOL. Luego empezaron a hacerse pasar por empleados de AOL para obtener la información de sus clientes a través de la aplicación de mensajería “AOL Messenger”, haciendo uso de ingeniería social. Fue en 1996 cuando por primera vez se utilizó el término “Phishing” para referirse a este tipo de estafas. El origen de la "ph" del término Phishing es un tributo al hácking telefónico “Phreaking” (Phone Hacking).

Cuando la gente empezó a desconfiar de los mensajes que se enviaban por estas aplicaciones de mensajería, los phishers empezaron a utilizar el email como vía de comunicación para perpetrar los ataques de phishing. Al principio, estos mensajes contenían muchos errores gramaticales y no eran muy sofisticados, pero fueron evolucionando rápidamente para ser cada vez más sofisticados y convincentes.

Con el crecimiento de Internet y de los pagos online el phishing fue extendiéndose y ganando interés para los ciberdelincuentes. Ya en septiembre de 2003, los phishers empezaron a registrar dominios que eran similares a otros ampliamente conocidos, como por ejemplo “yahoo-billing.com” y “ebay-fulfillment.com”, con intención de suplantar a estas dos compañías. En Octubre de 2003 se produjo una campaña de phishing

> contra los usuarios de Paypal. El email contenía un enlace el cual abría un popup que pedía las credenciales de acceso a Paypal, que eran robadas y enviadas a los atacantes. En 2004 se produjo otra campaña en la cual se instaba a los usuarios a realizar una donación para el candidato a la presidencia delos Estados Unidos John Kerry. (AndalucíaCERT, 2017, p.4-5)

Actualmente, el phishing es todavía un problema muy relevante, especialmente en América Latina, donde la cultura de prevención no se ha extendido y la legislación al respecto es incipiente, lo que convierte a estos países en blancos fáciles de ciber-ataques. Ello se ve reflejado en un informe elaborado por la empresa Kaspersky Lab, especializada en la venta de antivirus y antimalware, en el que se indica:

> Kaspersky Lab registró más de 746 mil ataques de malware diarios durante los últimos 12 meses en América Latina, lo que significa un promedio de 9 ataques de malware por segundo. Además, los ataques de phishing – correos engañosos para el robo de la información personal de los usuarios– han sido constantes en la región, principalmente en Brasil. Los resultados, presentados durante la Octava Cumbre de Analistas de Seguridad para América Latina que se está realizando en la Ciudad de Panamá, demuestran que toda la región ha experimentado una considerable cantidad de ciberamenazas, con la gran mayoría orientada al robo de dinero. (Latam Kaspersky, 2018)

1.2.¿EN QUÉ CONSISTE EL PHISHING?

El phishing no puede ser contemplado dentro de un concepto específico y único, por cuanto las conductas desplegadas por los ciberdelinuentes son diversas, sin embargo, estas conductas tienen características similares o particulares que permiten catalogarlas dentro del phishing y diferenciarlas de las demás conductas de delincuencia informática.

El termino Phishing es utilizado para referirse a uno de los métodos mas utilizados por delincuentes cibernéticos para estafar y obtener información confidencial de forma fraudulenta como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria de la victima. El estafador, conocido como phisher, se vale de técnicas de ingeniería social, haciéndose pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica, por lo general un correo electrónico, o algún sistema de mensajería instantánea, redes sociales SMS/MMS, a raíz de un malware o incluso utilizando también llamadas telefónicas.

Por consiguiente, y en pocas palabras, el phishing podría definirse como el envío masivo e indiscriminado de spam conteniendo información falsa, tendiente a la obtención de datos personales privados, conducta que se conoce como phishing

En primer lugar, se debe analizar a grandes rasgos, qué es aquello que se ha denominado phishing. En este sentido, en las últimas décadas ha surgido una nueva forma de comportamiento, que generalmente consiste en el envío masivo de correos electrónicos, los cuales simulan una comunicación de carácter oficial, con el fin de obtener por parte de los receptores de estos

> mensajes, informaciones de carácter confidencial. (Sánchez Bernal, 2009, p.107)

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", las letras ph en el término hace referencia a la primera modalidad del phishing mejor conocido como phreaking que es una antigua suplantación telefónica.

Señala Hancco (2017), respecto al phishing:

> También conocido como robo de identidad, esta modalidad de fraude consiste en el envío de supuestas promociones y ofertas comerciales que la víctima debe aceptar insertando sus datos en los formularios simulados que enviarán la información a los delincuentes y estos con dicha información obtendrán beneficios con perjuicio de la víctima, que cuando revise su estado de cuenta recién se dará cuenta del delito del cual ha sido objeto. (p.33)

Si bien todas estas definiciones hacen alusión a una suerte de estafa o defraudación cometida por medios electrónicos cuya finalidad es apoderarse del patrimonio de la víctima, no debemos caer en el error de suponer que la única aplicación del phishing es esa. El phishing como técnica para captura de datos personales no tiene un único uso, puede ser usada para capturar datos íntimamente

personales, sin que se encuentre presente el componente de trascendencia interna denominado "ánimo de lucro".

Y es que, como se verá más adelante, existen diferentes modalidades de phishing, una de las cuales –el spear phishing- bien podría ser usado por un sujeto que quisiera acceder a algún tipo de información confidencial de un conocido sin que ello implique un perjuicio patrimonial para la víctima.

En efecto, existen muchas razones por las cuales una persona querría acceder a información confidencial de su víctima, ello puede obedecer a fines de satisfacción sexual, de chantaje, de obtención de una posición de poder, entre otras. Sin olvidar claro, que uno de sus principales usos es con fines de lucro, de ahí que tradicionalmente se relacione al phishing con defraudaciones bancarias.

Así pues, durante el presente trabajo tendremos siempre presente que el phishing es, en esencia, el uso del spam mediante las tecnologías de información, para obtener datos confidenciales de la víctima, los cuales pueden luego ser usados para diversos fines.

1.3.TIPOS DE PHISHING

Cuando nos referimos a los tipos de phishing, no hacemos alusión a la finalidad por la cual se comete el acto de phishing, sino a las variaciones en el procedimiento efectuado por el phisher para obtener la información confidencial de la víctima. Estos tipos de phishing se pueden diferenciar e identificar en función del nivel de complejidad que requiere la técnica empleada, así como el nivel de

cooperación que debe ofrecer la víctima para la concreción del phishing, parámetros que son inversamente proporcionales.

1.3.1. DECEPTIVE PHISHING

Dentro de los tipos de phishing, el deceptive-phishing es el que más requiere una colaboración por parte de la víctima, pues la técnica empleada consiste en la suplantación de una entidad conocida para la víctima, a partir de lo cual se le solicita la introducción de sus datos en una página web específicamente diseñada para ello. “Consiste en el envío de un correo electrónico engañoso en el que se suplanta a una empresa o institución de confianza. El receptor pulsará en el enlace contenido en el mensaje, siendo desviado de manera inconsciente a un sitio web fraudulento” (Belisario Méndez, 2014, p.25).

Este tipo de ataque es el más sencillo a la hora de analizarlo técnicamente; normalmente está vinculado a la copia de un sitio conocido por la víctima, en el cual se cambia la dirección a donde llegan los datos ingresados. De este modo, el ciberdelincuente roba las credenciales ingresadas por la víctima, que pueden estar alojadas en texto plano en un archivo de texto o ser enviadas a alguna casilla de correo electrónico (Paus, 2015).

En ese sentido, la principal característica de este tipo de phishing tradicional es que está ligado a un solo sitio web en el cual se alojan todos los contenidos del portal falso.

Esta sería la forma en la que se originó el phishing (AOL). Su procedimiento es sencillo: consiste en el envío masivo de correos

> electrónicos en donde se suplanta una identidad legítima. En este email se piden unos datos por medio de un enlace ficticio y manipulado. Los motivos utilizados para e ngañar al usuario son varios como la existencia de algún problema en la cuenta bancaria del usuario. La finalidad de esto es que la víctima ingrese sus datos en la página web a la cual dirige el enlace y así obtener esta información que luego puede ser utilizada por el phisher de forma fraudulenta, como realizar compras o suplantar la. (Leguizamon, 2015, p. 20)

1.3.2. MALWARE-BASED PHISHING

En esta modalidad de ataque por phishing, el phisher es una persona con mayores conocimientos en informática, se vale de herramientas (programas informáticos) mucho más sofisticadas, y en muchos casos la colaboración de la víctima es poca o nula.

Según indica Leguizamon (2015):

> Este tipo de estafa implica la instalación de software malicioso en el ordenador de la víctima. Su propagación depende tanto de la ingeniería social y de la explotación de la vulnerabilidad del sistema. En el primer caso se necesita la acción de la víctima para que el ataque pueda dar lugar, por ejemplo que abra el archivo adjunto de algún correo electrónico y así el malware se le pueda instalar en el ordenador. En el segundo de los casos, el usuario tiene muy poca implicación. Es decir, aunque en muchas ocasiones es por parte del usuario la instalación de un malware, en muchos otros casos se pueden instalar debido a algún fallo en el sistema de seguridad del equipo. (p.21)

1.3.3. SPEAR PHISHING

El spear-phishing es un técnica mucho más personalizada, donde el phisher elige cuidadosamente a su víctima, la estudia, y luego despliega el engaño mediante medios informáticos, en este tipo de ataques el phisher se vale de algún tipo de información personal que haya podido captar de la víctima para elaborar un engaño convincente que vulnere sus defensas, esto podría ser valiéndose por ejemplo de sus intereses deportivos, creencias religiosas, hobbies, intereses culinarios, información laboral, etc.

> La diferencia entre los ataques de phishing común basado en email y el spear phishing es que no son ataques aleatorios y generalizados, sino que están dirigidos a una organización o individuo en particular. Los ataques de spear phishing tienen altas probabilidades de ser exitosos porque no son detectados fácilmente por herramientas de antispam. Utilizando suplantación de identidad, el origen del correo electrónico pareciera ser de una persona de alta jerarquía dentro de la organización solicitando algún tipo de información con carácter de urgencia e importancia, engañando así a usuarios con y sin conocimientos en informática. Así obtiene acceso completo a información de interés de la víctima. (Belisario, 2014, p.25)

Raramente se ven casos que afecten entidades bancarias o redes sociales, debido a que no buscan la masividad sino todo lo contrario; en realidad, este tipo de métodos es utilizado en ataques como los APTs, apuntando a empleados de empresas con perfiles determinados. Esto significa que las víctimas podrían recibir correos personificados con nombre y apellido, incluso falsificando

direcciones conocidas para generar una mayor empatía y confianza de un navegante incauto. Debemos tener en cuenta que si los ciberdelincuentes quisieran adentrarse en los sistemas buscarían el eslabón más débil dentro de la red. De este modo, no debemos esperar que el Gerente de Sistemas sea el blanco principal de este tipo de ataque, sino alguien con menos conocimientos técnicos de informática, como en muchos casos es alguien de áreas no relacionadas (por ejemplo, administración o recursos humanos).

Esta metodología, en conjunto con Ingeniería Social y un estudio previo de las víctimas, da como resultado una sólida técnica con la que muy fácilmente se podría comprometer un sistema o red corporativa bajo el robo de credenciales. (Paus, 2015)

Bajo esta técnica el phisher puede acceder a información que, si bien no le permita obtener beneficios económicos directamente, podría ser usada para obtener algún otro tipo de ventaja indebida, por lo que podría darse el caso de que el atacante sea alguien dentro del entorno personal o laboral de la víctima.

1.3.4. SMISHING

En este tipo de phishing –de amplia difusión en la actualidad- se hace uso de técnicas de ingeniería social mediante equipos celulares para que la víctima realice una de las siguientes acciones: haga click en un hipervínculo, llame a un número telefónico, o responda un mensaje de texto.

Como suele ocurrir, el objetivo de esta operación es obtener un redito económico, el cual muchas veces está ligado a estafas de distintas formas. En la región se encontraron campañas en las que luego de algunos mensajes de felicitaciones por

haber ganado algún tipo de premio, se pedían datos personales o incluso se instauraban falsos centros de atención telefónica donde de una manera muy profesional, engañaban a las víctimas pidiendo sus datos de cuentas bancarias e incluso los números de sus tarjetas de crédito. (Paus, 2015)

1.4.FASES DEL PHISHING

El phishing es una conducta compleja, por cuanto consiste en diversas fases o momentos que complican su tratamiento jurídico, pues resulta complejo determinar en qué momento se ha producido ya una afectación a un bien jurídico, y en qué momento empiezan los actos ejecutivos; además de que si es posible sancionar los actos preparatorios. Adicionalmente, la existencia de estas diversas fases hace que sea necesario determinar el momento de la consumación del delito.

1.4.1. FASE DE PLANIFICACION

En teoría general del delito se ha reconocido que el delito tiene dos fases, una interna y una externa; la fase interna o de ideación, se corresponde al plano abstracto en que el sujeto activo define en su mente los alcances del hecho que piensa cometer. De manera similar, esta fase consiste en la etapa en que el phisher se plantea los alcances de su conducta.

> Como bien dice su nombre, es la etapa donde el estafador prepara su ataque: decide quien será su víctima, cual es el método que utilizará, a que organismo o empresa va a suplantar, que busca con este ataque, que medios utilizará. Esta es una etapa, se podría decir “común” a todos los ataques phishing. El phisher es aquí donde toma una de las decisiones más

> importantes: si el ataque va a ser realizado de forma individual o de forma colectiva. Según esta decisión, el atacante también se planteará cuáles son los datos que desea conseguir: si son contraseñas de redes sociales, números de tarjetas bancarias, si quiere conseguir datos personales. (Leguizamón, 2015, p.15)

1.4.2. FASE DE PREPARACION

En este punto el phisher se agencia de los medios informáticos necesarios para cometer el acto de phishing de acuerdo a lo que ha ideado. Así por ejemplo, puede ir preparando las páginas web falsas, elaborando los correos fraudulentos, captando información personal de la víctima en caso del spear-phishing, elaborando un *keylogger* o creando los archivos necesarios para insertar malware en la computadora de la víctima.

Tal como indica Leguizamón (2015):

> En general no hay mucha diferencia entre los tres tipos de phishing según la complejidad y la participación, pero sí que hay diferencias en la manera de llevar a cabo el ataque, es decir, para su creación y consecución. Esto es así porque el delincuente según el tipo de información que quiera conseguir, tendrá que utilizar medios diferentes, es decir, teniendo en cuenta las necesidades de cada delito. Por ejemplo si hablamos de un destinatario individual, el correo electrónico que se le envía tiene que estar mucho más elaborado, mucho más preparado y personalizado ya que la víctima es más concreta. Si se tratara de destinatarios colectivos, al ser un envío masivo no hace falta que el correo que se les envía sea tan personal. (p.16)

1.4.3. FASE DE ATAQUE

Con todos los elementos que requiere a su disposición, el phisher procede a lanzar el ataque, que generalmente consiste en el envío de los emails, publicidad de facebook, mensajes de whatsapp, sms, etc.

> Una vez enviados estos correos, aquellos tipos de phishing que necesitan la participación de la víctima de una forma alta o media, van a tener éxito una vez estas caigan en la trampa, como abriendo el link fraudulento y dar sus datos personales. Aquí según el tipo de phishing que se haya elegido, las tareas serán diferentes. Si hablamos de un phishing con baja participación de la víctima, como un ataque al servidor, la tarea fundamental será llevar a cabo este ataque con los medios necesarios. Si hablamos de los otros dos tipos de ataque, la preparación consistirá en preparar las diferentes trampas para la víctima. En esta fase, es interesante conocer cómo se realiza un ataque phishing por medio de un malware. Es decir, lo que sería la "anatomía del phishing". Aquí distinguimos siete elementos esenciales que son: el malware en sí, la infección, la ejecución, la entrada de datos, el atacante y el servidor legítimo. Hay dos puntos de infección importantes: el momento de la propia infección, es decir cuando el malware entra en el sistema sin necesidad de ejecutarlo y cuando se ejecuta el código malicioso. (Leguizamon, 2015, p. 17)

Podría decirse que en este punto nos encontramos ya ante actos ejecutivos, pero ello implicaría que los actos de obtención de programas maliciosos, creación de páginas web falsas, etc, no serían pasibles de ser sancionadas como delitos, al ser meros actos preparatorios. Sin embargo, es preciso indicar que existen en la Ley de Delitos Informáticos algunos tipos penales

que sancionan de manera independiente algunas conductas que podrían considerarse actos preparatorios.

1.4.4. FASE DE RECOGIDA DE DATOS

Dependiendo del tipo de phishing así como las herramientas empleadas por el phisher, esta fase o etapa consiste en esperar que la víctima permita la ejecución del malware, ingrese sus datos confidenciales en la página falsa, ejecute el programa malicioso, descargue un archivo, u otro.

A partir de ello, dependiendo del nivel de participación del phisher necesario, éste procederá a recabar la información personal de la víctima. Actualmente este proceso se ha automatizado casi en su totalidad, y el phisher solo tiene que acceder a un dominio donde se ha almacenado toda la información brindada por la víctima.

Uno de los grandes problemas con la tipificación del phishing es si se debe o no considerar que en este punto ya se ha consumado el delito. Generalmente, la respuesta sería que dado que no se ha provocado todavía ningún perjuicio económico para la víctima, todavía no se ha consumado el delito. Sin embargo, dado que el phishing no necesariamente está vinculado al acceso a información financiera de la víctima, vale la pena preguntarse si tratándose de otro tipo de información personal e íntima de la víctima, el solo acceso a dicha información no constituye ya un perjuicio para la víctima y por tanto, habría consumación. Pongamos un ejemplo: un sujeto obsesionado por un compañera de trabajo procede a usar un ataque de spear-phishing (con base en las creencias religiosas de la víctima) para su computadora y

apropiarse de fotografías de contenido íntimo, las cuales usa para su satisfacción sexual personal, sin divulgarlas; posteriormente el sujeto es descubierto por encontrarse inmerso en otro delito informático, y al analizarse su computador, se encuentran las fotografías. Dicha conducta en agravio de la compañera de trabajo, ¿sería un hecho tentado? O debería ser tratado como un hecho consumado. La distinción pues, dependerá del momento en que se determina la consumación del ilícito en un eventual tipo penal, por lo que este problema, que parece teórico, tiene importantes aplicaciones prácticas.

1.4.5. FASE DE EJECUCION

Se conoce como tal a la etapa en la que el phisher hace uso de la información confidencial recabada, la cual puede usarla directamente para su propio beneficio, o puede brindársela a un tercero para que éste sea el beneficiario. Siguiendo el razonamiento anterior, si se considera que recién en esta fase se da la consumación del delito, algunas conductas quedarían impunes, como es el caso del phisher que obtiene información personal o íntima de la víctima pero no la usa para chantajearlo ni provocarle un perjuicio patrimonial.

Otro aspecto importante a debatir es qué grado de responsabilidad penal y bajo qué título de autoría se sancionaría a la persona que sin haber participado del proceso de obtención de la información, hace uso de ella para obtener una ventaja ilícita indebida.

1.4.6. FASE POST-ATAQUE

Esta fase corresponde a las acciones que realiza el phisher luego de producido el perjuicio, para evitar ser relacionado con el hecho que acaba de cometer. Según indica Mariana Leguizamón (2015):

> En este punto, el phisher tiene como objetivo, eliminar todo rastro que pudiera luego inculparle de este delito. Cabe decir, que si hablamos de un phishing bancario, el estafador luego procederá a la comisión de otro delito: el blanqueo de capitales o similares. (p.18)

1.5.NATURALEZA JURIDICA DEL PHISHING

En este punto, es importante precisar cuál es la naturaleza jurídica de la conducta denominada phishing, pues a partir de dicha definición se podrá determinar su tratamiento jurídico.

