



UNIVERSIDAD PARTICULAR DE CHICLAYO

FACULTAD DE DERECHO Y EDUCACIÓN

ESCUELA PROFESIONAL DE DERECHO



TESIS:

**El Phishing o Suplantación de la identidad digital, y su incidencia
dentro de la criminalidad informática en la legislación penal peruana
año 2022**

Autor:

HELFER JAIRO VALDEZ HERNÁNDEZ

Orcid.org/0009-0001-4873-2396

Asesor:

DR. AVELLANEDA CALLIRGOS, LOLO

Orcid.org/0000-0001-5133-5546

LINEA DE INVESTIGACIÓN

Derecho Público y Privado.

Pimentel, Perú - 2024



ACTA DE CONTROL DE ORIGINALIDAD DE LA INVESTIGACIÓN

Yo, **Enrique Rodas Ramírez**, Decano de la Facultad de Derecho y Educación ha realizado el debido control de originalidad de la investigación, el mismo que está dentro de los porcentajes establecidos para el nivel de pregrado, según la Directiva de Similitud vigente en la UDCH; además certifico que la versión que hace entrega es la versión final del informe presentado por el bachiller: **VALDEZ HERNÁNDEZ HELFER JAIRO**

Titulado: **"EL PHISHING O SUPLANTACIÓN DE LA IDENTIDAD DIGITAL, Y SU INCIDENCIA DENTRO DE LA CRIMINALIDAD INFORMÁTICA EN LA LEGISLACIÓN PENAL PERUANA AÑO 2022"**

Elaborado por el estudiante, **VALDEZ HERNÁNDEZ HELFER JAIRO** Se deja constancia que la investigación antes indicada tiene un índice de similitud del 16% verificable en el reporte final del análisis de originalidad mediante el software de similitud **TURNITIN**.

Por lo que se concluye que cada una de las coincidencias detectadas no constituyen plagio y cumple con lo establecido en la Directiva sobre el nivel de similitud de productos acreditables de investigación vigente.

Pimentel, 31 de marzo del 2025.


UNIVERSIDAD PARTICULAR DE CHICLAYO
FACULTAD DE DERECHO Y EDUCACIÓN
Dr. Enrique Rodas Ramírez
DECANO

El Phishing o Suplantación de la identidad digital, y su incidencia dentro de la criminalidad informática en la legislación penal peruana año 2022

INFORME DE ORIGINALIDAD

16%	16%	2%	6%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	hdl.handle.net Fuente de Internet	5%
2	revistas.pucp.edu.pe Fuente de Internet	2%
3	repositorio.uss.edu.pe Fuente de Internet	1%
4	angelderechoinformatico.blogspot.com Fuente de Internet	1%
5	repositorio.adp.edu.pe Fuente de Internet	1%
6	repositorio.ucv.edu.pe Fuente de Internet	1%
7	tesis.pucp.edu.pe Fuente de Internet	1%
8	www.slideshare.net Fuente de Internet	1%

TITULO DE LA TESIS:

**"EL PHISHING O SUPLANTACIÓN DE LA IDENTIDAD DIGITAL, Y SU
INCIDENCIA DENTRO DE LA CRIMINALIDAD INFORMÁTICA EN LA
LEGISLACIÓN PENAL PERUANA AÑO 2022."**

Para optar el Título Profesional de ABOGADO

Bach. VALDEZ HERNÁNDEZ HELFER JAIRO
AUTOR

Dr. Lolo Avellaneda Callirgos
ASESOR

Aprobado por el siguiente jurado:



Dr. Javier Soriano Diaz Diaz
Presidente



Mg. Mauro Alindor Yrigoin Soto
Secretario



Dr. Deyvi Jahir Vera Alvarez
Vocal

Tesis **titulada:** “El phishing o suplantación de la identidad digital, y su incidencia dentro de la criminalidad informática en la legislación penal peruana año 2022”, presentada por el Bachiller Helfer Jairo Valdez Hernández, a la facultad de Derecho y Educación de la Universidad Particular de Chiclayo, para optar el Título Profesional de Abogado.

Presentado por:

Helfer Jairo Valdez Hernández

Autor

DR. AVELLANEDA CALLIRGOS, LOLO

Asesor

Aprobado por Jurado

Presidente

secretario

Vocal

INDICE

INDICE.....	vi
RESUMEN	viii
ABSTRACT	ix
I.- INTRODUCCIÓN.....	1
II.- DESARROLLO.	4
IV METODOLOGIA.....	23
4.1.- Tipo de Investigación.	23
4.2.- Diseño de investigación.....	23
4.3.- Categorías, subcategorías y matriz de categorización.	23
4.4.- Escenario de estudio.....	25
4.5.- Participantes	25
4.6.- Técnicas e instrumentos de recolección de datos.....	25
4.7.- Procedimientos de recolección de datos e informaciones:	26
4.8.- Validez y confiabilidad.....	26
4.9.- Criterios de Rigor científico.	26
4.10. – Aspectos éticos	26
IV.- RESULTADOS	27
4.1.- De la entrevista.....	27
Diagrama global de objetivos:	43
4.2.- Discusión de resultados	44
CONCLUSIONES:.....	53
RECOMENDACIONES	55
ANEXOS	62
Anexo 01: Guía de entrevista	63
Anexo 02: Matriz de categorización.	68
Anexo 03: entrevistas	69

Índice de tablas:

Tabla 1: 4.3.- Categorías, subcategorías y matriz de categorización.	24
Tabla 2: Objetivo general	27
Tabla 3: Objetivo específico uno	32
Tabla 4: Objetivo específico dos	35
Tabla 5: Objetivo específico tres	39

RESUMEN

La investigación que se ha desarrollado titulada “El Phishing o suplantación de la identidad digital, y su incidencia dentro de la criminalidad informática en la legislación penal peruana año 2022”, está dentro del marco de investigaciones de ilícitos realizados mediante medios informáticos, en la actualidad vienen a ser las nuevas formas de criminalidad informática; el objetivo general fue Determinar la incidencia del ilícito de Phishing o suplantación de la identidad digital, dentro de la criminalidad informática en la legislación penal peruana año 2022; mediante una metodología de tipo básica descriptiva, con diseño cualitativo, se ha podido recaudar datos de información, mediante técnicas como la entrevista, la misma que mediante el instrumento de la ficha de entrevista se ha llegado a rescatar información de profesionales del derecho penal que mediante su opinión han participado en la presente investigación; entre las conclusiones que se han llegado, tenemos que el delito de Phishing está teniendo un evidente crecimiento y desarrollo, además es muy complicado enfrentarlo, inclusive para los especialistas, debido a que el ciber delincuente aplica técnicas de ingeniería informática con la finalidad de obtener los datos personales de los usuarios con la finalidad de suplantar su identidad. Si bien es cierto, se encuentra vigente la Ley 360096 que sanciona este delito, no ha sido eficaz debido a que no ha conseguido frenarlo.

Palabra clave: Delito informático / suplantación de la identidad

ABSTRACT

The research that has been developed titled "Phishing or impersonation of digital identity, and its impact on computer crime in Peruvian criminal legislation in 2022", is within the framework of investigations of crimes carried out through computer means, currently They become the new forms of computer crime; The general objective was to determine the incidence of the illicit phishing or digital identity theft, within computer crime in Peruvian criminal legislation in 2022; Through a basic descriptive methodology, with a qualitative design, it has been possible to collect information data, through techniques such as interviews, the same as through the instrument of the interview sheet, it has been possible to rescue information from criminal law professionals who, through their opinion have participated in this investigation; Among the conclusions that have been reached, we have that the crime of Phishing is having an evident growth and development, it is also very complicated to confront it, even for specialists, because the cyber criminal applies computer engineering techniques in order to obtain the personal data of users with the purpose of impersonating their identity. Although it is true that Law 360096 that punishes this crime is in force, it has not been effective because it has not managed to stop it.

Keyword: Computer crime / identity theft

I.- INTRODUCCIÓN

El desarrollo de investigaciones de ilícitos realizados mediante medios informáticos, se considera de mucha importancia, pues actualmente la criminalidad informática ha generado nuevas formas, hace ya varios años atrás; es decir de la computadoras (Pc), a las tablets, laptops, Iphone, que han invadido nuestra vida cotidiana, nuestro hogar y centro laboral; ahora son actividades y ocupaciones humanas, cotidianas; que con ayuda del internet el acceso a muchos espacios del mundo mediante las Apps, que consiente acceder remotamente a diversos sistemas informáticos haciendo que las personas víctimas ante modalidades nuevas de filtración de datos, usurpación de identidades y robos a través de este medio, entre otras cosas. (Zea, 2022)

Mediante la Unión europea, se hizo ratificación del Convenio de Budapest y la reciente creación de la Unidad Fiscal Especializada en Ciberdelincuencia del Ministerio Público son señales positivas del interés que va despertando este tema; sin embargo, aún hay mucho por trabajar, como la capacitación del personal fiscal, judicial y policial, y la dotación de tecnología para la División de Investigación de Delitos de Alta Tecnología de la Policía Nacional (DIVINDAT) y la Unidad de Peritajes Informáticos del Instituto de Medicina Legal y Ciencias Forenses. Asimismo, se hace necesaria crear fiscalías especializadas para esta clase de ilícitos en los distritos fiscales. (Unión Europea, 2021)