1.5.1. ACTOS PREPARATORIOS

Como se ha indicado previamente, el phishing tiene varias fases o etapas, las cuales se van ejecutando progresivamente. Así, resulta interesante analizar el momento en que el phisher ha obtenido la información personal de la víctima (por ejemplo, claves de acceso bancario), pero todavía no hace uso de las mismas. La cuestión es, si en este punto ya se ha cometido un delito, o nos encontramos todavía frente a los actos preparatorios para la comisión de algún delito. En países como España, estos actos no se pueden tipificar como un delito autónomo, ni como tentativa. Así lo afirma Miró Linares (2013):

> Podríamos tener en cuenta la doctrina jurisprudencial referida a los casos de sustracción de las claves de una tarjeta para posteriormente ser utilizadas en un cajero o comercio, en las que se considera que todavía no hay inicio de la tentativa ni el hecho es reconducible a ningún tipo patrimonial. (p.18)

Sin embargo, a nuestro entender, hay situaciones en las que la mera posesión de la información de la víctima es un acto con un alto grado de peligrosidad que justificaría la configuración de un delito al menos en grado de tentativa, como es el caso del phisher que tiene en su poder las claves de acceso bancarias de la víctimas, las cuales permiten realizar una transferencia de manera inmediata, este acto de posesión es de peligrosidad idónea para la realización de la transferencia en perjuicio de la víctima.

Y en otros casos la mera posesión de la información debería ser suficiente para configurar el delito, cuando la información obtenida por el phisher sea tal que su solo conocimiento ya suponga una afectación a algún bien jurídico de la víctima, como puede ser el caso de información íntima de contenido sexual, familiar, de salud, entre otros.

1.5.2. CONCURSO REAL DE DOS O MÁS DELITOS

El phishing tiene diversas fases, y como se precisó, de crearse un tipo penal que lo subsuma, será imprescindible determinar en qué momento se

produce la consumación del hecho, ello por cuanto parece que varias de las fases del phishing podrían subsumirse de manera independiente en un delito.

Veamos el típico caso de un phishing bancario: el phisher primero planea el ataque, para lo cual (1) estudia una entidad bancaria "Y" de reciente ingreso al mercado local; tras ello, (2) se agencia de los medios necesarios para cometer el acto, lo que consiste en elaborar una página web falsa idéntica a la de la entidad bancaria "Y", también se crea un perfil en facebook falso con el nombre similar al de la entidad Y; luego, (3) en diversos grupos de facebook publica el enlace de su página web falsa; tras ello, (4) espera a que algún incauto caiga en el engaño y acceda al enlace, donde deberá ingresar sus datos bancarios de la entidad "Y"; una vez logrado esto, el phisher (5) recopila y clasifica la información que ha obtenido de las víctimas; y finalmente, (6) hace uso de dicha información bancaria para realizar compras por internet a su favor.

A partir de este breve ejemplo, se plantea la siguiente interrogante: ¿Tiene contenido penalmente relevante la conducta del phisher que solo ha llegado a la segunda etapa? La respuesta dependerá de la interpretación que se dé al artículo 10 de la Ley de Delitos Informáticos, en el que se sanciona al que desarrolla mecanismos, programas informáticos o cualquier otro dato informático diseñado específicamente para la comisión de un delito informático, se trata de un delito de mera actividad.

Y es el caso que una página web falsa idéntica a la de una entidad bancaria podría considerarse como tal. Pero además, cuando el phisher hace

uso de la información bancaria de la víctima para realizar una compra por internet simulando ser el titular de la cuenta bancaria, ¿no comete también un delito de suplantación de identidad? Esta es la razón por la cual se podría decir que el phishing como conducta es lo suficientemente compleja para tipificarse en más de un delito independiente.

Pero, si la intención es crear un solo tipo penal que englobe a todas estas fases del phishing, lo lógico es que ya no sea admisible el concurso real de delitos, pues el tipo penal creado deberá ser autosuficiente para subsumir todo el proceso del phishing, y en aplicación de los principios de especialidad y subsunción, ser el único tipo penal aplicable a la conducta.

1.5.3. DELITO AUTÓNOMO

La posición de los autores respecto a la conducta conocida como phishing, es que si bien es un proceso con diversas fases y modalidades, es posible establecer un solo tipo penal que englobe a todo el proceso, partiendo del hecho de que incluso las diferentes modalidades de phishing tienen un aspecto en común, que es el uso de técnicas de ingeniería social y el spam como medio de acercamiento a la víctima.

1.5.4. ¿DELITO DE MERA ACTIVIDAD O RESULTADO?

En función de las consecuencias que produce la acción, los tipos penales pueden ser clasificados en formales (o de mera actividad) y materiales (o de resultado). En los delitos de resultado se exige para la

consumación y agotamiento que la conducta típica produzca además un efecto separado y distinguible de la conducta, mientras que en los delitos de mera actividad el contenido del injusto se agota en la simple realización de la conducta, sin que sea necesaria la producción de un resultado distinto a la conducta misma.

Ahora bien, el phishing es una conducta pluriofensiva, esto es, se afectan varios bienes jurídicos como veremos en el acápite siguiente, por lo que es relevante determinar si basta que se cree un peligro para el bien jurídico o es necesario que se produzca un resultado lesivo.

La dificultad en este punto radica en que es perfectamente posible que el phisher no sea la persona que produce el resultado de manera directa; como es el caso del phisher que prefiere vender la información que ha obtenido para que sea un tercero quien, usando dicha información, produzca el resultado lesivo para –por ejemplo- el patrimonio de la víctima.

Así pues, ¿ha consumado ya un ilícito el phisher que se limita a obtener la información confidencial de la víctima, o es preciso que se emplee dicha información y se cause un perjuicio tangible para la víctima? A nuestro criterio, la estructuración de un tipo penal de mera actividad permite solucionar el dilema de dejar impunes conductas que representan un riesgo tangible para un bien jurídico, de modo que en caso se concretice una lesión a los bienes jurídicos de la víctima podríamos encontrarnos ante un agravante.

1.6.EL BIEN JURIDICO AFECTADO EN EL PHISHING

Cuando hablamos de phishing, lo primero que viene a la mente es lo que comúnmente se ha pasado a denominado phishing bancario, aquel por el cual el phisher lo que obtiene es información financiera de la víctima (números de cuenta, contraseñas, token de seguridad, claves de internet, etc), la cual luego usa para realizar transferencias bancarias hacia sus cuentas o de un tercero. Por lo que es un error entendible el considerar que el phishing atenta exclusivamente contra el patrimonio.

Nada más lejos de la realidad; el phishing es un proceso por el cual el phisher obtiene información confidencial de la víctima. Esta información no necesariamente tiene que ser sobre la actividad bancaria del afectado. A través del phishing una persona podría acceder a las redes sociales, email, datos de la nube u otros de su víctima. Pongamos un ejemplo: un phisher obtiene a través de una falsa campaña benéfica los datos de acceso a la red social Facebook de una fémina; a partir de ello, el phisher accede a la red social y realiza una revisión de todas las conversaciones de la víctima, encontrando fotos íntimas que ésta le había enviado a su pareja y emplea dicha información para chantajear sexualmente a la víctima.

En este caso no se ha atentado contra el patrimonio de la víctima, sino contra su intimidad y libertad sexual. Es por eso que resulta importante identificar que la confidencialidad de la información sensible es el bien jurídico que típicamente se vulnera con esta conducta, independientemente de que luego se emplee la información obtenida para otros fines.

1.7. ¿QUÉ DEBE ENTENDERSE POR INFORMACIÓN SENSIBLE?

Como se ha indicado precedentemente, la confidencialidad de la información sensible es el bien jurídico principalmente afectado por el phishing. Pero debe entenderse que no toda la información de una persona puede considerarse información sensible; así, se tienen los llamados datos personales, que permiten identificar adecuadamente a una persona, pero que son de acceso público, como pueden ser el nombre y apellidos. Sin embargo, existe otro tipo de información cuya divulgación solo compete al titular de la misma, por lo que cualquier acceso ilegítimo a la misma se debe considerar una vulneración a un bien jurídico: nos referimos a la información sensible.

En la Ley 29733 – Ley de Protección de Datos Personales, en el artículo 5 se considera datos sensibles a aquellos "constituidos por los datos biométricos que por sí mismos pueden identificar al titular; datos referidos al origen racial y étnico; ingresos económicos; opiniones o convicciones políticas, religiosas, filosóficas o morales; afiliación sindical; e información relacionada a la salud o a la vida sexual".

CAPITULO II: EL PHISHING EN EL ORDENAMIENTO JURÍDICO PERUANO: CÓDIGO PENAL Y LEY DE DELITOS INFORMÁTICOS

2.1.LOS DELITOS INFORMÁTICOS EN EL PERÚ

En nuestro ordenamiento jurídico, el primer esbozo respecto a la intervención del derecho penal en el ámbito de la delincuencia informática lo constituye la Ley 27309 mediante el cual se incorporaron tres tipos penales al Libro Segundo, Capítulo V del Código Penal, los cuales eran los siguientes: 207-A, 207-B y 207-C.

Este intento incipiente de regular algunas conductas delictivas relacionadas al creciente auge del comercio electrónico y el almacenamiento masivo de datos sumamente importantes mediante las tecnologías de información no tuvo mayor éxito, debido a lo poco desarrollado del tema en el país y la vaguedad de las conductas tipificadas.

El primer tipo penal incorporado por la Ley 27309, en el artículo 207-A denominado Ingreso indebido a bases de datos y sistemas prescribía lo siguiente:

Artículo 207-A - "El que utiliza o ingresa indebidamente a una base de datos, sistema o red de computadoras o cualquier parte de la misma, para diseñar, ejecutar o alterar un esquema u otro similar, o para interferir, interceptar, acceder o copiar información en tránsito o contenida en una base de datos, será reprimido con pena privativa de libertad no mayor de dos años o con prestación de servicios comunitarios de cincuentidós a ciento cuatro jornadas. Si el agente actuó con el fin de obtener un beneficio económico, será reprimido con pena privativa de libertad no mayor de tres años o con prestación de servicios comunitarios no menor de ciento cuatro jornadas.

Lo relevante en este tipo penal es la inclusión del ánimo de lucro en el autor como un agravante, de manera que el legislador acertadamente comprendía que la intrusión del agente en las bases de datos no necesariamente obedecía siempre a un fin

lucrativo, pues el bien jurídico tutelado en este tipo de delitos informáticos es, primero, la confidencialidad de la información almacenada en las bases de datos a los que accede el agente; de ahí que, en caso de que el agente haga uso de dichos datos para obtener una ventaja económica indebida, dicha extensión de su conducta pueda ser reputada como un agravante.

En una posición que no compartimos, el autor Peña-Cabrera Freyre (2000) sostiene que:

> El legislador reprime con mayor pena, cuando la conducta es ejecutada con el afán de obtener dividendos económicos, de hacerse indebidamente de un patrimonio ilícito, con arreglo a lo establecido en el segundo párrafo del artículo 207°-A, lo cual lo aleja en realidad de la esencia sustantiva de los injustos informáticos, en la medida que ésta sería una modalidad típica de la estafa o del hurto por medio de instrumentos electrónicos. Aspecto que ha mentado en la doctrina nacional, estimar que el móvil lucrativo sólo ha de valorarse en lo que a esta circunstancia agravante se refiere, por lo que en el tipo base, resulta irrelevante el móvil o propósito del agente o autor de los comportamientos descritos. A nuestro entender, de común idea con lo antes anotado, esto no es así, al constituir los propósitos ulteriores elementos del ánimo que han de concurrir también en el comportamiento básico, con la única diferencia que la motivación lucrativa, ha despertado en el legislador una reprobación jurídico-penal más intensa. Si el autor ingresó de forma indebida a una base de datos, pero sólo con el objetivo de curiosear la información, conduce a una valoración negativa de la tipicidad penal. (p.729)

Esto es, desde nuestro punto de vista, errado, por cuanto el citado autor parece confundir el bien jurídico protegido en este tipo de delitos, el cual no necesariamente es el patrimonio de la víctima, sino la intimidad y confidencialidad de la información que considera lo suficientemente sensible como para almacenarla en bases de datos con sistemas de seguridad.

Así, cuando el legislador reprime con mayor severidad la obtención de un beneficio económico indebido para el autor, lo que se hace es considerar que en dicho caso se ha vulnerado más de un bien jurídico (intimidad de la información y el patrimonio) por lo que al tratarse de un delito con la posibilidad de ser pluriofensivo, se justifica la inclusión de una agravante específica.

En cuanto al segundo artículo incluido en el Código Penal mediante la Ley 27309, se tipificó en el artículo 207-B y describía lo siguiente:

Artículo 207-B - El que inutiliza, ingresa o interfiere indebidamente una base de datos, sistema, red o programa de computadoras o cualquier parte de la misma con el fin de alterarlos, dañarlos o destruirlos, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años y con sesenta a noventa días multa.

En cuanto a este tipo penal, es cuestionable si se requería la inclusión en el Código Penal de un tipo específico para regular los daños ocasionados a los datos almacenados en sistemas informáticos o simplemente bastaba con añadir una nueva modalidad al clásico delito de daños regulado en el artículo 205 del Código Penal.

Primero es necesario identificar que, si bien se hace uso de medios informáticos, la finalidad ulterior del agente es en sí provocar daños, dejar inutilizable, o destruir, la información contenida en el sistema informático atacado. Sin embargo, lo que

diferencia la conducta del clásico delito de daños radica en el "bien" objeto del delito. Es cierto que en algunos casos mediante el ataque a sistemas informáticos se puede producir daños en el *hardware* que soporta el *software* objeto del ataque, pero, en esencia lo que busca dañar el agente es la información confidencial o sensible ubicada en el sistema informático, en suma, se trata de datos o *software* que no siempre tendrá una valoración económica susceptible de medición.

Pues no debemos olvidar que el delito de daños es un delito contra el patrimonio, donde cobra especial relevancia el valor del bien objeto de destrucción o daño. Y es en los casos en que la información destruida o dañada no es susceptible de valoración económica que se evidencia la necesidad de tipificar independientemente los ataques a estos sistemas informáticos.

Tomemos por ejemplo el caso de un *hacker* que mediante el uso de un *virus computacional* consigue que se dañen de manera irreparable unas fotografías apreciadas por la víctima, o un proyecto de estudios que se encuentra en desarrollo y por tanto solo en formato digital; en estos supuestos no es posible establecer un valor económico para los bienes dañados, sin embargo, el perjuicio para la víctima es evidente.

Finalmente, el último artículo adicionado en la Ley 27309 solo incluía agravantes para las conductas antes analizadas, por lo que no amerita mayor análisis.

2.2.EVOLUCION DE LA LEY 30096

En el año 2013 se promulgó la Ley 30096, Ley de Delitos Informáticos (LDI), dispositivo normativo penal sancionador publicado en el diario El Peruano el 22 de octubre del 2013, dicha ley establece las sanciones penales para las conductas delictivas

a través de medios informáticos. Esta ley especial en su inicio prevé diez tipos penales, los cuales se encuentran sancionados de manera específica y divididos según el bien jurídico que aparentemente se vulnera en cada delito. Estos artículos son los siguientes:

Artículo	Conducta típica	Bien jurídico protegido
Art. 2.- Acceso ilícito	Acceder sin autorización	La privacidad
Art. 3.- Atentado contra la integridad de datos informáticos	Introducir, borrar, deteriorar, alterar, suprimir, hacer inaccesible	La integridad de los datos informáticos
Art. 4.- Atentado contra la integridad de sistemas informáticos	Inutilizar total o parcialmente, impedir el acceso, entorpecer o imposibilitar el funcionamiento	La integridad de los sistemas informáticos
Art. 5.- Proposición a niños, niñas y adolescentes con fines sexuales por medios tecnológicos	Contactar con un menor para: 1) solicitar u obtener material pornográfico; 2) llevar a cabo actividades sexuales con él	Indemnidad sexual y libertad sexual.
Art. 6.- Tráfico ilegal de datos	Crear, ingresar, o utilizar datos informáticos privados para comercializar, traficar, vender o facilitar información.	Privacidad de la información

Art. 7.- Interceptación de datos informáticos	Interceptar datos informáticos en transmisiones no públicas	La privacidad de los datos informáticos
Art. 8.- Fraude Informático	Obtener provecho mediante el diseño, introducción, alteración, borrado, supresión, clonación de datos informáticos	El patrimonio
Art. 9.- Suplantación de identidad	Suplantar la identidad de una persona natural o jurídica con perjuicio material o moral	La fe pública
Art. 10.- Abuso de mecanismos y dispositivos informáticos	Fabrica, diseña, desarrolla, vende, facilita, distribuye, importa u obtiene uno o más programas para cometer actos ilícitos	La seguridad pública

Adicionalmente, con fecha 10 de marzo de 2014, se publicó la Ley N° 30171 mediante la cual se modifica la Ley de Delitos Informáticos. En dicha Ley se modifican los artículos 2°, 3°, 4°, 5°, 7°, 8° y 10° de la Ley 30096, básicamente dicha modificación consiste en agregar a los antes mencionados artículos las palabras "deliberada e ilegítimamente", lo que no hace más que resaltar que los delitos previstos en dichos artículos solo pueden ser cometidos dolosamente.

Ello además guarda relación con la incorporación del artículo 12° a la Ley 30096 que establece que estará exento de responsabilidad penal quien realice las conductas descritas en los artículos 2°, 3°, 4° y 10° con el propósito de llevar a cabo

pruebas autorizadas u otros procedimientos autorizados destinados a proteger sistemas informáticos. Otro aspecto imporante fue la derogación del artículo 6° que estaba referido al tráfico ilegal de datos.

Respecto a la Ley de Delitos Informáticos, el jurista Villavicencio Terreros (2014) precisa:

> El artículo 1 de la Ley de delitos informáticos establece que la finalidad de la ley es prevenir y sancionar las conductas ilícitas que afectan los sistemas, las datas informáticos, el secreto de las comunicaciones; y otros bienes jurídicos de relevancia penal (como el patrimonio, la fe pública, la libertad sexual, etcétera) que puedan ser afectados mediante la utilización de las TIC, con la finalidad de garantizar las condiciones mínimas para que las personas gocen del derecho a la libertad y al desarrollo. Con esta ley se intenta garantizar la lucha eficaz contra la ciberdelincuencia.
>
> Esta Ley no responde solo a la necesidad de ejercer la función punitiva del estado enfocada en la protección de la información; sino que tiene como principal objetivo la estandarización de la ley penal peruana con el ordenamiento penal internacional, principalmente por el Convenio contra la cibercriminalidad del Consejo europeo (Cets 185), denominado Convenio de Budapest. (p.288)

2.3.ANALISIS DEL TIPO PENAL DE FRAUDE INFORMÁTICO

El citado Villavicencio Terreros (2014) al realizar un análisis de la Ley 30096 indica respecto al bien jurídico protegido de los delitos sancionados en dicha Ley que:

> El bien jurídico tutelado en los delitos informáticos se concibe en los planos de manera conjunta y concatenada; en el primero se encuentra la información de manera general (información almacenada, tratada y transmitida mediante los sistemas de tratamiento automatizado de datos), y en el segundo plano, los demás bienes afectados a través de este tipo de delitos como son la indemnidad sexual, intimidad, etcétera. respecto de la información deber ser entendido como el contenido de las bases y/o banco de datos o el producto de los procesos informáticos automatizados; por lo tanto se constituye en un bien autónomo de valor económico. Y es la importancia del valor económico de la información lo que ha hecho que se incorpore como bien jurídico tutelado. (…) Por tanto, en este tipo de delitos no se puede establecer a la información como el único bien jurídico afectado, por ser el principal y el más importante; sino a un conjunto de bienes que son afectados, debido a la característica de la conducta típica en esta modalidad delictiva que colisiona con diversos intereses colectivos. en es ese sentido que coincidimos con María Luz Gutiérrez Francés, quien señala que es un delito pluriofensivo, sin perjuicio de que uno de tales bienes este independientemente tutelado por otro tipo penal. (pp. 288-289)

En tal sentido, es importante identificar que en el delito de FRAUDE INFORMATICO regulado en el artículo 8 de la Ley de Delitos Informáticos el bien jurídico preponderante es el del patrimonio, ello atendiendo a su ubicación en el Capítulo V (Delitos Informáticos Contra el Patrimonio) de la Ley 30096. Ahora bien, el *phishing*, conforme se analizó en el capítulo precedente, generalmente vulnera el patrimonio del sujeto pasivo, aunque para ello previamente se hace uso de información

privada. En efecto, la mayor parte de casos que se registran en cuanto al *phishing* consisten en la obtención por parte del *phisher* de información sobre las cuentas bancarias de sus víctimas, con la finalidad de hacer uso de dicha información y extraer el dinero de las cuentas o hacer compras sin autorización.

De esto se entiende que el *phishing* como conducta antijurídica se encuentra íntimamente relacionado con los delitos contra la intimidad y contra el patrimonio. Empezaremos analizando el delito de fraude informático por cuanto resulta necesario determinar si en este tipo penal se podría encuadrar la conducta del *phishing*.

En este aspecto, es importante determinar qué constituye exactamente el bien jurídico protegido, pues si bien se indica que es el patrimonio, no se establece con claridad a qué hace referencia ello. Al respecto, el jurista Pérez López (2019) sostiene lo siguiente:

> El bien jurídico tutelado en el delito de Fraude Informático es el "patrimonio", desde la perspectiva del derecho a la propiedad que tiene el sujeto pasivo respecto a su base de datos informáticos y/o al adecuado funcionamiento de un sistema informático. (…) La identificación del bien jurídico protegido exige tener presente la orientación político-criminal asumida por el legislador y plasmada en la Ley de Delitos Informáticos, referidos a la protección del patrimonio económico, aunque, de acuerdo con Hugo Vizcardo, en doctrina se asume un carácter pluriofensivo de este tipo de ilícitos penales, ya que concomitantemente afectan, aparte del orden económico, el sistema

> informático, la libertad e intimidad personal, la titularidad del derecho intelectual, entre otros bienes jurídicos. (pp. 157-158)

En el mismo sentido Jimenez Herrera (2017) sostiene con acierto sobre el bien jurídico protegido en el delito de fraude informático:

> Para tener conocimiento de cuál sería el bien jurídico protegido por el Capítulo V de la vigente ley de los delitos informáticos, se debe partir, como en tantos otros grupos de delitos, de la rúbrica del mismo que en este caso reza: "Delitos contra el Patrimonio". En efecto, el bien jurídico protegido por este tipo penal va a ser el "patrimonio", aunque también se protegen otros bienes jurídicos, pero esto depende del caso concreto, ya que si el fin de la conducta delictiva es atentar contra los datos informáticos estaríamos ante la lesión de la confidencialidad, integridad y disponibilidad de datos informáticos, y si el atentado es a los sistemas informáticos, pues estaríamos ante la lesión a la confidencialidad, integridad y disponibilidad de los sistemas informáticos. Pero el bien jurídico primordial que va a proteger esta norma penal es el patrimonio. (p. 458)

Un aspecto resaltante de los delitos informáticos, y que ya habíamos delimitado, es que los tipos penales sancionados en la Ley 30096 no tutelan un solo bien jurídico, pues en su mayoría se trata de delitos pluriofensivos, donde más de un bien jurídico tutelado se ve vulnerado. La importancia de esto radica en que permite entender que en un tipo penal se sancionen diversas conductas, pues la complejidad de las interacciones en el mundo de la informática deja lugar a muchas posibilidades en la comisión de

ilícitos, de ahí que sea necesario regular con minuciosidad los tipos penales a fin de que no queden impunes determinadas modalidades de actuar ilícito.

Una vez dicho esto, es necesario indicar que la forma en que se han redactado los tipos penales sancionados en la Ley de Delitos Informáticos (en adelante LDI), dificulta su aplicación, al pretender encuadrarse en un solo tipo penal muchas conductas (verbos rectores) de las cuales algunas se alejan de la intención normativa del legislador. Uno de estos casos es el tipo penal de Fraude Informático, previsto en el artículo 8 de la Ley 30096, la cual textualmente indica:

Artículo 8. Fraude Informático

El que, a través de las tecnologías de la información o de la comunicación, procura para sí o para otro un provecho ilícito en perjuicio de tercero mediante el diseño, introducción, alteración, borrado, supresión, clonación de datos informáticos o cualquier interferencia o manipulación en el funcionamiento de un sistema informático, será reprimido con una pena privativa de libertad no menor de tres ni mayor de ocho años y con sesenta a ciento veinte días multa.

Lo primero que se advierte de la redacción normativa del artículo en análisis es la cantidad de verbos rectores sancionados: *diseñar, introducir, alterar, borrar, suprimir, clonar (datos informáticos) o interferir, manipular (el funcionamiento de un sistema informático).* Se han previsto ocho conductas que se encuadran en el tipo penal, más allá de los demás elementos objetivos del tipo como es el procurar obtener un provecho ilícito en perjuicio de tercero y hacerlo mediante las tecnologías de información o comunicación. Esta técnica legislativa parecería acertada, en función a

la posibilidad de encuadrar una conducta dentro de las muchas posibilidades que ofrece el tipo penal; sin embargo, esto no necesariamente es así.

Villavicencio Terreros (2014) al analizar este tipo penal refiere:

> Este tipo penal (fraude informático) sanciona diversas conductas. entre ellas a diseñar (proyecto o plan), introducir (entrar en un lugar), alterar (estropear, dañar, descomponer), borrar (desvanecer, quitar, hacer que desaparezca algo), suprimir (hacer cesar, hacer desaparecer), clonar (producir clones) datos informáticos o cualquier interferencia, o manipular (operar con las manos o con cualquier instrumento) el funcionamiento de un sistema informático procurando (conseguir o adquirir algo) un beneficio para sí o para otro en perjuicio de tercero; y por la forma como esta estructura (a propósito de la mala redacción que genera mucha confusión al momento de interpretar la figura, y las conductas inadecuadas como "diseñar, introducir, alterar, borrar y suprimir" que no encajan en el delito de fraude informático; estas conductas son propios del delito de daño) se clasifica como un delito de resultado porque no basta cumplir con el tipo penal para que se consuma el delito de fraude informático, sino que además, es necesario que esa acción vaya seguida de un resultado separado de la misma conducta el que consiste en causar un perjuicio a tercero, de otro modo el delito quedaría en tentativa. (p.297)

Por su parte, haciendo un análisis de la conducta típica en el delito de fraude informático, Romeo Casabona (2006) sostiene que:

> Estaremos ante un fraude informático, toda vez que el agente manipule datos informatizados, pero que esta manipulación consista en la incorrecta modificación del resultado de un procesamiento automatizado de datos, mediante la alteración de los datos que se introducen o están ya contenidos en el ordenador en cualquiera de las fases de su procesamiento o tratamiento informático, siempre que sea con ánimo de lucro y en perjuicio de tercero. (p.427)

En doctrina se reconocen diversas conductas que podrían encuadrar dentro de los alcances típicos del delito de fraude informático, las cuales, si bien no son desarrolladas de manera expresa en el artículo 8 de la Ley 30096 (pues como se indicó, la redacción normativa presentra problemas de precisión de los verbos rectores), por medios interpretativos podrían ser subsumidas en dicho tipo penal.

Así, para Solano citado por Jimenez Herrera (2017), el fraude informático puede ser:

- **Data diddiling, o introducción de datos falsos:** es una manipulación de datos de entrada al ordenador con el fin de producir o lograr movimientos falsos en transacciones de una empresa para otorgarle solvencia moral y económica a una persona que no la tiene.
- **Trojan horse o caballo de Troya:** consiste en introducir rutinas en un programa para que actúen en forma distinta a como estaba previsto.
- **Rounding down o la técnica de Salamé:** consiste en introducir al programa unas instrucciones para que remita a una determinada cuenta los céntimos de dinero de muchas cuentas corrientes. Aprovecha las repeticiones automáticas

de los procesos de cómputo. Es una técnica especializada, consistente en que las cantidades de dinero muy pequeñas, se van sacando repetidamente de una cuenta y se transfiere a otra.

- **Superzapping o llave:** llave no autorizada que abre cualquier archivo del ordenador por muy protegido que esté, con el fin de alterar, borrar, copiar, insertar o utilizar en cualquier forma no permitida, datos almacenados en un ordenador.
- **Trap doors o puertas falsas:** consiste en la práctica de introducir interrupciones en la lógica de los programas con el objeto de chequear en medio de procesos complejos, si los resultados intermedios son correctos, producir salidas de control con el mismo fin o guardar resultados intermedios en ciertas áreas para comprobarlos más adelante.
- **Logic bombs o bomas lógicas o cronológicas:** es una especie de bomba de tiempo que debe producir daños posteriormente como si se tratase de un sabotaje, venganza o deseo de perjudicar. Consiste en la introducción de un programa con un conjunto de instrucciones indebidas que van a actuar en una determinada fecha o circunstancias; destruyendo datos del ordenador, distorsionando el funcionamiento del sistema o paralizando el mismo. La bomba lógica se puede usar también como instrumento de extorsión y se puede pedir un rescate a cambio de dar a conocer el lugar en donde se halla.
- **Asyncronous attack o ataques sincrónicos:** basados em la forma de funcionar de los sistemas operativosy sus conexiones con los programas de aplicación a

los que sirven y soportan en su ejecución. Es un fraude de alto conocimiento técnico, difícil de detectar.

- **Scavenging o recogida de información residual:** es el aprovechamiento de información abandonada sin ninguna protección como residuo de un trabajo previamente autorizado. Puede efectuarse físicamente cogiendo papel de desecho de papeleras o electrónicamente, tomando información residual que ha quedado en memorias o soportes magnéticos.
- **Data leakage o divoulgación no autorizada de datos reservados:** es una variedad del espionaje industrial que sustrae información confidencial de una empresa.
- **Pippybacking and impersonation o toma no autorizada de información:** consiste en acceder a áreas restringidas para pillar información de una empresa, aprovechando que el empleado encargado del equipo no está presente.
- **Wiretgapping o pinchado de líneas telefónicas de transmisión de datos:** por medio de una radio, un módem y una impresora, para recuperar la información que circula en ellas.

2.4.ANALISIS DEL TIPO PENAL DE SUPLANTACION DE IDENTIDAD

Este tipo penal guarda estrecha relación con la conducta delictiva del phishing. Es más, algunas de las modalidades más comunes de phishing se podrían encuadrar dentro de este tipo penal. En efecto, Jimenez Herrera (2017) señala:

> La suplantación en línea o también denominada “phishing” o “spoofing”, es una forma de engañar a los usuarios para que revelen información personal o financiera mediante un mensaje de correo electrónico o sitio web fraudulento.

> Normalmente, una estafa por suplantación de identidad empíeza con un mensaje de correo electrónico que parece un comunicado oficial de una fuente de confianza, como un banco, una compañía de tarjeta de crédito o un comerciante en línea reconocido. En el mensaje de correo electrónico se dirige a los destinatarios a un sitio web fraudulento, donde se les pide que proporcionen sus datos personales, como número de cuenta o una contraseña. Después, esta información se usa para el robo de identidad. (p.470)

El citado autor si bien relaciona con acierto la conducta del phishing con el delito de suplantación de identidad, comete el error de circunscribir dicho tipo penal exclusivamente a los supuestos de phishing. Así pues, al desarrollar la tipicidad objetiva de este delito, describe:

> La mayoría de los métodos de phishing utiliza la manipulación en el diseño del correo electrónico para lograr que un enlace parezca una ruta legítima de la organización por la cual se hace pasar el impostor. URLs manipuladas, o el uso de subdominios, son trucos comúnmente usados por phisers, por ejemplo esta URL: http://www.nombredetubanco.com/ejemplo, en la cual el texto mostrado en la pantalla no corresponde con la dirección real a la cual conduce. Otro ejemplo para disfrazar enlaces es el de utilizar direcciones que contengan el carácter arroba: @, para posteriormente preguntar por el nombre de usuario y contraseña (contrario a los estándares). (…) Otros intentos de phishing utilizan comandos en JavaScripts para alterar la barra de direcciones. Esto se hace poniendo una imagen de la URL de la entidad legítima sobre la barra de dircciones, o cerrando la barra de direcciones

> original y abriendo una nueva que contiene la URL ilegítima. (Jimenez, 2017, pp. 472-473)

Lo cierto es, que como se analizó en el capítulo precedente, el phishing como término engloba diversas conductas que tienen una característica en común: apelan al uso de la ingeniería social a través del envío masivo de contenido destinado a engañar a la víctima quien termina posibilitando el acceso a información personal. Dentro de dichas conductas, el tipo de phishing al que hace referencia el autor citado, denominado *deceptive phishing*, es el que podría encuadrarse dentro de los alcances del tipo penal de suplantación de identidad, aunque ello no está exento de problemas de naturaleza jurídica que más adelante discutiremos.

El tipo penal de suplantación de identidad, ubicado en el artículo 9 de la Ley 30096, conforme a su redacción normativa prescribe lo siguiente:

> *"Artículo 9.- Suplantación de identidad*
>
> *El que, mediante las tecnologías de la información o de la comunicación suplanta la identidad de una persona natural o jurídica, siempre que de dicha conducta resulte algún perjuicio, material o moral, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años."*

Resulta relevante mencionar aquí que según se desprende de la propia redacción del tipo penal, el sujeto activo debe suplantar la identidad de una persona (natural o jurídica), lo que implica que se suplanta a una persona existente; esto es importante porque dicha distinción dejaría fuera del ámbito de aplicación del tipo las conductas en que el sujeto activo emplea para el engaño una identidad totalmente falsa, inventada, que no le pertenece a nadie.

Así lo reconoce Perez López (2019) cuando sostiene:

> El agente asume una identificación de otra persona, esta falsedad debe ser idónea y/o apta para engañar a alguien, de manera que la suplantación debe ser realizada a persona real y en principio viva, es decir, cuando se trata de una persona inexistente, este aspecto no podría estar abarcado en el tipo penal, convirtiéndose en una conducta atípica. (p. 169)

Ahora bien, como se indicó en el primer capítulo, existen modalidades como el spear-phishing que consisten en ataques más personalizados en los que el contenido del engaño dirigido a la víctima no necesariamente implica la suplantación de una persona natural o jurídica existente, pues la técnica de ingeniería social podría recaer sobre los gustos o preferencias de la víctima, o sobre sus creencias personales, con lo que no necesariamente el phisher tendría que suplantar a una persona, pues para inducir a la víctima a que revele información confidencial podría valerse de otros medios.

De esta manera se evidencia que el tipo penal de suplantación de identidad según lo dispuesto en el artículo 9 de la Ley de Delitos Informáticos solo tipifica parte de las conductas conocidas como phishing, pero deja vacíos respecto a otras, las cuales además no pueden ser tipificadas dentro de otros tipos penales.

Otro elemento objetivo del tipo lo constituye la existencia de un perjuicio causado, lo que convierte el delito de suplantación de identidad en uno de resultado. Al respecto Villavicencio Terreros (2014) indica:

> Este tipo penal sanciona el hecho se suplantar (ocupar con malas artes el lugar de alguien, defraudándole el derecho, empleo o favor que disfrutaba)

> la identidad de una persona natural o jurídica causando algún perjuicio. Esta figura penal (suplantación de identidad) se clasifica como un delito de resultado porque no basta con realizar la conducta típica el cual es suplantar la identidad, sino que además es necesario que esa acción vaya seguida de un resultado separado de la misma conducta el cual es causar un perjuicio. Por ejemplo. crear perfiles falsos en las redes sociales (correo electrónico, Facebook, twitter) atribuidos a personas naturales y/o jurídicas para engañar y perjudicar a terceros. (p.298)

Pero además, se ha previsto en el tipo penal que el perjuicio además de material puede ser moral. Esto obedece a que, como se indicó precedentemente, el tipo penal in comento pretende abarcar más conductas que solamente el *phishing*; así por ejemplo, se podría configurar este delito cuando un sujeto A crea un perfil falso de Facebook con los datos (nombre, foto, etc) de B para luego publicar contenido que afecte la buena reputación de B.

En este supuesto el perjuicio dista de ser material, pues en este caso el perjuicio causado a la dignidad o estima social de B constituyen lo que en doctrina se conoce como *daño moral* la cual ha sido definida como la "modificación disvaliosa del espíritu en el desenvolvimiento de su capacidad de entender, querer, o sentir, que se traduce en un modo de estar de la persona diferente de aquél en que se hallaba antes del hecho, como consecuencia de éste y anímicamente perjudicial" (Valderrama Moya, 2007, p.185).

Queda claro que la inclusión del perjuicio como elemento objetivo del tipo obedece a la intención del legislador de sancionar un amplio abanico de conductas,

sin que ello signifique penalizar conductas que no revistan relevancia jurídica al ser inocuas para la persona que ve suplantada su identidad; sin embargo, en ocasiones la necesidad de verificar la existencia de perjuicio dificulta las cosas cuando se trata de subsumir correctamente un hecho de phishing en la norma penal.

En el capítulo precedente expusimos que el phishing es una conducta compleja que se ejecuta en varias etapas. Tomemos por ejemplo un típico caso de *deceptive phishing* en la forma de un phishing bancario: primero el *phisher* determina la entidad bancaria a la que va a suplantar, luego diseña la página web falsa que simulará ser la de la entidad bancaria, posteriormente mediante publicidad o spam consigue que la víctima ingrese sus datos personales en la página falsa, y finalmente, con dichos datos retira el dinero de la cuenta de la víctima.

En este sencillo ejemplo no se evidencian mayores complicaciones para subsumir la conducta en el tipo penal analizado, pues el sujeto activo, a través de la suplantación de la identidad de una entidad bancaria (suplantando su portal web) logra causar un perjuicio para la víctima, pues al retirar sus fondos le perjudica patrimonialmente; sin embargo, cuando se introducen más variables, el ejemplo se vuelve mucho más complejo de tipificar conforme observaremos más adelante.

2.5.OTRAS POSIBILIDADES DE TIPIFICACIÓN

2.5.1. FALSEDAD GENÉRICA

Como se ha venido desarrollando, la conducta denominada *phishing* hace uso de técnicas de ingeniería social mediante la masificación que permiten las tecnologías de información para la

obtención de información sensible de parte de la víctima. En tal sentido, el agente apela al uso de información generalmente falsa, lo que podría encuadrarse en un supuesto de falsedad genérica, ello teniendo en cuenta que este delito sanciona a aquel que *comete falsedad simulando, suponiendo, alterando la verdad intencionalmente y con perjuicio de terceros*, lo cual se da en las principalidades modalidades de phishing.

Sin embargo, de la propia redacción del tipo penal de falsedad genérica ya se aprecian dificultades que harían imposible tipificar conductas de phishing en este delito. Primero, debemos indicar que el delito tipificado en el artículo 438 del Código Penal inicia de esta forma: *El que de cualquier otro modo que no este especificado en los en los capítulos precedentes.* Esto es pues, indicador de que se trata de un delito de carácter residual, cuya configuración se encuentra supeditada a que el hecho a subsumir no pueda hacerlo en otros delitos. La subsunción en el tipo penal de falsedad genérica es subsidiaria, no debe haber otro delito en el que se pueda subsumir el hecho.

Y, además, de acuerdo a su ubicación en el Código Penal, el delito de falsedad genérica se encuentra en los delitos contra la Fe Pública, lo que hace que el bien jurídico tutelado en dicho delito sea la fe pública; esto implica que dicho tipo penal no pueda abarcar la totalidad de conductas que engloba el *phishing*, pues como se analizó en el primer capítulo, este delito es pluriofensivo y no vulnera solo un bien jurídico, lo que hace necesaria la creación de un delito específico para sancionar una

conducta tan compleja. Máxime si la pena que regula el delito de falsedad genérica oscila entre los dos y cuatro años de pena privativa de libertad, lo que no guarda un adecuado nivel de proporcionalidad con la reprochabilidad exigida para una conducta lesiva como la del *phishing.*

2.5.2. ESTAFA

El tipo penal de estafa, ubicado en los delitos contra el patrimonio, tiene la siguiente redacción:

"Artículo 196.- Estafa

El que procura para sí o para otro un provecho ilícito en perjuicio de tercero, induciendo o manteniendo en error al agraviado mediante engaño, astucia, ardid u otra forma fraudulenta, será reprimido con pena privativa de libertad no menor de uno ni mayor de seis años".

Este es un delito para cuya configuración se requiere el cumplimiento de una serie de condiciones que se son los elementos objetivos del tipo, lo que además debe hacerse de manera secuencial, tal como han reconocido la doctrina y jurisprudencia.