Según la OEA (2023), señaló que la ciberdelincuencia, viene superando destacadamente a la delincuencia tradicional en el mundo físico, este tipo de delincuencia posee sui generis fortalezas en el mercado delictivo nivelando la oferta y la demanda criminógena, con barreras de entrada propias; además, mediante una variada oferta y muy amplia; oferta de servicios. Ante esta problemática es necesario que los Estados, hagan una amplia concientización de protección tecnológica “evangelización” a los cibernautas en seguridad informática y ciberseguridad, teniendo en cuenta que el factor humano a la parte a quien se debe investigar y perseguir el crimen mediante una cultura de prevención personal y a nivel de organizaciones con posibilidades de cometer ilícitos con la finalidad de llegar a controlar la ciberdelincuencia.

Desde la implementación de la Ley 30096 sobre delitos informáticos en nuestro país, se establecieron sanciones y penas específicas para diversas infracciones. Entre ellas, el Phishing o suplantación de identidad digital se destaca como una modalidad que permite a los delincuentes obtener contraseñas y acceso a cuentas bancarias en cuestión

de segundos, aprovechándose de la confianza de las víctimas a través de redes sociales, software y plataformas en línea (Espinoza,2020)

En el contexto de la COVID-19, se cometieron diversos ilícitos de informática a nivel mundial, donde se ha demostrado que hay poca capacidad de persecución. La necesidad que tenemos en la presente investigación es porque en nuestro Estado peruano, existe una deficiente legislación y la poca que existe sostiene bastantes vacíos normativos en la Ley N°30096 y su modificación con la Ley N°30171. La rama del Derecho tiene que intervenir en el análisis del tipo penal, y la doctrina con la jurisprudencia para lograr impulsar aspectos normativos que corrijan y mejoren hacer frente a este problema.

Los informes del Ministerio Público señalaron que en los últimos años hasta el 2020, se han registrado 21,687 denuncias por delitos informáticos, siendo en tiempos de pandemia por la COVID-19 donde se incrementó la ciberdelincuencia siendo los diversos fraudes informáticos, suplantaciones de identidad y estafas virtuales, entre otros conformando a la ciberdelincuencia. (MINJUS, 2022)

Ante lo expuesto, nuestra investigación analizó aspectos normativos que puedan incorporarse como es el tipo penal señalado en la Ley 30096, considerando las insuficiencias de los procedimientos tecnológicos presentados en diversas instituciones públicas entre ellas el caso de RENIEC.

La Defensoría del Pueblo (2023), señaló en su publicación que, en la Región Lambayeque, las fiscalías provinciales Penales y Mixtas que se las mismas desplegadas en provincias y distritos tienen conocimiento e investigan 955 denuncias desde el año 2022 que representan un 4.4% de las denuncias a nivel nacional (representa 21,687 hechos denunciados), ciberdelitos previstos en la Ley de Delitos Informáticos (2020).

La causa del problema residió en que existen vacíos normativos de la Ley N°30096, que permiten el incremento de los delitos cibernéticos los cuales vulneran la protección de datos personales, y que sus consecuencias por dichas violaciones de datos, se encuentra plasmada en la Ley N°30096, Ley de Delitos Informáticos.

En relación al objetivo de desarrollo sostenible (ODS) el perfil de nuestro estudio se relacionó con el objetivo dieciséis, al relacionarse ampliamente a derechos humanos, donde la sociedad defiende y respeta los derechos individuales, además el derecho a la expresión, intimidad, acceso a la información, etc.

Ante lo expuesto, se planteó el problema: ¿De qué manera el Phishing o suplantación de la identidad digital, viene incidiendo dentro de la criminalidad informática en la reglamentación penal peruana durante el año 2022?

Así mismo se consideraron las siguientes preguntas específicas: a) ¿Cuáles son los aspectos doctrinales y jurídicos de delitos informáticos en la legislación peruana?, b) ¿Se encuentra adecuado el tipo penal de suplantación de identidad digital en la legislación penal peruana?, c) ¿Qué señala la Ley 30096 de ilícitos informáticos y su modificación Ley 30171, respecto a la criminalidad informática en el sistema penal peruano?

La justificación del presente proyecto, fue desde un aspecto teórico, que permitirá analizar la problemática evolutiva de los delitos informáticos, pues se tomará en cuenta la doctrina emitida por los juristas internacionales y naciones, la jurisprudencia con la cual es que las partes procesales invocan dentro del proceso penal, así como el tipo penal se encuentra prescrito.

Desde un aspecto practico, permitió difundir la problemática que viene acosando la provincia de Chiclayo mediante ciberdelitos teniendo como tipo penal la suplantación de la identidad digital cuyas acciones forman parte de la inseguridad ciudadana.

Desde el punto de vista metodológico, ha tenido su justificación al haberse planteado métodos, tipos de estudio y análisis de datos, que han servido para profundizar el problema de los delitos informáticos en su figura de la suplantación de la identidad digital en la provincia de Chiclayo. Para abordar este problema, se sugiere considerar los aspectos penales clave que deben ser integrados en la configuración de los tipos penales relacionados con el phishing, específicamente la utilización de comunicaciones digitales fraudulentas con el objetivo de obtener información personal de terceros.

Se consideraron desarrollar los objetivos siguientes, el general: Determinar la incidencia del ilícito de Phishing o suplantación de la identidad digital, dentro de la criminalidad informática en la legislación penal peruana año 2022.

Así, como los específicos: a) describir los aspectos doctrinales y jurídicos de delitos informáticos en la legislación peruana; b) desarrollar el tipo penal de suplantación de identidad digital en la legislación penal peruana; c) analizar la criminalidad informática en el sistema penal peruano mediante la ley 30096 ley de delitos informáticos y su modificatoria Ley 30171.

II.- DESARROLLO.

Para desplegar el estudio, se han considerado antecedentes internacionales, naciones y locales; de esta manera desde el punto de vista internacional, se cita el estudio desarrollado en México, por Solís (2020), en su investigación que tituló “Robo informático, considerado como nueva modalidad llamada phishing”, el objetivo de la investigación fue: establecer el modus operandi de las bandas criminales en los ilícitos contra el patrimonio mediante medios electrónicos, esto con un diseño cualitativo-descriptivo, y selección de datos en las entidades afectadas, cuyo resultado indica que el robo de información en el sistema bancario crea esta figura antijurídica, donde existe una actuación mediante modus operandi similar al robo digital, existe un reporte durante el año 2020 en México de un promedio de 71.5%. Llegando a la conclusión: que en México se encaminan respecto a legalizar mejores sanciones a delito, a pesar de las innovaciones tecnológicas no se debe dejar de lado futuras modalidades delictivas.

El autor argumenta que el phishing son técnicas de ingeniería utilizando links, envíos de correo con la finalidad de obtener datos que suplanten la identidad del usuario bancario, y generalmente este delito es cometido por organizaciones criminales muy bien estructuradas y con los recursos tecnológicos idóneos para conseguir su finalidad ilícita.

En Chile, el investigador Oxman (2021) en su investigación “Estafas informáticas a través de internet. Acerca de la imputación penal del phishing y el pharming”; siendo el objetivo general analizar las estafas informáticas desarrolladas a través de internet, y la imputación penal del phishing y el pharming. La metodología utilizada es de tipo básica, con diseño cuantitativo, y de instrumento se desarrolló la encuesta; el resultado señala, que mayormente el fraude informático se presenta en el sistema bancario, debido a que actualmente el derecho penal analiza la estafa como un ilícito especial, así también se llega entre sus conclusiones: que frente a las nuevas modalidades delictivas (fishing) no se registra consecuentemente a que la ley de manera general no es actualizada ante los nuevos ilícitos presentados.

El autor pretende manifestar que la normativa de Chile necesita una regulación pertinente de carácter urgente para conseguir enfrentar el requerimiento de punición necesario para los delitos bancarios perpetrados mediante la banca online en todos sus

ámbitos como en el Código Penal y en las Leyes penales del delito informático, garantizando de esa forma las transacciones civiles y comerciales realizadas mediante instituciones bancarias.

En España, de acuerdo con un artículo publicado por EFE en (2021), titulado "Estafa cibernética, ilícito de moda que brota los colores a la víctima", señala el registro del aumento significativo en los casos de estafa informática en los últimos meses, siendo las empresas las más afectadas. La cibercriminalidad ha crecido un 40% en los últimos años, impulsada por crecimiento tecnológico, la comercialización electrónica e innovadores medios de comunicación y trabajo. Ante esta situación, el Estado propone y requiere la implementación de una mayor seguridad jurídica cibernética para proteger de manera efectiva la integridad y los datos personales de las personas.

En este trabajo, el autor refiere que infiere que se han presentado varias figuras de estafa cibernética, y en estas se utilizan la información bancaria o personal del usuario bancario para perpetrar el ilícito, generando una pérdida de su dinero depositado del agraviado, desde nuestra perspectiva, las entidades bancarias tienen que implementar un sistema mas seguro para sus usuarios, puesto que, ellos cobran una comisión por depositar nuestro dinero, debiendo garantizar que permanecerá en el banco sin inconvenientes.