Salinas Siccha (2013) reconoce que:

> El injusto penal de estafa tiene componentes o elementos particulares que deben aparecer secuencialmente en la conducta desarrollada por el agente. El orden es el siguiente: 1. Engaño, astucia, ardid u otra forma fraudulenta. 2. Inducción a error o

> mantener en él. 3. Perjuicio por disposición patrimonial. 4. Obtención de provecho indebido para sí o para un tercero. (p.1136)

Esto hace que el tipo penal de estafa sea inaplicable para los supuestos que contiene la conducta del *phishing*, ello por cuanto en el *phishing* no se da el supuesto de disposición patrimonial voluntaria. Lo que generalmente obtiene el *phisher* a través del engaño producido en el sujeto pasivo es información, nunca se trata de un acto de disposición patrimonial voluntario, pues a diferencia de los supuestos típicos de estafa en que el sujeto activo induce a error a la víctima para que le confíe parte de su patrimonio, en el phishing el sujeto pasivo no realiza ningún tipo de transferencia de su patrimonio hacia el sujeto activo, sino que le permite acceso a información, la cual puede luego ser usada por el phisher de diferentes maneras, las cuales pueden o no significar un perjuicio patrimonial para la víctima.

2.5.3. HURTO

El tradicional delito de hurto, ubicado en los delitos contra el patrimonio, tiene como elemento objetivo el apoderamiento del bien mueble. Su imposibilidad para aplicarse a los supuestos de *phishing* es evidente toda vez que se trata de un delito cuya configuración se

encuentra supeditada a la existencia del elemento de trascendencia interna denominado ánimo de lucro.

En el Exp. N° 445-98, la Sala Penal de Apelaciones para procesos sumarios con reos libres de la Corte Superior de Justicia de Lima precisó:

> Conforme a su tipicidad objetiva, el tipo penal define el delito de hurto y exige como presupuestos objetivos: la pre-existencia de un bien mueble; que el agente se apodere ilegítimamente de un bien mueble para obtener un provecho; que exista sustracción del bien del lugar donde se encuentre; que dicho bien sea total o parcialmente ajeno; además del elemento subjetivo del dolo, es decir, la conciencia y voluntad de la realización de todos los elementos objetivos y ánimo de lucro.

Asimismo, la Sala Penal de la Corte de Justicia de Lima volvió a aclarar que:

> El ánimo de provecho implica situar la cosa en la esfera de disponibilidad real que haga posible su utilización como si fuera dueño de ella, lo que en autos se encuentra probado, pues los procesados tenían la total disponibilidad del bien mueble, no importando si llegó o no a obtener efectivamente el provecho ni la forma de materialización, pues el tipo descrito en la norma penal no exige que se haya efectivizado el provecho, sino que la finalidad perseguida por el agente sea obtenerlo, entendiéndose que el mismo se cumple desde el momento en que el sujeto activo

del delito tiene la disponibilidad del bien mueble sobre el cual recayó la acción. (Exp. N° 347-2004-Junin del 11-10-2004)

Y, tal como se ha indicado ya con anterioridad, la conducta cometida por el *phisher* no necesariamente sigue un ánimo de lucro, pues debemos recordar que el primer objetivo del phisher no es el patrimonio de la víctima, sino su información sensible, sin perjuicio de que en algunos casos sí se persiga un fin económico, lo que en todo caso tampoco podría configurar un supuesto de hurto, pues en el phishing el apoderamiento del patrimonio de la víctima es una segunda fase, que no implica un desplazamiento físico de un bien mueble de la víctima, sino que un desplazamiento virtual a través de las tecnologías de información.

2.6.PROBLEMÁTICA DEL PHISHING EN EL PERU

El Perú, como todos los demás países del mundo, ha intentado ajustarse al salto de modernidad que impera a nivel global, lo que ha significado un incremento en el tiempo que las personas dedican al uso de las tecnologías de información, desde usos relacionados a trabajo, banca, ocio, entretenimiento, información, educación, entre otros.

Ello, como se advirtió en el primer capítulo, también significa un incremento en las posibilidades de comisión de ilícitos mediante las tecnologías de información y comunicación.

Nuestro país no ha sido ajeno a esto, como se evidencia en un reporte del 13 de julio del 2020 en el diario El Comercio (en su versión virtual), donde se dio a conocer sobre esta modalidad delictiva y las formas de evitarlo:

> Este delito digital se basa en el robo de datos: contraseñas, información privada, claves bancarias y tarjetas de crédito. Los estafadores se hacen pasar por una persona o empresa de confianza y mediante una comunicación, ya sea un mensaje de texto (SMS) o correo electrónico, sustraen información valiosa de los usuarios, que sin darse cuenta han dejado ingresar un virus en sus aparatos electrónicos.
>
> El phishing consiste en que un atacante intenta engañarte para que facilites tu información personal haciéndose pasar por alguien que conoces. Los correos de tipo phishing generalmente contienen enlaces a una página falsa que suplanta la identidad de una empresa o servicio, por lo que si una persona introduce sus datos, inmediatamente esta información estará en manos del estafador.

Esta mención en un diario de amplia difusión obedece a la gran cantidad de casos que se registran en el país, siendo que las posibilidades de ser víctima de phishing se dan al usar redes sociales, navegar en internet, en videojuegos, servicios de streaming, etc.

2.7.EL CASO DEL INTERMEDIARIO O COMPLICE

El *phishing*, como se ha indicado, cuenta con varias fases, de las cuales es importante reconocer al menos dos, una fase en la que el phisher obtiene la

información de la víctima que le va a permitir provocar un perjuicio a ésta, y otra en la cual hace uso de dicha información. En el denominado *phishing bancario* que no es más que otra forma de aplicación del *deceptive phishing*, el *phisher* usualmente se vale de terceros, que pueden o no tener conocimiento de la ilicitud de la conducta, para que sean éstos quienes sean los beneficiados de las transferencias bancarias realizadas en perjuicio de la víctima luego de que se ha obtenido su información bancaria.

Esta situación plantea una serie de dificultades en cuanto a una adecuada tipificación del phishing. Es evidente que la existencia de esta posibilidad (el uso de terceros para concretar el perjuicio a la víctima) implica que en el caso del phishing la consumación solo podrá darse con la materialización de este resultado, pues de otro modo no se podría sancionar la conducta de los terceros. En efecto, en el caso de los terceros, la posibilidad de sancionar su conducta radica en la figura jurídica del partícipe, específicamente en el caso del cómplice primario, pues el aporte que el tercero realizaría sería de tipo esencial para lograr la consumación del hecho.

Ahora bien, como se sabe, la complicidad en nuestro ordenamiento jurídico tiene que darse en la fase ejecutiva y previo a la fase de agotamiento, pues no existe complicidad post-consumativa. Por lo que en una propuesta de tipificación, se debe tomar en cuenta que la consumación del delito estará supeditada a la materialización de un resultado: perjuicio de algún tipo para la víctima.

De otro lado, este tercero no puede ser considerado co-autor, por cuanto no necesariamente tiene un dominio sobre el hecho y muchas veces no tiene siquiera conocimiento exacto de la forma en que se producirá el perjuicio a la víctima,

aunque sí tenga una idea general de que se trata de una conducta ilícita –lo que en todo caso posibilita que se le pueda sancionar a título de dolo eventual, pues la complicidad debe ser dolosa-.

CAPITULO III: FUNDAMENTOS JURIDICOS PARA LA TIPIFICACIÓN DEL PHISHING

3.1.EL PRINCIPIO DE LEGALIDAD

En la concepción moderna del Derecho Penal, se acepta que uno de los principios base de todo ordenamiento jurídico es el de legalidad. Este principio puede ser resumido en el conocido aforismo latín *"nulla crime, nulla poena sine lege"* propuesta por Ansel von Feuerbach, que puede ser entendido como que no puede haber delito, no hay pena, sin ley. Esta garantía individual consiste en exigirle al Estado ley escrita, cierta y previa como presupuestos de la imposición de un castigo.

> El principio de legalidad muestra sus efectos sobre el poder penal limitándolo a lo señalado en la ley, y sobre los ciudadanos, buscando que conozcan, en todo momento, cuáles son las consecuencias jurídicas de su conducta y la manera cómo van a ser aplicadas. En la actualidad, no se acepta un poder absoluto del Estado sobre los particulares. Por esta razón, el principio de legalidad cumple un importante rol de garantía para los ciudadanos y se constituye como un límite formal a la función punitiva estatal, pues le está prohibido imponer penas a conductas que no hayan sido previamente calificadas en la ley como delictivas. (Villavicencio Terreros, 2006, pág. 135)

Este principio es el más importante de nuestro ordenamiento jurídico, y como tal tiene reconocimiento no solo en nuestro Código Penal, cuenta también con reconocimiento constitucional, así lo expresa García Cavero (2012):

> El principio de legalidad está reconocido en el artículo 2 inciso 24 literal d) de la Constitución Política y en el artículo II del Título Preliminar del Código penal. Este principio garantiza la imparcialidad del Estado, en tanto tiene que determinar de manera general y antes de la realización del delito las

características del hecho prohibido y la reacción penal que cabe contra el responsable. (p. 138)

Así, este principio actúa como un límite al poder punitivo del Estado, de manera que se evita la posibilidad de que una persona sea sancionada en base a subjetividades o por criterios antojadizos del juzgador; así, el principio de legalidad funciona como una garantía individual frente a la administración de justicia.

En virtud a este principio, se valida nuestra hipótesis, pues nos especifica que no hay forma de sancionar actualmente la conducta delictiva conocida como phishing, siendo que conforme se analizó en los capítulos precedentes, los tipos penales vigentes en el Código Penal y la Ley 30096 no permiten tipificar adecuadamente el phishing, de manera que esto genera la impunidad de la conducta.

3.1.1. LA RESERVA DE LEY

Conforme sostiene García Cavero (2012), “la llamada reserva de ley establece que solamente por ley se pueden crear delitos y establecer penas. En este sentido, la ley se constituye en la única fuente inmediata del Derecho penal” (p. 143), por lo tanto, en nuestro país, solo con una norma con rango de ley es posible la creación de delitos.

Este principio valida nuestra hipótesis, pues para la tipificación del phishing en nuestro ordenamiento jurídico se hace necesaria la modificación de la Ley 30096, pues solo mediante normas con rango de ley se puede tipificar un delito.

3.1.2. LA TAXATIVIDAD DE LA LEY

Como consecuencia del principio de legalidad, el legislador se encuentra obligado a ser preciso en la redacción de las leyes que crean delitos; así, los tipos penales deben ser lo más preciso posibles, se debe establecer de manera certera cuáles son los presupuestos que configuran una conducta pasible de ser sancionada penalmente. Así, en palabras de Jacobs citado por García Cavero (2012), "para evitar posibles abusos por parte de la Administración de Justicia en un sistema democrático de distribución del poder, es necesario que se excluyan del Derecho penal leyes absolutamente indeterminadas mediante la exigencia de una determinación de la conducta punible y la pena a imponer" (p. 146)

Este principio comprueba nuestra hipótesis, pues en virtud de ello se hace evidente el error en la redacción de los tipos penales vigentes actualmente en la Ley 30096, de manera que su imprecisión al ser un calco del Convenio de Budapest incide en su incapacidad para subsumir la conducta del phishing.

3.1.3. LA PROHIBICION DE LA ANALOGIA

Esta manifestación del principio de legalidad alude a la injerencia que este principio tiene también en la labor interpretativa de los jueces, en la medida que se les impide aplicar la analogía para sancionar una conducta, por muy reprochable que parezca aquella; así, el principio de legalidad actúa también como un límite a la actividad interpretativa de los jueces.

Respecto a la analogía, "puede ser entendida como el proceso por el cual son resueltos los casos no previstos por la ley, extendiéndoles a ellos las disposiciones

previstas para casos semejantes (analogía *legis*) o están deducidos de los principios generales del derecho (analogía *juris*)" (Villavicencio Terreros, 2006, p. 90)

Para explicar este supuesto, García Cavero (2012) indica:

> La ley, como sabemos, tiene un nivel de generalización y deja al juez la tarea de especificar en el caso concreto los elementos del tipo penal. El juez no puede, por tanto, realizar una mayor generalización de los elementos del tipo penal, de manera que amplíe el ámbito de aplicación de la ley penal para un supuesto concreto. Si el juez penal generaliza más los conceptos utilizados por la ley penal con la finalidad de incluir un determinado hecho concreto en el ámbito de regulación de la ley penal, entonces habrá realizado una analogía prohibida por el Derecho penal. (p. 169)

Sin embargo, resulta preciso reconocer que hay un tipo de analogía que sí está permitida en nuestro ordenamiento jurídico, y es la denominada *analogía in bonam partem* según la cual es posible aplicar la analogía cuando la finalidad es eximir o atenuar la pena. Un ejemplo de su aplicación podría ser el siguiente:

> El reconocimiento de un efecto eximente a supuestos equiparables a la fuerza irresistible prevista como causa de exclusión de la responsabilidad penal en el artículo 20 inciso 6 del CP. En efecto, los casos de actos reflejos o de estados de sonambulismo, los ataques de epilepsia o las convulsiones que produzcan la afectación de un bien jurídico deben ser tratados también como causas de exclusión de la responsabilidad penal, ya que, aun cuando no estén expresamente contemplados en el artículo 20 del CP, no hay duda que resultan

completamente equiparables a la fuerza irresistible que sí se encuentra expresamente regulada. (García Cavero, 2012, p. 170)

El subprincipio de prohibición de la analogía valida nuestra hipótesis en la medida que sustenta la necesidad de establecer un nuevo tipo penal para tipificar al phishing, pues permite demostrar que los tipos penales vigentes, con sus deficiencias, son insuficientes para subsumir el phishing, y no hay interpretación que permita adecuar los verbos rectores a los supuestos de phishing, pues ello implicaría analogía *in malam partem* algo que está prohibido de acuerdo a este principio.

3.2.EL PRINCIPIO DE PROTECCION DE BIENES JURÍDICOS

La potestad punitiva del Estado solo debe ser activada ante serias lesiones o amenazas a bienes jurídicos, debiendo entenderse como tales a los intereses y valores sociales más importantes. “Actualmente, toda norma de la parte especial del Código Penal o Leyes especiales deben proteger por lo menos un bien jurídico. De aquí que, para aplicar la sanción penal se requiera necesariamente que se haya lesionado o puesto en peligro un bien jurídico protegido” (Bramont-Arias Torres, 2002, p. 92)

Denominado también principio de lesividad, se encuentra recogido en el Artículo IV del Título Preliminar del Código Penal, y permite orientar el poder punitivo del Estado “hacia finalidades exclusivamente sociales y evita las distorsiones moralistas o el uso de instrumentos violentos para sostener la pura autoridad del Estado” (Villavicencio Terreros, 2006, p. 95).

Además, respecto a los bienes jurídicos, Villavivencio (2006) sostiene que:

Son los valores fundamentales y predominantes de toda sociedad –y no solo de un grupo determinado- que proporciona el ordenamiento de protección de

> Derechos Humanos y los principios constitucionales, como su fuente inspiradora, para de esta manera delimitar (y no solo legitimar) al poder penal, buscando erradicar la posibilidad de la arbitrariedad. (p. 97)

La aplicación de este principio valida nuestra hipótesis, por cuanto corrobora que el tipo penal propuesto debe tutelar un bien jurídico valioso para la sociedad, y en nuestro caso se ha identificar que el phishing es una conducta pluriofensiva, que afecta siempre la confidencialidad de la información, pero que además puede afectar otros bienes jurídicos como el patrimonio y la fe pública.

3.3. PERSPECTIVA TEÓRICA DE LOS TESISTAS

El Perú es un estado democrático de derecho, y como tal, las bases de su ordenamiento jurídico no pueden dejar de lado el principio de legalidad, ello importa un irrestricto respecto a los subprincipios de reserva de ley, taxatividad, irretroactividad y prohibición de la analogía. Por tanto, en nuestro ordenamiento jurídico no se puede sancionar una conducta que no haya sido debidamente tipificada como delito antes de la comisión del hecho.

Esto genera en nuestro país que conductas reprochables no puedan ser perseguidas penalmente, como es el caso del phishing, una conducta que se presenta en diversas modalidades y que puede afectar distintos bienes jurídicos como puede ser el derecho a la intimidad, el patrimonio y la fe pública. Ello por cuanto los tipos penales existentes en el Código Penal y en la ley especial de la materia (Ley 30096 de Delitos Informáticos) son insuficientes para tipificada adecuadamente la conducta, teniendo en cuenta que se trata de tipos penales genéricos que son una copia de lo dispuesto en el Convenio de Budapest y presentan deficiencias que no pueden ser salvadas mediante

interpretación, pues en el derecho penal la interpretación extensiva se encuentra proscrita, así como también la interpretación analógica.

Tomemos por ejemplo el delito de suplantación de identidad, en cuya descripción normativa se establece que será sancionado aquel que "suplante la identidad de una persona natural o jurídica", pero ¿qué sucedería entonces con un supuesto en el cual un delincuente suplante la identidad digital de un *streamer* o de un conocido jugador de *esports* para obtener información confidencial de sus seguidores? Resulta evidente que dicho acto trae un perjuicio, por lo que en aplicación del principio de lesividad, resulta pertinente sancionar dicha conducta mediante un tipo penal.

Además, el principio de legalidad (teniendo en cuenta todas sus manifestaciones) nos obliga a la creación de un tipo penal específico para regular con certeza y precisión todas las situaciones relacionadas al *phishing*, para lo cual primero debe identificarse que en todas las modalidades de *phishing* el delincuente se vale de técnicas de ingeniería social y spam para acceder a la información confidencial de la víctima.

Por lo que, si se pretende crear un tipo penal que sancione el phishing, ello debe incluirse dentro de la redacción normativa, y además debe entenderse que la intimidad y confidencialidad de la información son los bienes jurídicos principalmente afectados.

Asimismo, tal como se sustentó en capítulos anteriores, nuestra posición es que el phishing debe ser tipificado como un delito de mera actividad, pero que pueda agravarse en caso de identificarse la producción de un resultado lesivo para los bienes jurídicos de la víctima, de manera que no queden impunes los supuestos en los que no se logra identificar a la víctima o no se cuenta con la colaboración de aquella.

GLOSARIO DE TÉRMINOS

- **Delito informático:** Hablamos de aquellos casos donde el tipo penal clásico es perfeccionado utilizando a las nuevas tecnologías como medio para su comisión, dotándolo de esa manera de muchos de los inconvenientes o desafíos clásicos de los delitos informáticos, tales como el anonimato, internacionalidad, dificultad en la obtención de evidencia digital, entre otros. (Temperini, 2018, p. 55)
- **Informática:** Jiménez Herrera (2017) la define como "una disciplina de la ciencia que investiga la estructura y propiedad de la información científica, y hace posible el tratamiento automático y racional de la información por medio del ordenador" (p.33).
- **Ingeniería social:** Proceso de la comunicación para engañar a un usuario con una finalidad económica, sacarle dinero o producir lo que se denomina como suplantación de identidad, la obtención de datos personales o institucionales de terceros. (Sain, 2018, p. 11)
- **Mula o mulero:** Se denomina así en la doctrina a aquellas personas que, sin realizar las fases previas del phishing, actúan posibilitando la consumación del hecho, brindando sus cuentas bancarias para la realización de las transferencias que materializan el perjuicio patrimonial para la víctima.
- **Phishing:** Una forma de ingeniería social que se basa en el spam para maliciosamente solicitar información de usuarios de computadora, tales como datos de ingreso o datos de cuentas financieras. (Chandarman y Van Niekerk, 2017, p. 136)
- **Spam:** Correo electrónico masivo no solicitado destinado a transmitir publicidad comercial de forma gratuita o engañar a las personas para que visiten páginas web ilegales o sospechosas. (Rojas Galeano, 2013, p. 50)

III. MATERIALES Y MÉTODOS

3.1.TIPO DE INVESTIGACIÓN

- **Investigación aplicada:** La Investigación Aplicada tiene por objetivo resolver un determinado problema o planteamiento específico, enfocándose en la búsqueda y consolidación del conocimiento para su aplicación y, por ende, para el enriquecimiento del desarrollo cultural y científico. En la presente investigación, se estudió un problema observado en la realidad nacional, el cual fue abordado desde varias perspectivas, luego de lo cual se pudo dar un proyecto de ley que actúe como solución al problema, mediante la tipificación de la conducta denominada phishing como un delito específico en la ley de delitos informáticos.

- **Según naturaleza o profundidad: Descriptiva**. La investigación descriptiva, según Monje Álvarez (2011) señala que: "se propone este tipo de investigación describir de modo sistemático las características de una población, situación o área de interés. (…) busca únicamente describir situaciones o acontecimientos" (p.100). En la presente investigación, se describió la realidad problemática y todos los temas relacionadas al mismo; se describió primero en qué consiste concretamente la conducta denominada phishing, se describieron sus fases y modalidades, asimismo se describió el alcance y limitaciones del los tipos penales existentes en nuestro ordenamiento jurídico, lo cual nos permitió tener un panorama más claro y detallado de cada sub tema y así poder analizar e interpretar la descripción de manera ordenada pudiendo conseguir conclusiones favorables para confirmar que nuestra hipótesis fue acertada.