Entre los estudios que se han considerado a nivel nacional, se tiene en cuenta al investigador Schwartz, (2020), en su trabajo titulado "Reporte ciberseguridad riesgos, avances y el camino a seguir en américa latina y el caribe" siendo el objetivo trazado fue analizar las tácticas optadas por nuestro país para luchar contra la ciberdelincuencia, siendo afiliarse al Convenio de Budapest mediante Resolución Legislativa N.º 30913, la metodología fue básica descriptiva, con diseño trasversal, que permitió culminar la investigación.

El resultado señala que los daños económicos recibidos mediante ataques cibernéticos superan en el PIB el 1%, de esta manera mediante medios de la tecnología se crean oportunidades para que los ciberdelincuentes ejecuten ilícitos en el sistema digital; las conclusiones a las que llega: es que doce países son los que aprueban estrategias nacionales respecto ciberseguridad. El convenio cuenta con objetivos basados en la capacidad nacional que deben tener los países para la prevención del ilícitos cibernéticos, contrarrestando de esta manera las amenazas cibernéticas lo que exigen a los países en contar con legislaciones, capacitaciones y política.

El desarrollo tecnológico en todos sus ámbitos ha generado un reto representado un reto para la defensa y seguridad de las Naciones, ya que, a evidenciado un amplio desarrollo y también ha generado una gran vulneración al derecho del patrimonio de las personas, esto representa un desafío grande donde los actores políticos de sus diversos niveles tienen que garantizar y asumir la defensa y seguridad de la ciudadanía en el Estado, una medida pertinente es que el Estado capacite a los policías encargados de esta división no solo se trata de dotarlos de recursos o herramientas tecnológicas, sino de instruirlos para que estén en capacidad de enfrentar con celeridad este escenario donde muchas veces no se logra identificar al sujeto activo.

De acuerdo con Flores (2020), en su tesis titulada “Tecnología y violencia en Perú. En Hiper derecho”, su objetivo fue Describir los niveles de la tecnología e índices de violencia en Perú. la metodología a través del método de investigación cualitativa y diseño de investigación descriptivos, se concluye que Perú se posiciona como el quinto país en América Latina que más sufre ataques cibernéticos, afectando predominantemente al sector financiero. Ante esta situación, una de las prioridades actuales en Perú es desarrollar estrategias y mecanismos efectivos para combatir la gran cantidad de ataques cibernéticos y, de esta manera, garantizar la seguridad informática.

Adicionalmente a ello Flores argumento que las mujeres son las mas propensas en ser víctimas del ciberacoso y otras figuras de violencia, a merced del desarrollo de la tecnología, sin embargo, el MIMP (Ministerio de la Mujer y Poblaciones Vulnerables) logro presentar una plataforma denominada “No al acoso virtual” donde se lograron registrar 102 de denuncias (febrero y marzo 2018), es evidente que debemos considerar a las mujeres de escasos recursos que no cuentan con el conocimiento del uso de las plataformas digitales y mucho menos tienen acceso a la tecnología.

Asimismo, Avalos (2020), en su trabajo titulado “Informe de análisis N°04 ciberdelincuencia: pautas para una investigación fiscal especializada”, cuyo objetivo fue Analizar el Informe N°04 ciberdelincuencia: pautas para una investigación fiscal especializada”, La metodología es aplicada, con enfoque cualitativo, analizando una diversidad de delitos informáticos, el resultado de la investigación señala en este tipo de investigaciones el Ministerio Público necesita reconstruir los elementos de imputación, para una adecuada imputación penal, asimismo Se concluye que Perú debe reconocer la importancia de incorporar operadores con especialización fiscal para sus servidores públicos, como parte integral de una política institucional efectiva. No obstante, es

fundamental enumerar estas especializaciones y considerar que el uso de la tecnología podría establecer indicadores clave para la obtención de pruebas digitales, siendo estas cruciales para el desarrollo de investigaciones.

El autor indicó que, de octubre-2013 y diciembre-2020, la DIVINDAT reconoció la totalidad de 12,169 ilícitos que se relacionan a la Ley 30096. De estos, 9,515 representa el 78% pertenecen a fraudes informáticos, continúan los ilícitos de suplantación de identidad (13%) terminando con (6%) de los ilícitos contra datos y sistemas informáticos.