3.2.MÉTODOS DE INVESTIGACIÓN

3.2.1. MÉTODOS CIENTÍFICOS:

a. Método Inductivo.

En la presente investigación se hará uso del método inductivo, método que es característico de las investigaciones cualitativas.

En la búsqueda cualitativa, en lugar de iniciar con una teoría y luego "voltear" al mundo empírico para confirmar si ésta es apoyada por los datos y resultados, el investigador comienza examinando los hechos en sí y en el proceso desarrolla una teoría coherente para representar lo que observa. Dicho de otra forma, las investigaciones cualitativas se basan más en una lógica y proceso inductivo (explorar y describir, y luego generar perspectivas teóricas). Van de lo particular a lo general. (Hernández, Fernández y Baptista, 2014, p.8).

El método inductivo se dirige de lo particular a lo general, es decir se explora, se observa, se describe y se analiza la realidad para posteriormente desembocar en conclusiones y teorías. Y efectivamente será el método utilizado en la presente investigación puesto que a través del análisis de las investigaciones fiscales del distrito fiscal del Santa en materia de phishing se llegará a la conclusión de que la falta de tipificación de dicha conducta incide en su impunidad.

b. Método comparativo

El método comparativo, aplicable a las investigaciones cualitativas, "permite conocer la totalidad de los hechos y fenómenos de la realidad estableciendo sus semejanzas y diferencias en forma comparativa. Los resultados de las comparaciones

metodológicas nos llevan lógicamente a encontrar la verdad." Este método se usará en la presente investigación para establecer las semejanzas y diferencias que presentan los ordenamientos jurídicos de otros países con el nuestro en la regulación de los delitos informáticos, y específicamente del phishing**.**

3.2.2. MÉTODOS JURÍDICOS

a. Dogmático.

Este método, a decir de Ramos Núñez (2000):

> Se inscribe en el ámbito de pensamiento que ubica al Derecho como una ciencia o técnica formal y, por consiguiente, como una variable independiente de la sociedad, dotada de autosuficiencia metodológica y técnica (…) una tesis de grado que se inspira en el método dogmático visualizará el problema jurídico solo a la luz de las fuentes formales. (p.112)

En ese sentido este método va a permitir que en la presente investigación se pueda recurrir a las fuentes formales del derecho; como doctrina nacional y extranjera, derecho comparado y jurisprudencia acerca del análisis del phishing, si requiere una regulación que permita la sanción de conductas punibles que no se encuentran correctamente reguladas en nuestro ordenamiento jurídico.

b. Hermenéutico.

En la presente investigación se hará uso de este método pues la hermenéutica como método básico del conocimiento científico implica la observación de los hechos o fenómenos de hechos fácticos y su interpretación, para determinar su

significado y sentido (Aranzamendi Ninacondor, 2013); en la presente investigación este método nos es útil, porque el presente estudio versa sobre el phishing, que es un fenómeno social que cobra mayor relevancia en la sociedad conforme a los avances tecnológicos. A través del método interpretativo podremos analizar diversos elementos involucrados en nuestra problemática para proponer la regulación de la conducta en mención.

c. Histórico.

También utilizaremos el método histórico debido a que necesariamente haremos un análisis de la normativa vigente a fin de determinar si se regula o no la conducta delictiva materia de estudio, y para tal fin, se recurrirá al método histórico como medio para entender la voluntad del legislador al redactar la normativa vigente conforme a la Ley de Delitos Informáticos.

d. Interpretación literal

Este método será usado en la investigación para determinar el alcance de algunos de los verbos rectores descritos en los tipos penales de la Ley de Delitos Informáticos, pues se trata de términos que no tienen un significado jurídico específico, siendo menester recurrir a su significado gramatical. De acuerdo con lo señalado por Rubio Correa (2009):

> Para el método literal, el procedimiento de interpretación consiste en averiguar lo que la norma denota mediante el uso de las reglas lingüísticas propias al entendimiento común del lenguaje escrito en el que se halla

> producida la norma, salvo que los términos utilizados tengan algún significado jurídico específico y distinto del común, en cuyo caso habrá que averiguar cuál de los dos significados está utilizando la norma. Es decir, el método literal trabaja con la gramática y el diccionario. (p.238)

e. Ratio legis

Este método consiste en determinar la razón de ser de un texto normativo a partir del texto mismo del cuerpo normativo en el que dicha norma se encuentra. Será usado principalmente al realizar el análisis de los tipos penales que conforman los delitos incluidos en la Ley 30096 Ley de Delitos Informáticos, al tratarse de un cuerpo normativo específico para los delitos informáticos. En efecto, Du Pasquier citado por Donayre Lobo (2014) indica:

> Sucede que el estudio de la letra misma de la ley conduce a resultados dudosos y que haya que recurrir a investigaciones más amplias. Es entonces que se inspirará en el texto, confrontando el artículo en cuestión con otras disposiciones legales, estudiando lo que se denomina “la economía general de la ley”, es decir su plan. El lugar que ocupa un artículo en un documento legislativo, el título y el subtítulo bajo los cuales está ordenado pueden ser determinantes para la apreciación de su alcance. (p.192)

Por lo que, para determinar el alcance de los tipos penales de fraude informático y suplantación de identidad, será relevante analizar su ubicación dentro del cuerpo normativo estructurado al que pertenecen, Ley 30096.

f. Sistemático

El Método de Interpretación Sistemático alude a la idea de que una norma no es un mandato aislado, sino que responde a un sistema jurídico normativo orientado hacia un determinado rumbo en el que, conjuntamente con otras normas, se encuentra vigente; he ahí que, siendo la norma parte de dicho sistema y no siendo posible que desentone o se oponga al mismo, el significado y sentido de la norma jurídica podrá ser obtenido de los principios que inspiran dicho sistema, y dichos principios bien podrían ser deducidos con mayor claridad a partir de las otras normas.

En la presente investigación se usará este método de interpretación al analizar los diversos tipos penales en los que podría subsumirse la conducta del phishing, siendo necesario para ello identificar el sistema normativo al que pertenecen.

3.3.DISEÑO DE LA INVESTIGACIÓN

El diseño de investigación que emplearemos en el presente proceso de investigación será principalmente el Diseño de Investigación de la Teoría Fundamentada, respecto del cual, según señala Hernandez Sampieri (2014): “La teoría fundamentada es un diseño y un producto. El investigador produce una explicación general o teoría respecto a un fenómeno, proceso, acción o interacciones que se aplican a un contexto concreto y desde la perspectiva de diversos participantes” (p.72).

Pero además, atendiendo a la necesidad de brindar una solución al problema identificado, haremos uso también del tipo de diseño propio de las investigaciones

jurídicas denominado Diseño Propositivo; Tantalean Odar (2015) señala respecto a este tipo de diseño que:

> (…) de lo que se trata es de elaborar una propuesta de cambio, adición o supresión de alguna institución o regulación jurídica. Su nombre mismo indica que el investigador se dedica a la construcción de una propuesta que mejore las relaciones sociales a través de la regulación jurídica que se erige. Por tanto, no basta en este tipo de estudios con recomendar la propuesta, sino que es menester generar y argumentar contundentemente sobre la conveniencia de la propuesta elaborada. (p.232)

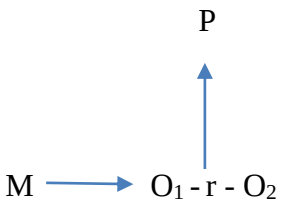
En el mismo sentido, Witker Velásquez (1995) indica respecto a la investigación propositiva: "(…) se trata de cuestionar una ley o institución jurídica vigente para, luego de evaluar sus fallas, proponer cambios o reformas legislativas en concreto, por lo que generalmente estas tesis culminan con una proposición de reforma o nueva ley sobre la materia" (p.11).

Ello se debe a que, a partir de la identificación de las causas que ocasionan el problema materia de investigación, se dotará de una solución, sin someter dicha solución a ninguna prueba de experimentación. Esto es que, se enfocará en explicar cómo es que la falta de una regulación precisa en el ordenamiento jurídico provoca que los casos de phishing en el país no puedan ser objeto de persecución penal y dichos actos ilícitos queden impunes.

Por lo que, frente a dicha problemática, nuestro proyecto de investigación buscará dar solución a dicho fenómeno, y es mediante la propuesta de incorporación

del phishing en la Ley de delitos informáticos –Ley 30096- y que de este modo no siga quedando impune y se permita a los operadores de justicia actuar frente a este fenómeno social con las bases legales que garanticen una efectiva persecución penal.

Por tanto, teniendo en cuenta que los diseños elegidos son de tipo no experimental, ya que no se someterá a ningún sistema de prueba, el esquema del diseño de investigación es el siguiente:



Donde:

M = Muestra 15 fiscales del Distrito Fiscal del Santa

O_1 = Observación de la variable tipificación del phishing en el ordenamiento jurídico peruano

O_2 = Observación de la variable impunidad del phishing en el Perú

r = Correlación entre las variables

P = Propuesta elaborada por los autores del estudio

3.4.UNIVERSO, POBLACIÓN Y MUESTRA

3.4.1. UNIVERSO

Es el conjunto de elementos (personas, objetos, programas, sistemas, sucesos, etc.) globales, finitos e infinitos, a los que pertenece la población y la muestra de estudio en estrecha relación con las variables y el fragmento problemático de la realidad, que es materia de investigación. (Carrasco Díaz, 2005, p.236) Así, teniendo en cuenta nuestras variables y su operacionalización, el universo de nuestra

investigación lo constituyen todos los magistrados que investigan casos penales, que son quienes pueden investigar denuncias por phishing.

3.4.2. POBLACIÓN

"Es el conjunto de todos los elementos (unidad de análisis) que pertenecen al ámbito espacial donde se desarrolla el trabajo de investigación" (Carrasco, 2005, p. 236-237). Es por ello que, la población de la presente investigación la constituyen los fiscales penales de todos los distritos fiscales del país.

3.4.3. MUESTRA

"Es una parte o fragmento representativo de la población, cuyas características esenciales son las de ser objetiva y reflejo fiel de ella, de tal manera que los resultados obtenidos en la muestra puedan generalizarse a todos los elementos que conforman dicha población" (Carrasco Díaz, 2005, p.237).

La muestra que se ha elegido en la presente investigación está constituida por quince magistrados fiscales penales del Distrito Fiscal del Santa. Es así que, esta muestra se eligió en base al tipo de muestra no probabilística intencionada, puesto que, no se utilizó ninguna regla matemática o estadística, sino que se eligió por nuestro propio criterio, teniendo en cuenta que en la muestra intencionada "el investigador procura que la muestra sea lo más representativa posible, para ello es necesario que conozca objetivamente las características de la población que estudia" (Carrasco Díaz, 2005, p.243).

Siendo que como investigadores escogimos esta muestra dado que el distrito fiscal del Santa es un distrito en el cual hemos laborado y conocemos su realidad, por

tanto, tenemos conocimiento de la existencia de investigaciones fiscales relacionadas a hechos de phishing, y además nuestra propia práctica laboral nos permite la comunicación con los magistrados de este distrito. Muestra que nos ayudarán a arribar a la conclusión de que es la falta de una tipificación precisa sobre el phishing lo que ocasiona que los magistrados del país no puedan sancionar a quienes cometen dichos actos, generando que queden impunes. Y por tal motivo, es imperativo modificar la Ley de Delitos Informáticos para incorporar el phishing como un tipo penal independiente.

3.5.TÉCNICAS E INSTRUMENTOS DE RECOLECCIÓN DE DATOS

3.5.1. TÉCNICAS.

a. Fichaje.

Esta técnica permitirá obtener la información necesaria (libros, revistas jurídicas, artículos online) para el desarrollo del marco teórico. “Documento donde el investigador recopila, con criterio selectivo y siguiendo ciertas normas técnicas, toda información sustancial referida a un tema específico, que luego le sirva para la sustentación teórica” (Rojas Cairampoma, 2002, p.29). Esta técnica será utilizada en el presente proyecto a través de la recolección de la información que permitirá almacenar la información (marco teórico y marco conceptual).

b. Encuesta.

“Puntualmente, la encuesta puede definirse como una técnica de investigación social para la indagación, exploración y recolección de datos,

mediante preguntas formuladas directa o indirectamente a los sujetos que constituyen la unidad de análisis del estudio investigativo" (Carrasco Díaz, 2005, p.314). Esta técnica será usada para evaluar la percepción de los magistrados del distrito fiscal del Santa respecto a la actual tipificación de los delitos informáticos, así como su experiencia en la investigación de denuncias por phishing.

3.5.2. INSTRUMENTOS:

a. Fichas bibliográficas.

Utilizada para la localización de la fuente bibliográfica, contienen los datos de identificación de un libro o de algún documento escrito sobre el objeto de estudio.se hacen para todos los libros o artículos que pueden ser útiles a la investigación.

b. Fichas de resumen.

Empleada para realizar las síntesis de las ideas o conceptos básicos que se consideran de mayor importancia para la investigación, se extrae mayormente de un texto extenso. Se consignan mediante nuestras propias palabras, las ideas, datos que nos proporciona el autor.

c. Fichas textuales

Son aquellas que transcriben literalmente o al pie de la letra una parte del contenido de una obra, artículo o trabajo consultado; pueden o no ir entre comillas. Utilizadas en sus dos formas (menos y más de 40 palabras), respetando las normas APA séptima edición 2019.

***d.* Cuestionario.**

Este tipo de instrumento permite la obtención de respuestas directas a través del pliego de preguntas que se le entrega a los miembros encuestados. “Las preguntas para el cuestionario se elaboran en atención a las variables del problema de investigación, así como en estrecha relación con los indicadores e índices que se han derivado de ellas” (Carrasco Díaz, 2005, p.318).

3.5.3. FUENTES PRIMARIAS:

a) Realidad social. A través del incremento de casos de phsihing a través de los años, más ahora en tiempos de pandemia que se han multiplicado las transacciones realizadas online.

b) Observación Indirecta. Los tesistas obtienen información de las noticias nacionales, internacionales, la legislación y doctrina comparada.

3.5.4. FUENTES SECUNDARIAS

a) Documentos.

3.6.TÉCNICAS DE PROCESAMIENTO Y ANÁLISIS DE DATOS

a. ANÁLISIS DE CONTENIDO:

Sobre esta técnica de análisis de contenido, Andréu Abela (2018) indica:

> El análisis de contenido en un sentido amplio, que es como lo vamos a entender en este trabajo, es una técnica de interpretación de textos, ya sean escritos, grabados, pintados, filmados..., u otra forma diferente donde puedan existir toda clase de registros de datos, trascripción de entrevistas, discursos, protocolos de observación, documentos, videos,... el denominador común de todos estos materiales es su capacidad para albergar

> un contenido que leído e interpretado adecuadamente nos abre las puertas al conocimientos de diversos aspectos y fenómenos de la vida social. (p.2)

Esta técnica contribuyó a fortalecer los puntos principales que forman el desarrollo del presente trabajo de investigación; aplicándolo de la siguiente forma: Realizamos acopio de información, respecto al tema del phishing, cómo se da esta conducta, sus modalidades, que bienes jurídicos afecta y su falta de regulación en el sistema jurídico peruano; por lo que recurriremos a diversos medios para obtener la bibliografía necesaria, tales como libros, ensayos, revistas, legislación comparada y doctrina comparada, en modalidad física y virtual.

Consecutivamente a la recolección de la información necesaria, realizamos el estudio y análisis de los mismos, ya que a través de ellos pudimos interpretar los conceptos para conferir coherencia a nuestros temas para orientarlos y explicarlos en función de nuestra problemática, es así que consignamos temas específicos en los capítulos de la presente investigación tales como: El phishing como comportamiento penalmente relevante, el phishing en la legislación peruana, el phishing en el derecho comparado; de los cuales no solo se brinda textualmente la información obtenida (marco teórico) sino la relacionamos para aplicarlo con nuestros objetivos a fin de concebir la elaboración de nuestro proyecto de tipificación del phishing.

Por último, se realizó un análisis, del contenido textual y legal de los temas referentes al phishing como conducta penalmente relevante, las modalidades de phishing, los sujetos intervinientes, el delito de phishing en la legislación, doctrina

nacional y comparada, jurisprudencia nacional e internacional; así como ensayos e investigaciones de alcance internacional.

b. TECNICA DE CORTE Y CLASIFICACIÓN:

Debido a la abundante información que se recabó, teniendo en cuenta las técnicas e instrumentos de recolección de datos que se aplicarán, se requirió el uso de esta técnica de procesamiento, en la cual según Hernández et al. (2014):

> Después de revisar, manejar y marcar el texto, el cortar o editar y clasificar, consiste en identificar expresiones, pasajes o segmentos que parecen importantes para el planteamiento y luego juntarlos conceptualmente (sería como agrupar objetos en el "cajón o pila" que le corresponde: juguetes, artículos de cocina, ropa, etc.). Hay diversas técnicas para ello. La más difundida es el método de comparación constante. Se hace mediante el programa o en un procesador de textos (hace tres décadas se hacía con tarjetas de colores). (p.439)

En tal sentido, dicha técnica nos permitió identificar los diversos conceptos importantes para la comprobación de nuestra hipótesis.

3.7.METODO DE ANALISIS DE DATOS

Para el análisis de los datos que se obtendrán de acuerdo a la aplicación de los instrumentos, se usará el aplicativo SPSS versión 22 para luego ser tabulados y procesados, los mismos que serán presentados a través de tablas y figuras estadísticas.

IV. RESULTADOS Y DISCUSIÓN DE RESULTADOS

RESULTADO N° 01

En el Código Penal existen algunos delitos que guardan relación con la conducta del *phishing*, tales como estafa, falsedad genérica y hurto; sin embargo, un análisis de la tipicidad objetiva de dichos tipos penales permite concluir que son insuficientes para subsumir la complejidad del *phishing.*

DISCUSIÓN DE RESULTADO N° 01

De acuerdo a los bienes jurídicos que afecta la conducta del *phishing* la cual, como recordamos, es pluriofensiva, se puede identificar algunos tipos penales ubicados en el Código Penal, que guardan cierta relación con el *phishing*, al punto que algunos fiscales al tomar conocimiento de un hecho de phishing, pretenden tipificarlos en alguno de los delitos como es hurto, estafa o falsedad genérica, sin embargo dicha calificación no soportaría un control de acusación, debido a la imposibilidad de encuadrar todo el procedimiento del phishing en la redacción normativa de dichos tipos penales.

Así por ejemplo, el hurto se muestra insuficiente para subsumir todas las modalidades de phishing, pues al tratarse de un delito contra el patrimonio, necesariamente exige la presencia del *animus lucrandi*, mientras que en el phishing no siempre el autor busca acceso al patrimonio de la víctima, pues si bien generalmente el phishing se traduce en pérdida patrimonial para la víctima, la primera acción del phisher es acceder a la información de la víctima, no a su patrimonio. Es más, en ocasiones el *phisher* directamente tiene como objetivo la información sensible de la

víctima y no su patrimonio, por lo que el tipo penal de hurto resulta abiertamente insuficiente para tipificar dichos supuestos.

De otro lado, debido a que en las modalidades más conocidas de phishing el procedimiento incluye la participación de la víctima, quien descuidadamente proporciona cierta información que luego recoge el *phisher* o permite la descarga e instalación oculta de *software* malicioso, algunos fiscales y magistrados equiparan el phishing con los supuestos tradicionales de estafa, al considerar que el *phisher* induce a error a la víctima.

La Corte Suprema de Justicia en la Casación N° 421-2015, Arequipa, ha desarrollado los elementos objetivos del tipo penal de estafa, considerando dentro de ellos al desplazamiento patrimonial voluntario: *"Dentro del tipo de estafa debe entenderse por disposición patrimonial a todo comportamiento que realiza el titular del patrimonio, con la mira de cumplir determinados fines, generando que el objeto patrimonial salga de su esfera de dominio introduciéndose ilícitamente en la esfera de dominio del autor del delito. Así, existe una disminución en el patrimonio del sujeto pasivo por su propia voluntad como consecuencia del error en su representación de la realidad producto del engaño."*

Considerando ello, somos de la opinión que resulta imposible subsumir los supuestos fácticos del phishing en la tipicidad objetiva del delito de estafa, conforme a lo regulado en el Código Penal peruano, debido a que en el phishing el sujeto pasivo no realiza ningún tipo de disposición patrimonial, y es que si bien en algunos casos la víctima proporciona información *–como es el caso del deceptive phishing-*, dicha información no es *per se* un desplazamiento patrimonial. Recordemos que en la estafa

el sujeto pasivo tiene la voluntad –*aunque sea viciada*- de entregar su patrimonio al sujeto activo, mientras que en el phishing el sujeto pasivo no tiene voluntad ni conocimiento de que se va a realizar un desplazamiento patrimonial a favor del *phisher* o de un tercero; es el propio *phisher* quien, usando la información extraída del sujeto pasivo, realiza transferencias patrimoniales a su favor o –*generalmente*- de un tercero.

RESULTADO N° 2

Los tipos penales regulados en la Ley 30096, modificada por Ley 30171, son insuficientes para tipificar adecuadamente la conducta del phishing, debido a que se trata de tipos penales que describen conductas genéricas, lo que impide ajustar el procedimiento del phishing a los verbos rectores descritos en los tipos penales de fraude informático y suplantación de identidad descritos en la Ley 30096.

DISCUSIÓN DE RESULTADO N° 02

Este resultado se obtiene del análisis de la Ley Nº 30096 que regula los Delitos Informáticos en el país. En dicho cuerpo normativo se establecen capítulos para dividir los tipos penales según los bienes jurídicos tutelados por cada tipo penal. Así, atendiendo a que el phishing es una conducta pluriofensiva, esto es, afecta más de un bien jurídico, corresponde analizar los delitos regulados en la Ley 30096 que guarden concordancia con los bienes jurídicos principalmente afectados por el phishing, esto es: la intimidad, el patrimonio y la fe pública. La Ley 30096 establece como únicos delitos informáticos relacionados a dichos bienes jurídicos al Fraude Informático y la Suplantación de Identidad.

Respecto al delito de fraude informático, de la redacción normativa advertimos que –además de ser una copia de lo descrito en el Convenio de Budapest- engloba diversos verbos rectores, a saber: *diseño, introducción, alteración, borrado, supresión o clonación (de datos informáticos) y la interferencia, manipulación (del funcionamiento de un sistema informático).*

Guarda cierta lógica que los supuestos tradicionales de phishing bancario sean tipificados por los operadores de justicia en este tipo penal, pues se encuentra ubicado en el título de "Delitos Contra el Patrimonio". Sin embargo, como se sustentó en el Capítulo I, el phishing recurre a técnicas de ingeniería social y el empleo de comunicación masiva –*spam*-, no a las sofisticadas técnicas informáticas que parecen estar reguladas en el tipo penal *in comento*.

La conducta descrita en el fraude informático puede resumirse en la interferencia y manipulación de datos informáticos o sistemas informáticos. El autor Jimenez Herrera (2017), en una posición que compartimos, resume que el fraude informático es "(…) una acción deliberada de manipulación de datos: en la entrada, en el programa o en la salida de datos o de sistemas informáticos" (p.459).

Más adelante, el mismo autor prosigue, citando a Romeo Casabona:

> Estaremos ante un fraude informático, toda vez que el agente manipule datos informatizados, pero que esa manipulación consista en la incorrecta modificación del resultado de un procesamiento automatizado de datos, mediante la alteración de los datos que se introducen o están ya contenidos en el ordenador en cualquiera de las fases de su procesamiento o tratamiento

informático, siempre que sea con ánimo de lucro y en perjuicio de tercero. (Romeo, citado por Jimenez Herrera, 2017, p.461)

Compartimos dicha línea de pensamiento, pues el fraude informático como delito hace referencia a conductas mucho más especializadas, las cuales requieren para su ejecución un elevado nivel de conocimiento informático, pues en este caso el sujeto activo directamente interfiere con el funcionamiento de un sistema informático o los datos que se encuentran informatizados en un computador. En este supuesto delictivo se podrían subsumir las conductas denominadas *data diddiling* (o introducción de datos falsos) que consiste en una manipulación de los datos de entrada al ordenador; *trojan horse* (el comúnmente denominado virus troyano); *superzapping* o llave lógica; *trap doors* o puertas falsas; *logic bombs* o bombas lógicas; *scavenging* o recogida de datos; *wiretgapping* o pinchado de líneas telefónicas de transmisión de datos; etc.

Mientras que el phishing, como se estudió en el Capítulo I, consiste en emplear *spam* para aprovechar la vulnerabilidad psicológica de la víctima, para lo cual se remite el mensaje a multitud de personas con la esperanza de que alguna confíe en el mensaje y permita el acceso a sus datos confidenciales. El phishing como técnica informática no requiere generalmente que el sujeto activo tenga amplios conocimientos informáticos, su peligro radica en la fácil difusión de los mensajes fraudulentos a través del *spam* y actualmente la publicidad.

Por tanto, resulta evidente que el phishing no puede ser subsumido en el tipo penal de fraude informático, de manera que cuando los fiscales califican hechos de phishing dentro de dicho tipo penal se ven limitados al momento de formalizar investigación preparatoria, pues no hay forma de realizar la imputación concreta

determinando cuál ha sido la conducta específica del *phisher* en relación a los verbos rectores previstos en el tipo penal del artículo 8 de la Ley 30096 Fraude Informático, lo que genera que muchas investigaciones sean sobreseídas ante los cuestionamientos de la defensa del procesado. Esto desemboca pues, en un clima de impunidad.

Otro de los delitos previstos en la Ley 30096 es el de Suplantación de Identidad, y como su nombre lo indica, este tipo penal sanciona a aquel que suplanta la identidad de una persona natural o jurídica, siempre que de dicha conducta resulte algún perjuicio.

A nuestra consideración, algunas modalidades de phishing podrían subsumirse en este tipo penal, e incluso el denominado phishing bancario estaría mejor calificado en este tipo penal que en el de fraude informático; sin embargo, el tipo penal no está exento de deficiencias.

El autor Jimenez Herrera (2017), sostiene sobre este tipo penal: La suplantación de identidad en línea, o también denominado *phishing* o *spoofing*, es una forma de engañar a los usuarios para que revelen información personal o financiera mediante un mensaje de correo electrónico o sitio web fraudulento.

Discrepamos con el autor en la medida de que equipara el delito de suplantación de identidad exclusivamente con el *phishing* y el *spoofing*. El phishing es una conducta diversa y cambiante. Si bien es cierto, algunas modalidades de phishing podrían encuadrarse en este tipo penal, existen otras modalidades para las cuales el tipo penal resulta insuficiente, como es el caso del spear-phishing.

Y es que la principal deficiencia de este tipo penal radica en que, requiere para su configuración que el sujeto activo necesariamente suplante la identidad de una persona natural o jurídica, esto es, el agente se vale de una identidad ya existente, por lo que en el caso que el *phisher* se limite a crear una identidad falsa, su conducta sería atípica y por lo tanto impune.

En efecto, según la Real Academia de la Lengua Española, el verbo suplantar significa: ocupar con malas artes el lugar de alguien, defraudándole el derecho, empleo o favor que disfrutaba; donde lo relevante es que la acción de suplantar implica la existencia de otra persona que es la que viene a ser suplantada, por lo que no se podría suplantar a alguien que no existe, y así, la creación de una identidad falsa no se puede considerar suplantación.

Otro supuesto que no podría subsumir el tipo penal radica en la modalidad conocida como spear-pishing, en la cual el sujeto activo realiza un "ataque" mucho más personalizado, basado en las preferencias, gustos, creencias o información personal de la que disponga de la víctima; en este tipo de phishing el sujeto activo no necesariamente suplanta la identidad de otra persona, se limita a hacer creer a la víctima que puede obtener algo que desea y a partir de ello elabora el engaño para obtener la información que necesita de la víctima. Nuevamente, esta conducta resultaría atípica.

Por lo que, a todas luces el tipo penal de suplantación de identidad resulta insuficiente para subsumir todas las modalidades de phishing.

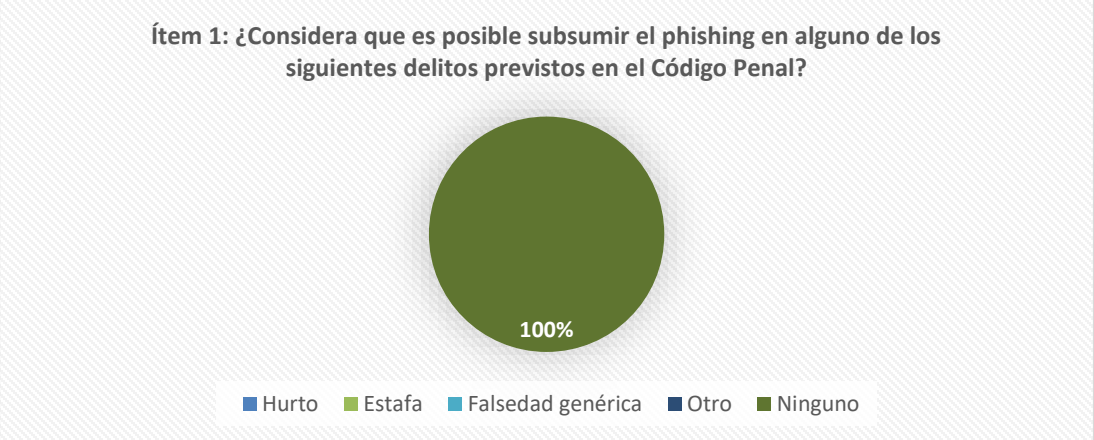
RESULTADO N° 03

En el Distrito Fiscal del Santa, los fiscales experimentan serias dificultades para tipificar adecuadamente los hechos de phishing que se denuncian, trayendo como consecuencia que casi ningún caso supere la etapa de investigación preliminar, y los pocos casos que llegan a ser formalizados, terminan por ser sobreseídos debido a la imposibilidad de fundamentar un requerimiento acusatorio por no existir un tipo penal adecuado para subsumir el hecho.

DISCUSIÓN DE RESULTADO N° 03

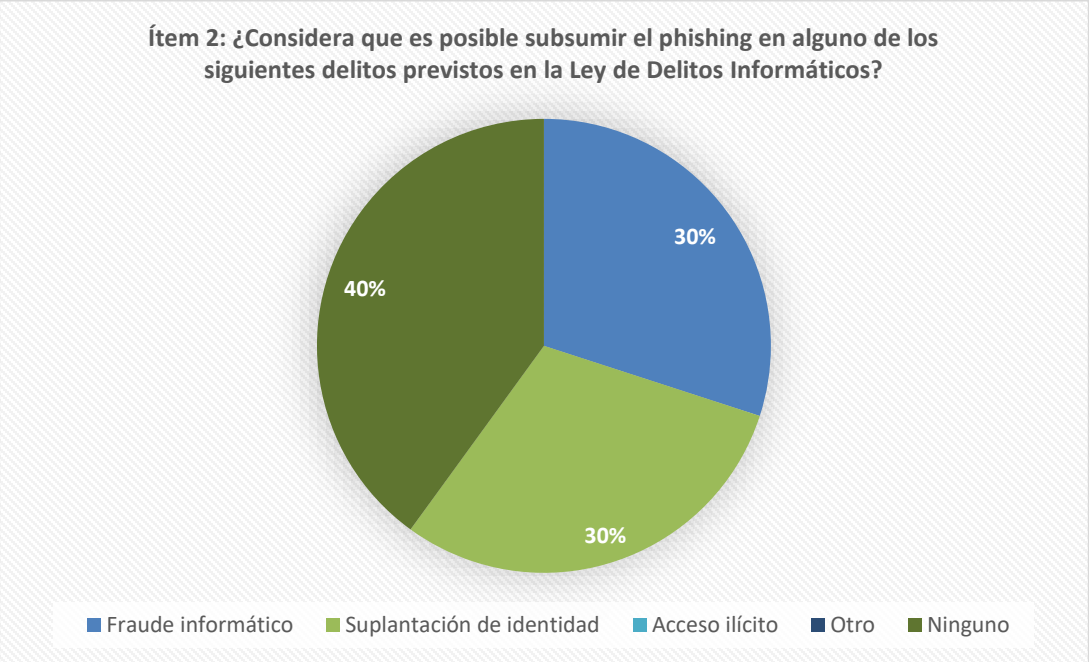
Este resultado se obtuvo a partir del análisis de las respuestas brindadas por distintos magistrados del Distrito Fiscal del Santa a la encuesta presentada por los autores en relación al phishing en la práctica fiscal. Ello se concluye a partir de las respuestas brindadas por los encuestados quienes fueron 20 magistrados del Distrito Fiscal del Santa.

Por ejemplo, a la pregunta de si consideraban posible subsumir el phishing como conducta en alguno de los tipos penales regulados en el Código Penal, se obtuvieron los siguientes resultados:



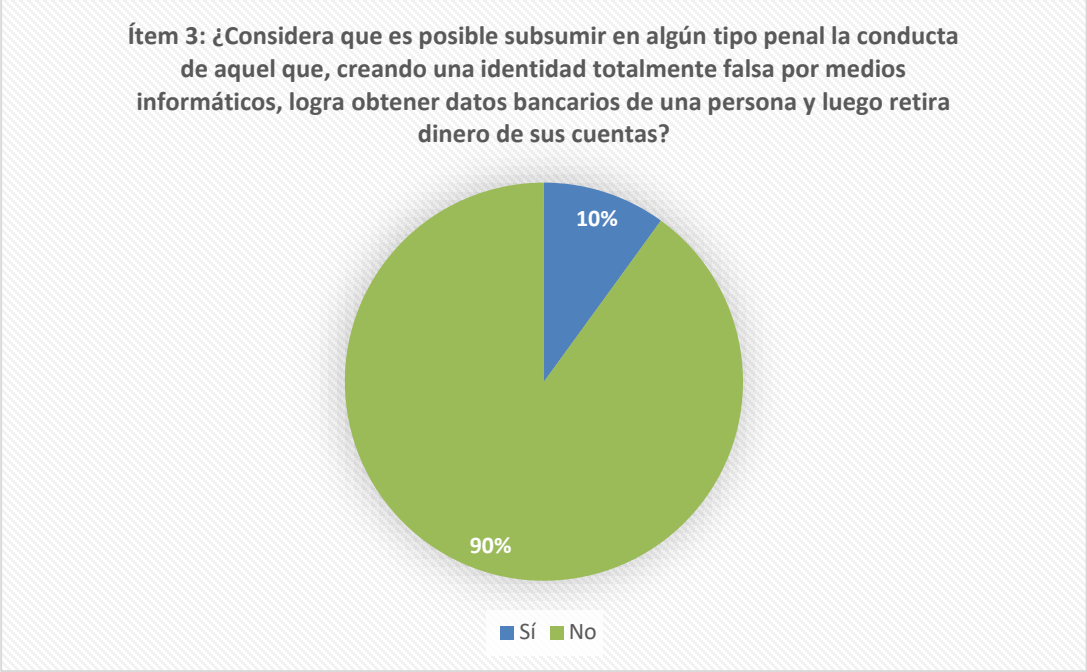
Ello permite concluir que la totalidad de los encuestados considera imposible subsumir el phishing en algún delito del Código Penal.

En cuanto al segundo ítem del cuestionario, se obtuvieron los siguientes resultados:



Y podemos observar que si bien algunos magistrados consideraron que era posible calificar los hechos de phishing dentro de los tipos penales de Fraude Informático o Suplantación de Identidad, una gran parte de los magistrados encuestados consideran que el phishing no puede ser calificado en ninguno de los tipos penales previstos en la Ley de Delitos Informáticos, por lo que se advierte que no existe un criterio uniforme en cuanto al tratamiento que se debe dar al phishing.

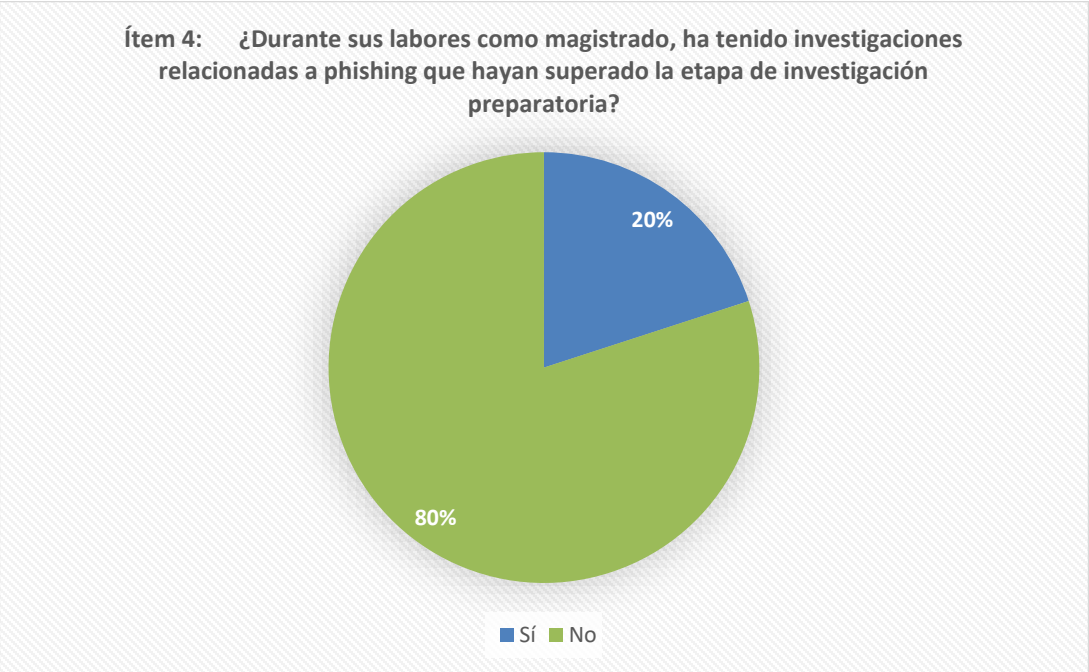
Respecto al tercer ítem del cuestionario, se obtuvieron los siguientes datos:



Esta pregunta fue de gran importancia en el cuestionario, pues se planteó un supuesto correspondiente a un tipo de phishing denominado spear-phishing, una modalidad que a nuestro entender no se puede tipificar en ninguno de los tipos penales existentes. Y de los resultados se advierte que el 90% de los encuestados consideraron que hay un vacío legal en relación al supuesto fáctico planteado. Los tesistas compartimos la idea de que algunos supuestos de phishing podrían –con esfuerzo- ser encuadrados en el tipo penal previsto en el artículo 9 de la Ley de Delitos Informáticos - suplantación de identidad, sin embargo, dicho tipo penal tiene algunas limitaciones que lo vuelven imposible de aplicar para otros supuestos, para los cuales no hay una forma adecuada de tipificación actualmente.

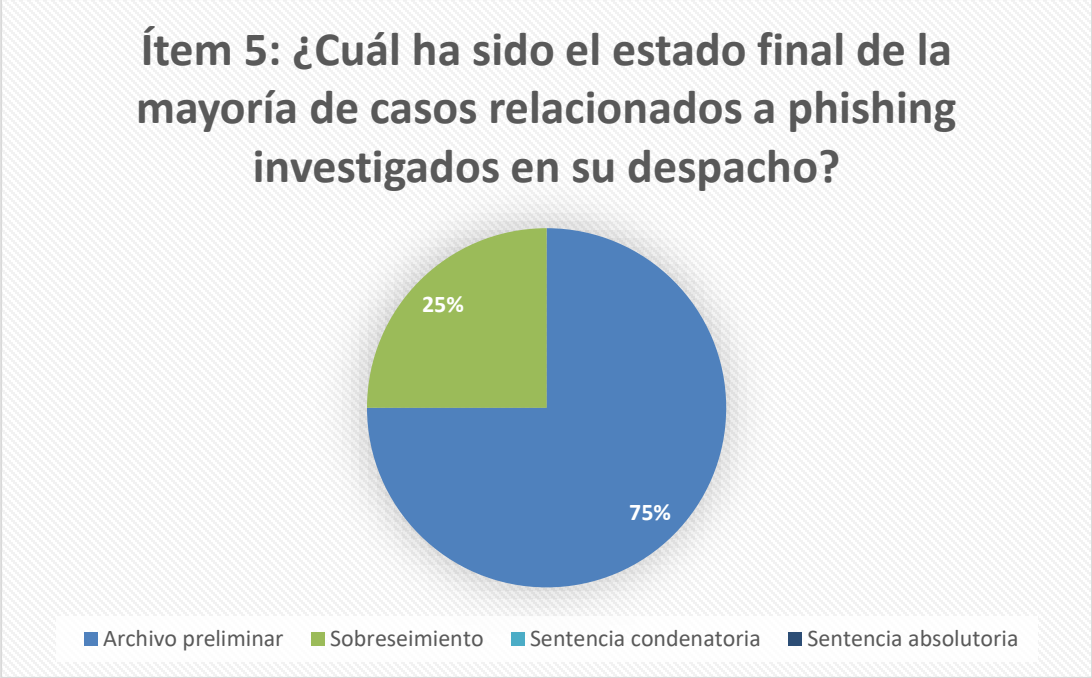
Y a nuestro entender, lo adecuado sería crear un tipo penal que englobe todas las conductas relacionadas al phishing, partiendo del punto en común para todas sus modalidades, esto es, el uso de técnicas de ingeniería social y la masividad que permite la informática.