Vílchez, (2020) en su tesis titulada “La ciberdelincuencia en el contexto de la pandemia del coronavirus. Una aproximación desde el marco convencional”, se enfocó en analizar los factores que han favorecido el aumento de la ciberdelincuencia, revelando las dificultades en la investigación y enjuiciamiento de estos delitos, la falta de capacitación adecuada de la policía y el uso insuficiente de técnicas especializadas. Con métodos de investigación cualitativos y diseños de investigación descriptivos, los hallazgos de la investigación indican que la crisis sanitaria global provocada por la pandemia del COVID-19 ha llevado a un aumento del uso de medios tecnológicos para las relaciones sociales y económicas, lo que a su vez ha incrementado la ciberdelincuencia. Vílchez concluye que una de las prioridades del sistema judicial penal es abordar las deficiencias legales existentes en Perú para identificar a los autores de delitos cibernéticos y superar las dificultades impuestas por los cortos plazos de investigación.

El autor señaló que en tiempos de Covid-19 permitió evidenciar que las personas usan la tecnología la mayor parte del día, convirtiéndose en el quehacer diario, sin considerar status, edad, genero, profesión, todas las personas usan estas herramientas tecnológicas es en esta circunstancia que los ciberdelitos aumentaron de manera masiva, De acuerdo al Ministerio público se tuvo un total de 21687 denuncias correspondientes a la modalidad de fraude informático, evidencia clara del aumento de los delitos informáticos en la emergencia sanitaria.

Tal como lo señala Zeballos (2020), en su estudio de analizar los ilícitos informáticos: sus fraudes principales informáticos cometidos mediante E-Commerce, el objetivo fue: determinar el fraude y sus principales modalidades informáticas que se pueden cometer a través del E-Commerce: se desarrolló con una metodología fue mediante el tipo aplicada, con enfoque cualitativo, analizando una diversidad de delitos

informáticos, la técnica fue el análisis documental, se cuenta como resultado que uno de los desafíos para que nuestro país ejecute una innovación digital sobrelleva a reflexionar ante los peligros que vulneran la seguridad informática; Se concluye que es esencial proteger la infraestructura de la información y crear un consejo de ciberseguridad para gestionar los riesgos informáticos. Además, es crucial fomentar la colaboración en el intercambio de información entre los sectores público y privado, con el fin de denunciar eficazmente los ataques cibernéticos y proporcionar estabilidad informática a los usuarios.

El autor, por todo lo argumentado señaló que es esencial que el gobierno genere o le atribuya a los operadores judiciales mecanismos para que enfrenten la ciberdelincuencia, sobre todo a la Oficina técnica del Ministerio Público y la DIVINDAT mayores herramientas tecnológicas con la finalidad de que realicen una investigación adecuada para lograr la identificación del sujeto activo.

A nivel local, se ha tenido a Fuentes (2021), señala en su análisis sobre las modificaciones de la ley 30096 para unir los ilícitos de phishing, pharming y carding como ilícitos sancionables penalmente con prisión, para someter la ciberdelincuencia en Lima-2019; el estudio tuvo como objetivo examinar la Modificación de la Ley 30096 para incluir los delitos de phishing, pharming y carding como delitos penalizables con prisión, con el fin de disminuir la ciberdelincuencia en Lima en 2019. La metodología empleada fue una investigación básica, utilizando entrevistas y encuestas, cuyos datos fueron analizados mediante el sistema SPSS. Los resultados revelaron la necesidad de incorporar el phishing y el pharming como modalidades delictivas realizadas a través de sistemas informáticos que vulneran derechos digitales. Se concluyó que una de las características de estas defraudaciones es la generación de miedo en las víctimas, utilizándolo como medio para engañarlas y robar su información personal.

Estas figuras delictivas representaron el engaño vigente que la globalización ocasiona, un detalle de este argumento es que, si se hubiese informado o capacitado a las personas de forma oportuna del uso de las TIC, las estadísticas de estos delitos como el pharming, phishing o carding, no hubiese sido tan alarmantes, es por ello que la Ley N°30096 posee diversas deficiencias legislativas respecto de la tipificación jurídica de las actividades consideradas de estos delitos en cuestión

De acuerdo a la investigación de Román (2022) en su tesis que tituló “Modificación legislativa de la ley N.º 30096 de delitos informáticos para su eficacia contra la ciberdelincuencia en la ciudad de Chiclayo”, presenta el objetivo donde se proponen cambios legislativos a la Ley N°30096 sobre Delitos Informáticos para combatir eficazmente el ciberdelito. Se fundamenta teóricamente en la teoría del delito informático; diagnostica la situación actual del cibercrimen; la metodología del estudio se adoptó un enfoque de métodos mixtos y la herramienta de recolección de datos fue un cuestionario administrado a 20 abogados especialistas en derecho penal. Los resultados demostraron que existen diversos tipos de delitos y estos delitos no están debidamente regulados por la ley y se concluyó que el delito informático se refiere a actividades ilícitas realizadas utilizando una computadora o cualquier dispositivo electrónico conectado a una red conectada.