En relación al cuarto ítem del cuestionario se obtuvo lo siguiente:



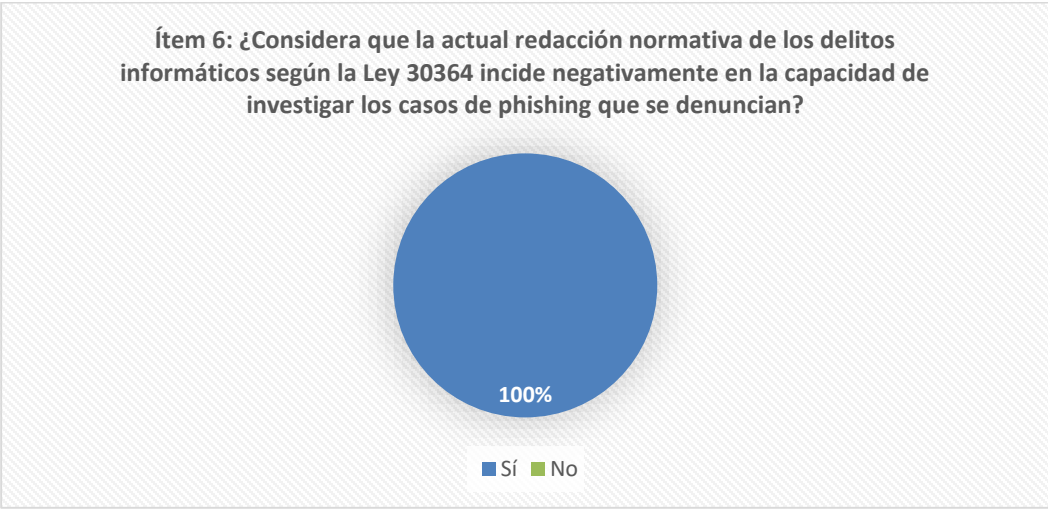
Estos resultados muestran que solo el 20% de los magistrados encuestados tuvo investigaciones que hayan superado la etapa de investigación preparatoria, ello evidencia que la gran mayoría de investigaciones relacionadas a phishing son archivadas en la etapa de investigación preliminar.

Sobre las respuestas al ítem cinco del cuestionario se pudo obtener como resultados lo siguiente:



Los resultados a esta pregunta son esclaredores, pues la gran mayoría de casos relacionados a phishing, de acuerdo a los magistrados encuestados, tienen como resultado el archivo a nivel de investigación preliminar o el sobreseimiento, de manera que son pocos o ninguno los casos que llegan a juicio.

Y, en cuanto al ítem sexto del cuestionario se obtuvieron los siguientes resultados:



Estos resultados muestran que la totalidad de los encuestados considera deficiente la redacción normativa de los delitos previstos en la Ley 30364, y que ello tiene repercusiones en la forma en que se investigan los casos de phishing.

RESULTADO N° 04

Ninguno de los tipos penales vigentes en el país es suficiente para sancionar adecuadamente el phishing, por lo que en atención al principio de legalidad, corresponde la creación de un tipo penal que regule la conducta, a fin de evitar su impunidad.

DISCUSION DE RESULTADO N° 4

El phishing es una conducta compleja, y el principal problema de los tipos penales vigentes en la actualidad, radica en que no abordan de manera específica el phishing, sino que pretenden subsumir una variedad de conductas a la vez como si nombrar verbos genéricos fuera la solución a la complejidad de los delitos informáticos.

Pese a la existencia de una Ley Especial para regular los delitos informáticos, la misma ha demostrado ser insuficiente, llevando a la impunidad muchos casos, por su falta de claridad en la redacción de los tipos penales y su escasa falta de dinamismo: recordemos que los tipos penales recogidos en la Ley 30096 no son más que una copia de los enunciados enumerados en el Convenio de Budapest, sin que se haya hecho el mínimo esfuerzo por adecuar los lineamientos del convenio a la realidad y actualidad peruana.

Esto resulta en un conjunto de dispositivos normativos ineficaces y de difícil aplicación. Tomemos el caso del delito de Fraude Informático, contiene al menos 8 verbos rectores, pero ninguno se haya debidamente detallado en su aplicación, ello conlleva a que tampoco se haya producido una interpretación de dicho delito vía jurisprudencia. En efecto, la ausencia de jurisprudencia en materia de delitos informáticos es preocupante y no hace más que evidenciar el problema: no se están aplicando condenas en base a los tipos penales regulados en la Ley de Delitos Informáticos, ello se corrobora con la falta de sentencias a nivel de Corte Superior o Corte Suprema en materia de delitos informáticos, según la página web del Poder Judicial de Jurisprudencia Nacional Sistematizada, donde ni siquiera es posible realizar una búsqueda en base a los delitos tipificados en la Ley 30096.

Sin embargo, esta falta de sentencias en materia de delitos informáticos –y más específicamente phishing- en la jurisprudencia peruana, no es más que una consecuencia natural ante la ausencia de un tipo penal que regule con exactitud el phishing, pues recordemos que en el derecho penal existe el principio de legalidad, en virtud del cual no se puede sancionar a alguien si la conducta no estuvo tipificada como delito previamente.

V. CONCLUSIONES

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.

VI. RECOMENDACIONES

1. Se recomienda la capacitación de los operadores de justicia a fin de que puedan identificar con exactitud cuándo nos encontramos frente a una situación fáctica que amerita ser tipificada como un delito informático.

2. Se recomienda la creación de un tipo penal específico para tipificar la conducta del phishing, en el cual se deberá dar relevancia al derecho a la intimidad y la confidencialidad de la información personal como bien jurídico afectado. Además, dicho tipo penal deberá estar recogido en la Ley de Delitos Informáticos, atendiendo a que se trata de una acción cometida usando medios informáticos.

3. Se recomienda a los órganos jurisdiccionales (Cortes Superiores y Corte Suprema) definir con exactitud, mediante la emisión de jurisprudencia uniforme, cuáles son las modalidades típicas de cada uno de los tipos penales regulados en la Ley de Delitos Informáticos, a fin de desarrollar y complementar la falta de claridad de los tipos penales allí regulados.

4. Se recomienda la incorporación del tipo penal de *"Obtención fraudulenta de información confidencial"* dentro del Capítulo destinado a los delitos informáticos contra la intimidad en la Ley 30096 – Ley de Delitos Informáticos, a fin de que se sancione adecuadamente el phishing en algunas modalidades que actualmente son atípicas.

VII. REFERENCIAS BIBIBLIOGRÁFICAS Y VIRTUALES

7.1.LIBROS FISICOS

Aranzamendi Ninacondor, L. (2013). *Instructivo teórico-práctico del diseño y redacción de la Tesis en Derecho*. Editora y Librería Jurídica Grijley.

Bramont-Arias Torres, L (2002). *Manual de Derecho Penal Parte General*. (2ª ed). Editorial y Distribuidora de Libros S.A.

Carrasco Diaz, S (2005). *Metodología De La Investigación Científica*. Editorial San Marcos.

Fernández Fernández, C. y Ortega Chacón, D. (2009). *Metodología y técnicas de la investigación jurídica*. Universidad Privada Antenor Orrego.

García Cavero, P. (2012). *Derecho Penal Parte General.* (2ª ed). Jurista Editores EIRL.

Hernández Sampieri, R., Fernández Collado, C., y Baptista Lucio, M. (2014). *Metodología De La Investigación*. (6ta ed.). INTERAMERICANA EDITORES, S.A. DE C.V.

Jiménez Herrera, J. (2017). *Manual de derecho penal informático.* (1ª ed). Jurista Editores EIRL.

Noguera Ramos, I. (2014). *Guía para elaborar una tesis de derecho.* Editora y Librería Jurídica Grijley.

Perez López, J. (2019). *Delitos regulados en leyes penales especiales*. (1ª ed.). Gaceta Jurídica.

Ramos Núñez, C. (2007). *Cómo hacer una Tesis de Derecho y no Envejecer en el Intento*. (4ª ed.). Gaceta Jurídica.

Ricardo Altmark, D. y Molina Quiroga, E. (2012). *Tratado de derecho informático*. (1ª ed., Tomo I.). La Ley.

Rojas Cairampoma, M. (2002). *Manual de Investigación y Redacción Científica*. Book Xx press.

Rubio Correa, M. (2009). *El sistema jurídico. Introducción al derecho.* (10ª ed.). Lima, Perú: Fondo Editorial.

Sain, G. (2018). *La estrategia gubernamental frente al cibercrimen: la importancia de las políticas preventivas más allá de la solución penal. En R. Parada & J. Errecaborde, CIBERCRIMEN Y DELITOS INFORMÁTICOS. Los nuevos tipos penales en la era de internet.* (1ª ed.). ERREIUS.

Saldaña Martínez, M. (2018). *Algunas cuestiones sobre delitos informáticos en el ámbito financiero y económico. Implicancias y consecuencias en materia penal y responsabilidad civil. En R. Parada & J. Errecaborde, CIBERCRIMEN Y DELITOS INFORMÁTICOS. Los nuevos tipos penales en la era de internet*. (1ra ed.). ERREIUS.

Salinas Siccha, R. (2013). *Derecho Penal Parte Especial.* Editora y Librería Jurídica Grijley.

Solís Espinoza, A. (2001). *Metodología de la Investigación Jurídica Social.* Editores B y B.

Temperini, M. (2018). *Delitos informáticos y cibercrimen: alcances, conceptos y características. En R. Parada & J. Errecaborde, CIBERCRIMEN Y DELITOS INFORMÁTICOS. Los nuevos tipos penales en la era de internet*. (1ª ed.). ERREIUS.

Thomas, F., Böhm, C., y Romero, J. (2006). *Nuevos caminos y conceptos en la psicología jurídica*. Lit Verlag.

Valderrama Moya, K. (2007). *Fundamentos para la cuantificación del daño moral*. REVISTA ESDEN, Agosto/Octubre, Año 1, Nro. 2.

Villavicencio Terreros, F. (2006). *Derecho Penal Parte General*. Editora y Librería Jurídica Grijley.

Villa Stein, J. (2008). *Derecho Penal Parte General*. (3ª ed). Editora y Librería Jurídica Grijley.

Witker Velásquez, J. (1995). *La investigación jurídica*. McGraw-Hill.

7.2.LIBROS VIRTUALES

AndaluciaCERT (2017). *Informe de divulgación Phishing*. [Informe]. https://www.andaluciaesdigital.es/documents/410971/1437699/phising+2017/01950ce7-731f-48a6-821a-79388e571bff?version=1.0

Andréu Abela, J. (2018). *Las técnicas de Análisis de Contenido: Una revisión actualizada*. [Monografía]. http://mastor.cl/blog/wp-content/uploads/2018/02/Andreu.-analisis-de-contenido.-34-pags-pdf.pdf

Belisario Mendez, A. (2014). *Análisis de Métodos de Ataques de Phishing*. [Tesis]. http://bibliotecadigital.econ.uba.ar/download/tpos/1502-0840_BelisarioMendezAN.pdf

Camara Peruana de Comercio Electrónico. (2021) *Reporte oficial de la industria ECOMMERCE EN PERU*. [Informe]. CAPECE. https://www.capece.org.pe/observatorio-ecommerce/

Chandarman, R. y Van Niekerk, B. (2017). *Students' cybersecurity awareness at a private tertiary educational institution [Conciencia de los estudiantes sobre ciberseguridad en una institución educativa terciaria privada]*. *African Journal of Information and Communication*. http://www.scielo.org.za/scielo.php?script=sci_arttext&pid=S2077-72132017000100007&lang=en

Código Penal Colombiano [CPC]. Ley 599 de 2000. 16 de setiembre del 2020 (Colombia). https://leyes.co/codigo_penal.htm

Donayre Lobo, G. (2014). La interpretación jurídica: propuestas para su aplicación en el derecho tributario. *Derecho y Sociedad*, *2*(43), 183-206. http://revistas.pucp.edu.pe/index.php/derechoysociedad/article/view/12569

Díaz Gómez, A. (2010). *El delito informático, su problemática y la cooperación internacional como paradigma de su solución: El Convenio de Budapest*. REDUR, (8), 169-203. https://www.unirioja.es/dptos/dd/redur/numero8/diaz.pdf

Gabaldon, L. y Pereira, W. (2008). *Usurpación de identidad y certificación digital: propuestas para el control del fraude electrónico. Sociologías*, (20), 164-190. http://www.scielo.br/scielo.php?script=sci_arttext&pid=S1517-45222008000200008& lang=en

Gonzales Juarez, D. y Peña Enriquez, J. (2012). *Estudio del impacto de la ingeniería social – phishing* [Tesis de pregrado, Universidad Nacional Autónoma de México]. https://repositorio.unam.mx/contenidos/estudio-de-impacto-de-la ingenieria-social-phishing 3506472?c=BJbD08&d=false&q=*:*&i=3&v=1&t=search_0&as=0

Hancco Zapana, E. (2017). *La tipificación del bien jurídico protegido en la estructura del tipo penal informático como causas de su deficiente regulación en la Ley 30096, Perú - 2017* [Tesis de pregrado, Universidad Nacional de San Agustín de Arequipa]. http://repositorio.unsa.edu.pe/handle/UNSA/6436

Herrera Calderon, E. (2016). *El Phishing como Delito Informático y su Falta de Tipificación en el Código Orgánico Integral Penal* [Tesis de pregrado, Universidad Central de Ecuador]. http://www.dspace.uce.edu.ec/handle/25000/8132

JWigodski. (14 de julio de 2010). Metodología de la Investigación. *Población y muestra*. http://metodologiaeninvestigacion.blogspot.com/2010/07/poblacion-y-muestra.html

Mariana Leguizamon, M.S. (2015). *El phishing.* [Tesis de pregrado, Universidad Jaume I – Castellón de la Plana]. http://repositori.uji.es/xmlui/bitstream/handle/10234/127507/TFG_Leguizam %C3%B3n_Mayra. pdf?sequence=1

Microsoft. (setiembre de 2020). *Microsoft Digital Defense Report.* https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWxPuf

Menchaca, M. (2014). *Derecho Informático*. https://www.scribd.com/document/384235685/Derecho-Informatico-Marcelo-Menchaca

Ministerio Público (2019). *Boletín Estadístico del Ministerio Público.* https://agenciafiscal.pe/Storage/modsnw/pdf/12055-k1Nl6Ag7Le1Bg4B.pdf

Ministerio Público (2020). *Anuario estadístico del Ministerio Público,* https://cdn.www.gob.pe/uploads/document/file/1895323/ANUARIO%202020%20FINAL%203.pdf.pdf

Miró Linares, F. (2013). La respuesta penal al ciberfraude. Especial atención a la responsabilidad de los muleros del phishing. *Revista electrónica de ciencia penal y criminología*, *1*(15), 43-44. https://dialnet.unirioja.es/servlet/articulo?codigo=4407809

Monje Álvarez, C. (2011). *Metodología de la Investigación Cuantitativa y Cualitativa:Guía Didáctica*. https://www.uv.mx/rmipe/files/2017/02/Guia-didactica-metodologia-de-la-investigacion.pdf

Moron Lerma, E. y Rodríguez, M (2002). Traducción y breve comentario del Convenio sobre Cibercriminalidad. *Revista de derecho y proceso penal*. https://dialnet.unirioja.es/servlet/articulo?codigo=272446

Oxman, N. (2013). *Estafas informáticas a través de Internet: acerca de la imputación penal del "phishing" y el "pharming"*. Revista de Derecho de la Pontificia Universidad Católica de Valparaíso, *1*(41), 211-262.

https://scielo.conicyt.cl/scielo.php?script=sci_arttext&pid=S0718-68512013000200007&lang=en

Pardo Vargas, A. (2018). *Tratamiento jurídico penal de los delitos informáticos contra el patrimonio*, Distrito Judicial de Lima, 2018 [Tesis de Maestría, Universidad Cesar Vallejo]. http://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/20372/Pardo_VA.pdf?sequence=1&isAllowed=y

Paus, L (2015). *5 tipos de phishing en los que no debes caer.* [Ensayo]. https://www.welivesecurity.com/la-es/2015/05/08/5-tipos-de-phishing/

Puentes Beainny, D. (2019). *El delito de la suplantación de páginas web para capturar datos personales y el hurto por medios informáticos: necesidad y distinción.*[Monografía].https://repository.usta.edu.co/bitstream/handle/11634/19286/2019davidpuentes.pdf?sequence=13

Rodríguez Caro M. (30 de octubre de 2015). Estafa informática. El denominado phishing y la conducta del "mulero bancario": categorización y doctrina de la Segunda Sala del Tribunal Supremo. *Noticias Jurídicas.* http://noticias.juridicas.com/conocimiento/articulos-doctrinales/10617-estafa-informatica-el-denominado-phishing-y-la-conducta-del-ldquo%3Bmulero/

Romeo Casabona, M. (2006). El cibercrimen. Nuevos retos jurídico-penales, nuevas respuestas político-criminales. *Revista de derecho y proceso penal.* https://dialnet.unirioja.es/servlet/libro?codigo=571090

Rojas Galeano, S. (2013). *Revealing non-alphabetical guises of spam-trigger vocables* [Reconocimiento de variantes enmascaradas de vocablos desencadenadores de correo indeseado]. DYNA, *3*(80), 50-51. http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0012-73532013000600006& lang=en

Sánchez Bernal, J. (2009). *El bien jurídico protegido en el delito de estafa informática, en Cuadernos del Tomás N° 1*. [Monografía]. https://dialnet.unirioja.es/servlet/ articulo?codigo=3760666

Sánchez, C. (27 de enero de 2020). *Citar Libro – Referencia Bibliográfica*. Normas APA (7ma edición). https://normas-apa.org/referencias/citar-libro/

Tantaleán Odar, R. (2015). El alcance de las investigaciones jurídicas, en AVANCES. *Revista de investigación jurídica, 3*(10), 11. http://mail.upagu.edu.pe/files_ojs/journals/6/articles/133/submission/copyedit/133-13-458-1-9-20151124.pdf

Valle Matute, J. (2013). *El delito informático de phishing* [Tesis de maestría, Universidad Regional Autónoma de los Andes]. http://dspace.uniandes.edu.ec/handle/ 123456789/2819

Vega Aguilar, J. (2010). *Los delitos informáticos en el Código Penal* [Tesis de maestría, Universidad Católica de Santa María]. http://tesis.ucsm.edu.pe/repositorio/bitstream/handle/UCSM/6824/88.0774.MG.pdf?sequence=1&isAllowed=y

Villavicencio Terreros, F. (2014). *Delitos informáticos.* IUS ET VERITAS, (49), 284-304. http://revistas.pucp.edu.pe › index.php › iusetveritas › article › download.