El autor desde su perspectiva argumentó que es fundamental parametrizar que comportamientos deben considerarse como un ilícito informático o no, para disminuir la carga procesal innecesaria a los juzgados, por ejemplo, si una persona está utilizando y difama a otra se estaría vulnerando el derecho al honor, pero no configuraría un ilícito informático, Si una persona accede de manera ilegal o malintencionada a un sistema de datos sin la autorización correspondiente y sabotea la base de datos, dicha acción se clasifica como un delito informático. Por lo tanto, el gobierno debe invertir en la capacitación de su Policía Nacional del Perú (PNP).

Según Gonzales (2021) en su investigación relacionada con el comercio electrónico y la problemática de la ciberdelincuencia en momentos de Covid-19”, su objetivo es establecer estándares de protección y defensa del consumidor y garantizar que estos cuenten con acceso a dispositivos para que sus derechos sean protegidos y evitar participar en delitos cibernéticos. Como aspecto metodológico, se realizó un estudio aplicado, fue de diseño no experimental y la muestra fue de 50 participantes, en el que se consideran expertos en investigaciones a fiscales, jueces y abogados especialistas en derecho penal, el resultado obtenido en análisis plantea cuestiones derivadas de la ciberdelincuencia en la era de la Covid-19 y comercialización electrónica. Se concluyó al identificar el problema del cibercrimen en momentos de COVID-19, pudiendo hacer mejor el comercio electrónico otorgando seguridad a la data y eliminando las amenazas producto de la utilización de la tecnología. Entonces, el estudio analiza la problemática de la comercialización electrónica y el cibercrimen en la época del COVID-19.

Según el autor, a efectos de confinamiento como medida seguridad para la salud de las personas, aquellos han recurrido a realizar compras o pagos virtuales para satisfacer sus necesidades, sin embargo, ha sido aprovechado por los ciberdelincuentes para generar enlaces falsos y de esa forma acceder a los datos de los usuarios y afectar su dinero disponible en las tarjetas, determinamos que las entidades comerciales que han implantado esta medida de compra, inviertan en un sistema adecuado de seguridad para detectar estos virus y poder informar a sus clientes de forma oportuna evitando así que dejen de realizar estas compras, ya que, todos tenemos el temor de ser víctima de estos fraudes, aun mas cuando las entidades bancarias no se responsabilizan en la mayoría de las circunstancias de estos delitos.

La teoría del Cibercrimen, indica que un criterio particular para resistirse a esta realidad actual es la circunstancia de que se considere a los sistemas informáticos y el ciberespacio como causales y simples mecanismos en la perpetración de los cibercrímenes, inclusive equiparando a estos últimos ilícitos computacionales o Matellanes, (2019) de conexidad medial a la red para que traten la información, sistemas informáticos y los datos. Tengamos en cuenta que los ilícitos relacionados al internet, contrario sensu de los ciberdelitos, tutelan los bienes jurídicos como el patrimonio económico o la intimidad previamente a la seguridad de los datos, sistemas informáticos e información, tutelados de un modo directo.

Según Roldan (2023), citando a Roxin se establece que en la teoría de la imputación objetiva: el nivel del estudio de este modo de imputación del resultado legal el autor no varía, se requiere considerar que el peligro que se aporta no debiendo valorarse completamente, sin los que tienen que existir en el ciberespacio y generar consecuencias idóneas en el ámbito digital, de forma directa o como consecuencia lógica de los procesos de tratamiento de información o datos a través de los sistemas informáticos.

La teoría del derecho penal e ilícito informático, indica que la problemática de los delitos informáticos, se ha considerado como una circunstancia en nuestra vida, vigente en nuestra economía y realidad social. Aquello a determinado el origen de un conjunto de derechos que engloba que el ordenamiento jurídico tenga que tutelar. En efecto, el criterio fundamental vigente es la búsqueda de una reforma efectiva que controle y supervise el ámbito penal, ya que, el modelo tradicional de castigo no ha brindado un adecuado resguardo.

En los inicios del fenómeno informático para frenar este nuevo modo de delincuencia se usó imágenes o tipos criminales tradicionales y habituales, concretamente vinculado con los ilícitos de propiedad, sin embargo, desde distintas perspectivas se argumenta que no se abarco en totalidad ya que se limitó a crear ilícitos propios vinculados a los ilícitos informáticos. (Leyva, 2021)

A continuación, se desarrolló las categorías de estudio: la suplantación de identidad digital o el phishing, se conceptualiza como una técnica usada por el delincuente para que perpetre sus fraudes, a través del engaño para que se manipulen a las agraviadas, el phishing se considera según la literatura o etimología como un tipo de pesca.