Zabala, A. (2017). *Responsabilidad bancaria frente al delito de phishing en Colombia*. [Monografía]. https://repository.ucatolica.edu.co/bitstream/10983/14943/1/Art%C3%ADculo%20 Phishing%20-%20Alexander%20Zabala.pdf

Zapata, F. (2000). *¿Qué son la Población y la Muestra de una Investigación?*: https://www.lifeder.com/poblacion-muestra/

Zorrilla Tocto, K. (2018). *Inconsistencias y ambigüedades en la ley de delitos informáticos Ley Nº 30096 y su modificatoria Ley Nº 30171, que imposibilitan su eficaz cumplimiento* [Tesis de Maestría, Universidad Nacional de Ancash Santiago Antúnez de Mayolo – Huaraz]. http://repositorio.unasam.edu.pe/handle/UNASAM/2332

7.3. NOTICIAS

Kaspersky Latam. (2018). *Panorama de amenazas. Phishing.* https://latam.kaspersky.com/about/press-releases/2018_panorama-de-amenazas-phishing

Redacción Gestión. (2021). *Phishing, el ciberataque que más se incrementó en el país por pandemia.* https://gestion.pe/tecnologia/phishing-el-ciberataque-que-mas-se-incremento-en-el-pais-debido-a-pandemia-noticia/

VIII. ANEXOS

ANEXO 01: PROPUESTA DE LEY

"AÑO DE UNIVERSALIZACIÓN DE LA SALUD"

PROYECTO LEY Nº …….

PROYECTO DE LEY DE INCORPORACIÓN DEL ARTÍCULO 7-A A LA LEY DE DELITOS INFORMÁTICOS LEY 30096, PARA IMPLEMENTAR EL DELITO DE ATENTADO CONTRA LOS DATOS PERSONALES MEDIANTE TECNICAS DE INGENIERIA SOCIAL

Los bachilleres de la Escuela Académica Profesional Derecho y Ciencias Políticas de la Universidad Nacional Del Santa, CARITO NATIVIDAD HIDALGO CORONEL Y GERSON STEVE SOLANO VIDAL, en ejercicio del derecho a la iniciativa legislativa prevista en el artículo 107° de la Constitución Política del Perú y concordante con los artículos 75 ° y 76 ° del Reglamento del Congreso de la República, proponen el siguiente Proyecto de Ley:

I. EXPOSICIÓN DE MOTIVOS

El derecho penal, en el cual se materializa la potestad sancionadora del Estado, no puede ser ajeno a los cambios sociales y el avance tecnológico de la sociedad, por lo que ante el surgimiento de nuevas modalidades delictivas se hace necesario adecuar los tipos penales cuando sea posible, o crear nuevos cuando no sea así.

Dentro de las modalidades delictivas más empleadas por los cibercriminales, el phishing en sus diversas modalidades ha alcanzado un elevado auge, lo que se evidencia de la multitud de denuncias que se registran ante la autoridad policial y fiscal.

Si bien la Ley 30096 Ley de Delitos Informáticos regula diversos dispositivos legales destinados a combatir la cibercriminalidad, los mismos resultan insuficientes ante la sofisticación y dinamismo de las conductas ejecutadas por los ciberdelincientes, quienes varían constantemente la forma en que llevan a cabo sus actos ilícitos. Esto genera un clima de impunidad, pues una de los principios generales del derecho penal –el principio de legalidad- impide que se sancione una conducta si no ha sido previamente regulada como delito.

Así, la actuación de los magistrados –jueces y fiscales- operadores del derecho penal, se encuentra limitada cuando se enfrentan a casos cada vez más difíciles de subsumir en los tipos penales existentes, pues en el derecho penal existen otras limitaciones como la prohibición de la analogía y la obligación de interpretar restringidamente los tipos penales.

Por tal motivo, es importante la creación de un tipo penal que englobe las nuevas modalidades de phishing teniendo en cuenta todas las limitaciones de los tipos penales vigentes, a fin de que toda conducta derivada del empleo de técnicas de ingeniería social para la obtención de datos confidenciales de la víctima, pueda ser sancionada adecuadamente.

II. VIGENCIA DE LA NORMA QUE SE PROPONE

Respecto a la de vigencia de la norma propuesta, se tiene que no afecta la normatividad Constitucional; por el contrario, asegura la Norma Constitucional Peruana:

Nuestra Constitución Política establece en su artículo 2 numeral 24 literal "d" que "*Toda persona tiene derecho: (...) A la libertad y a la seguridad personales. En consecuencia: (...) Nadie será procesado ni condenado por acto u omisión que al tiempo de cometerse no esté previamente calificado en la ley, de manera expresa e inequívoca, como infracción punible; ni sancionado con pena no prevista en la ley*".

III. ANÁLISIS DEL COSTO-BENEFICIO

En cuanto al Costo de la presente Iniciativa Legislativa, no genera un gasto para el Estado peruano adicional al que ya se hace para poder proceder a legislar: copias y el pago a los legisladores y asesores del Congreso. Respecto al Beneficio es de suma importancia, pues permitirá a los magistrados del país (jueces y fiscales) investigar y sancionar adecuadamente un hecho ilícito que genera un grave detrimento patrimonial y personal para muchas personas que son víctimas de *phishing*. Esto, por tanto, dotará de mayor seguridad a la población frente al accionar de personas inescrupulosas que acceden a información sensible que posteriormente es usada en perjuicio de la víctima.

Por consiguiente, el Beneficio será para la población en general, pues se dotará a los jueces y fiscales de la posibilidad de sancionar una conducta perjudicial para la población.

IV. FORMULA LEGAL

El Congreso de la República
Ha dado la Ley siguiente:

LEY QUE INCORPORA EL ARTÍCULO 7-A EN LA LEY DE DELITOS INFORMÁTICOS LEY 30096

Artículo 1°.- Incorpórese el artículo 7-A en el Capítulo IV de la Ley de Delitos Informáticos, Ley 30096.

Artículo 7-A.- Obtención fraudulenta de información confidencial

"1. El que con objeto ilícito o sin estar facultado para ello, diseñe, desarrolle, venda, ejecute, programe o envíe páginas electrónicas fraudulentas, enlaces o ventanas emergentes, con la finalidad de obtener información sensible de un tercero, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años, siempre que la conducta no constituya delito sancionado con pena más grave.

2. Si el agente emplea o comercializa la información sensible obtenida, y se ocasiona un perjuicio patrimonial a la víctima o un tercero, la pena privativa de libertad será no menor de cuatro ni mayor de ocho años.

3. La pena a la que se refiere el inciso precedente será agravada en cinco años si para la consumación del delito han participado más de dos personas."

DISPOSICIÓN COMPLEMENTARIA

Única: La presente modificación será de aplicación a los procesos penales que se inicien al momento de la publicación en el diario oficial el peruano.

ANEXO 02: ENCUESTA A LOS MAGISTRADOS DEL DISTRITO FISCAL DEL SANTA

UNIVERSIDAD NACIONAL DEL SANTA

FACULTAD DE EDUCACION Y HUMANIDADES

CUESTIONARIO N ° 01

ENCUESTA SOBRE LA SITUACION JURIDICA DEL PHISHING EN EL PERÚ

OBJETIVO: Verificar el resultado de las investigaciones fiscales por denuncias de phishing en el Distrito Fiscal del Santa.

INSTRUCCIONES:

Estimado Magistrado: Nos encontramos realizando un trabajo de investigación a fin de determinar si es necesaria una modificación en la Ley de Delitos Informáticos para incorporar un tipo penal específico que regule el phishing, para lo cual se les pide su colaboración respondiendo algunas preguntas sobre las incidencias de su labor fiscal en relación al tema de estudio. Sus respuestas son muy importantes para alcanzar nuestro objetivo. Gracias por su colaboración.

I. TIPIFICACION DEL PHISHING EN EL ORDENAMIENTO JURIDICO PERUANO

1. **¿Considera que es posible subsumir el phishing en alguno de los siguientes delitos previstos en el Código Penal?**

   a. Hurto ( )
   b. Estafa ( )
   c. Falsedad genérica ( )
   d. Otro ( )
   e. Ninguno ( )

2. **¿Considera que es posible subsumir el phishing en alguno de los siguientes delitos previstos en la Ley de Delitos Informáticos?**

   a. Fraude informático ( )
   b. Suplantación de identidad ( )
   c. Acceso ilícito ( )
   d. Otro ( )

e. Ninguno ( )

3. **¿Considera que es posible subsumir en algún tipo penal la conducta de aquel que, creando una identidad totalmente falsa por medios informáticos, logra obtener datos bancarios de una persona y luego retira dinero de sus cuentas?**

   a. Sí ( )
   b. No ( )

II. SITUACION DEL PHISHING EN LAS INVESTIGACIONES FISCALES

4. **¿Durante sus labores como magistrado, ha tenido investigaciones relacionadas a phishing que hayan superado la etapa de investigación preparatoria?**

   a. Sí ( )
   b. No ( )

5. **¿Cuál ha sido el estado final de la mayoría de casos relacionados a phishing investigados en su despacho?**

   a. Archivo preliminar ( )
   b. Sobreseimiento ( )
   c. Sentencia condenatoria ( )
   d. Sentencia absolutoria ( )

6. **¿Considera que la actual redacción normativa de los delitos informáticos según la Ley 30364 incide negativamente en la capacidad de investigar los casos de phishing que se denuncian?**

   a. Sí ( )
   b. No ( )

ANEXO 03: NOTICIA NACIONAL – PHISHING, EL CIBERATAQUE QUE MÁS SE INCREMENTÓ POR LA PANDEMIA

Menú | GESTIÓN | Phishing, el ciberataque que más se incrementó en el país por...

Phishing, el ciberataque que más se incrementó en el país por pandemia

Las empresas tendrían que incrementar su inversión en ciberseguridad ahora que están más expuestas por el trabajo remoto y el uso de dispositivos personales, afirma el líder regional de consultoría en riesgo cibernético en Marsh.

El phishing ocurre cuando el estafador se gana la confianza de la víctima haciéndose pasar por una persona o empresa conocida. (Foto: Reuters).

ÚLTIMAS NOTICIAS

WhatsApp: qué hacer si no se pueden descargar archivos...

Día del Padre: Google celebra a los papás con doodle que simu...

Tres carreras profesionales de videojuegos que se pueden...

Redacción Gestión
redacciongestion@diariogestion.com.pe

Actualizado el 27/01/2021 08:15 p.m.

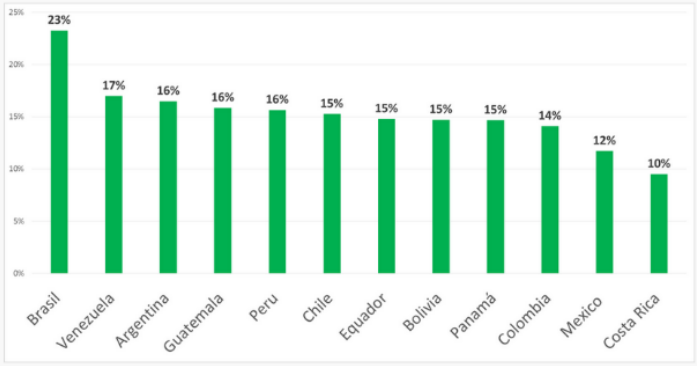
El 49% de las empresas peruanas percibió un incremento en los ataques cibernéticos a raíz de la pandemia, según el estudio Estado del Riesgo Cibernético en Latinoamérica en Tiempos del COVID-19 . La encuesta también revela que el 21% considera que la ingeniería social (phishing) es el ciberataque que más se ha incrementado, mientras que el 20% sostiene que ha sido el malware.

El phishing ocurre cuando el estafador se gana la confianza de

ANEXO 04: NOTICIA INTERNACIONAL – KASPERSKY LAB REGISTRA UN ALZA DE 60% EN ATAQUES CIBERNÉTICOS EN AMÉRICA LATINA

Kaspersky Lab registró más de 746 mil ataques de malware diarios durante los últimos 12 meses en América Latina, lo que significa **un promedio de 9 ataques de malware por segundo**. Además, los ataques de phishing –correos engañosos para el robo de la información personal de los usuarios– han sido constantes en la región, principalmente en Brasil. Los resultados, presentados durante la Octava Cumbre de Analistas de Seguridad para América Latina que se está realizando en la Ciudad de Panamá, demuestran que toda la región ha experimentado una considerable cantidad de ciberamenazas, con la gran mayoría orientada al robo de dinero.

Según **Dmitry Bestuzhev, Director del Equipo de Investigación y Análisis para América Latina en Kaspersky Lab,** hubo un incremento del 60% en ataques cibernéticos en la región, donde Venezuela registra el mayor número de los ataques en proporción a su población con un total de 70.4%, seguido por Bolivia (66.3%) y Brasil (64.4%). Al igual que en 2017, Brasil continua encabezando a los países latinoamericanos en términos de alojamiento de sitios maliciosos ya que 50% de los hosts ubicados en América Latina que se utilizaron en ataques



Ranking de países latinoamericanos afectados por phishing durante los primeros 7 meses de 2018

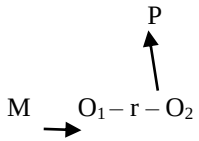
Según Assolini, el período preferido por los cibercriminales para realizar ataques de este tipo en América Latina es el **Viernes Negro (*Black Friday*). Sólo en 2017 se bloquearon más de 380.000 ataques de phishing ese día -- casi 4 veces más que en un día normal**. La táctica es fácil pero efectiva: miles de correos electrónicos falsos, con supuestas ofertas tentadoras de electrodomésticos, smartphones, entre otros productos, son enviados para llamar la atención de las víctimas. A partir de eso, si el usuario hace clic en el enlace, será redirigido a un sitio falso donde colocará los datos de la tarjeta para efectuar la compra, facilitándoles sus datos a los cibercriminales sin desconfiar de nada.

ANEXO 5. MATRIZ DE CONSISTENCIA.

Título: EL PHISHING COMO CONDUCTA DELICTIVA NO REGULADA EN EL ORDENAMIENTO JURIDICO PERUANO. PROPUESTA DE INCORPORACIÓN DEL ARTÍCULO 7-A EN LA LEY DE DELITOS INFORMÁTICOS 30096

<table>
<tr><th>Problema</th><th>Objetivos</th><th>Hipótesis</th><th>Variables</th><th>Dimensiones</th><th>Método</th></tr>
<tr><td rowspan="3">¿Cuáles son los fundamentos jurídicos para tipificar el phishing en el ordenamiento jurídico peruano y evitar su impunidad como conducta delictiva?</td><td>a. Desarrollar los fundamentos jurídicos para tipificar el phishing en el ordenamiento jurídico peruano y evitar su impunidad como conducta delictiva.</td><td>Dado que es necesario tipificar el phishing en el ordenamiento jurídico peruano para evitar la impunidad de la conducta, es probable que los fundamentos jurídicos que lo justifiquen sean el principio de legalidad y el principio de lesividad.</td><td rowspan="2">V1
La tipificación del phishing en el ordenamiento jurídico peruano.</td><td>Phishing</td><td rowspan="3">El método es cualitativo, Tipo de investigación será de teoría fundamentada y propositivo.

El diseño

M: Muestra 15 fiscales del Distrito Fiscal del Santa
O1: Observación de la variable tipificación del</td></tr>
<tr><td>Específicos
Objetivo específico 1:
Determinar la relación que existe entre los tipos penales previstos en el Código Penal y la impunidad del phishing.</td><td rowspan="2"></td><td>Tipos penales</td></tr>
<tr><td>Objetivo específico 2
Determinar la relación que existe entre los tipos penales previstos en el Código Penal y la impunidad del phishing.</td><td>V2
Impunidad del phishing en el Perú</td></tr>
</table>

	Objetivo específico 3: Verificar el resultado de las investigaciones fiscales por denuncias de phishing en el Distrito Fiscal del Santa.			Estado final de las investigaciones finales	phishing en el ordenamiento jurídico peruano O2: Observación de la variable impunidad del phishing en el Perú r: Correlación entre variables. P: Propuesta elaborada por los autores del estudio. **Técnicas de recolección de datos** La encuesta. El fichaje **Instrumento:** El cuestionario Fichas textuales Fichas bibliográficas Fichas de resumen
	Objetivo específico 4: Proponer la incorporación del phishing como un tipo penal independiente en la Ley de Delitos Informáticos30096.				

ANEXO 6. MATRIZ DE OPERACIONALIZACION DE VARIABLES.

Variable	Dimensión	Indicadores	ÍTEMS
V.C.1. Tipificación del phishing en el ordenamiento jurídico peruano	Phishing	Bien jurídico vulnerado	*a. Patrimonio* *b. Fe pública* *c. Intimidad*
	Tipos penales	Código Penal	*a. Hurto* *b. Estafa* *c. Falsedad genérica*
		Ley de Delitos Informáticos	*a. Interceptación de datos informáticos* *b. Fraude informático* *c. Suplantación de identidad*
V.C.2 La impunidad del phishing	Investigaciones Penales	Estado final de las investigaciones fiscales	*a. Archivo* *b. Sobreseimiento* *c. Sentencia absolutoria* *d. Sentencia condenatoria*

DECLARACION JURADA DE AUTORÍA

Yo, Gerson Steve Solano Vidal, **estudiante** / docente de la

Facultad:	Ciencias		Educación	X	Ingeniería		
Escuela Profesional:	Derecho y Ciencias Políticas						
Departamento Académico:	Humanidades y Ciencias Sociales						
Escuela de Posgrado	Maestría			Doctorado			
Programa:							

De la Universidad Nacional del Santa; Declaro que el trabajo de investigación intitulado:

"EL PHISHING COMO CONDUCTA DELICTIVA NO REGULADA EN EL ORDENAMIENTO JURIDICO PERUANO. PROPUESTA DE INCORPORACIÓN DEL ARTÍCULO 7-A EN LA LEY DE DELITOS INFORMÁTICOS 30096"

presentado en 138 folios, para la obtención del Grado académico:			( )
Título profesional:	(X)	Investigación anual:	( )

- He citado todas las fuentes empleadas, no he utilizado otra fuente distinta a las declaradas en el presente trabajo.
- Este trabajo de investigación no ha sido presentado con anterioridad ni completa ni parcialmente para la obtención de grado académico o título profesional.
- Comprendo que el trabajo de investigación será público y por lo tanto sujeto a ser revisado electrónicamente para la detección de plagio por el VRIN.
- De encontrase uso de material intelectual sin el reconocimiento de su fuente o autor, me someto a las sanciones que determinan el proceso disciplinario.

Nuevo Chimbote, 14 de julio del 2021

Firma:

Nombres y Apellidos: GERSON STEVE SOLANO VIDAL

DNI: 70012820

NOTA: ***Esta Declaración Jurada simple indicando que su investigación es un trabajo inédito, no exime a tesistas e investigadores, que no bien se retome el servicio con el software antiplagio, ésta tendrá que ser aplicado antes que el informe final sea publicado en el Repositorio Institucional Digital UNS.***

DECLARACION JURADA DE AUTORÍA

Yo, Carito Natividad Hidalgo Coronel, **estudiante** / docente de la

Facultad:	Ciencias		Educación	X	Ingeniería		
Escuela Profesional:	Derecho y Ciencias Políticas						
Departamento Académico:	Humanidades y Ciencias Sociales						
Escuela de Posgrado	Maestría		Doctorado				
Programa:							

De la Universidad Nacional del Santa; Declaro que el trabajo de investigación intitulado:

"EL PHISHING COMO CONDUCTA DELICTIVA NO REGULADA EN EL ORDENAMIENTO JURIDICO PERUANO. PROPUESTA DE INCORPORACIÓN DEL ARTÍCULO 7-A EN LA LEY DE DELITOS INFORMÁTICOS 30096"

presentado en 138 folios, para la obtención del Grado académico:			( )
Título profesional:	(X)	Investigación anual:	( )

- He citado todas las fuentes empleadas, no he utilizado otra fuente distinta a las declaradas en el presente trabajo.
- Este trabajo de investigación no ha sido presentado con anterioridad ni completa ni parcialmente para la obtención de grado académico o título profesional.
- Comprendo que el trabajo de investigación será público y por lo tanto sujeto a ser revisado electrónicamente para la detección de plagio por el VRIN.
- De encontrase uso de material intelectual sin el reconocimiento de su fuente o autor, me someto a las sanciones que determinan el proceso disciplinario.

Nuevo Chimbote, 14 de julio del 2021

Firma:

Nombres y Apellidos: CARITO NATIVIDAD HIDALGO CORONEL

DNI: 47956379

NOTA: ***Esta Declaración Jurada simple indicando que su investigación es un trabajo inédito, no exime a tesistas e investigadores, que no bien se retome el servicio con el software antiplagio, ésta tendrá que ser aplicado antes que el informe final sea publicado en el Repositorio Institucional Digital UNS.***