Fue una técnica de ingeniería muy reconocida en el marco de la virtualidad, donde se puede afectar mediante dos modalidades básicas: En primer lugar, es suplantar la identidad del personal del banco con la pretensión de obtener la información confidencial, en segundo lugar, se genera usando una comunicación electrónica, como llamadas tecnológica o correos. (Espinoza,2018)

El Observatorio de Cibercriminalidad-Fraudes Virtuales (2020), en el mismo enfoque, conceptualiza al phishing como una figura delictiva que pretende buscar a los sujetos de derecho con mayor vulnerabilidad en a red. A través de una técnica de ingeniería social, el atacante simula ser una empresa o entidad bancaria para hacer incurrir al usuario en un error.

En el ámbito internacional, la perpetración de este delito aumento significativamente a raíz del desarrollo tecnológico, ya que, el hacker lo han venido perfeccionando, este delito tiene distintas figuras: suplantación, clonación, sustracción de data, introducir virus en el ámbito de las webs o sistemas financieros. Inclusive los Estados como Italia, España, Francia, que tienen una eficiente ingeniería informática con cualquier país de Latinoamérica son atacados pese a sus reformas normativas y sistemas modernos, además con todo ello les resulta complicado enfrentar a la ciberdelincuencia en sus diversas figuras.

El Estado Peruano no estuvo ajeno a esta realidad, ya que, es evidente la falencia que posee para otorgar la protección adecuada a la seguridad informática, Pese a que tenemos a la Ley N°30096 para enfrentar esta figura delictiva, sin embargo, es ambigua y general ya que no especifica, por ejemplo: las figuras de los fraudes y sus penas respectivas. Debido a ello se considera esencial que se aborde el fenómeno del phishing,

donde si bien es cierto, no todos en primer lugar comprenden el significado del delito por su denominación.

En la actualidad, este delito es una figura de fraude informático más lesivo para que la sociedad se desarrolle, ya que, implica que se sustraigan los datos de las tarjetas de crédito, contraseñas, datos personales. (Rosas,2022)

De igual manera, el phishing no representa un riesgo solo para las personas naturales, sino también para las personas jurídicas, las cuales han sido afectadas por esta nueva figura de fraude. En cuanto al origen del término "phishing", Leguizamón explica lo posterior: La palabra proviene de "fishing", que significa pescar. Se utiliza este término porque la pretensión de estafar es "pescar" a usuarios de internet para que divulguen información sensible. Dicho de otro modo, buscan que las personas caigan en la trampa y compartan su información confidencial

Ricra (2020) indicó que hay razones para emplear el término "Ph" en lugar de "F" al referirse a este concepto. Se amerita a merced de que los hackers eran conocidos como "phreaks", término que proviene de "phreaking", el cual hace referencia a la comprensión y análisis de la tecnología moderna. Respecto a los términos "hacker" como "phreaker" siempre han estado interrelacionados, y debido a esta conexión, se utiliza el "ph" para facilitar el reconocimiento de los ciberataques.

El autor cita al jurista Leguizamón, quien describe el phishing de manera sencilla como un procedimiento en el que un ciberdelincuente se pone en contacto con la víctima, generalmente a través de mensajes de texto o correos electrónicos. El delincuente se presenta falsamente como una persona o banco confiable con el fin de obtener información confidencial de la víctima, como contraseñas, claves de acceso a sus estados financieros. Una vez que el delincuente ha obtenido estos datos de modo fraudulento, los utiliza para acceder a las cuentas personales de la víctima y apropiarse de su dinero. Además, el autor señala que la técnica de phishing más común consiste en el envío masivo de correos electrónicos a direcciones de Gmail, Hotmail, entre otras, con el objetivo de engañar a la víctima y lograr que esta proporcione sus datos personales al atacante.

Con el transcurso de los años, la técnica de phishing ha ido perfeccionándose, lo que hace cada vez más difícil identificar un correo falso, facilitando la comisión de este delito. De forma cotidiana, recibimos diversos tipos de mensajes en nuestros correos electrónicos y teléfono. Aunque en muchas ocasiones estos mensajes nos resultan

molestos debido a su obvia falsedad, en otras situaciones podemos distraernos o emocionarnos al recibir una oferta atractiva, conllevando a caer en la trampa y ser víctimas de los ciberdelincuentes.

De manera similar, se presentaron otras figuras de ilícitos informáticos. El “pharming” (otra forma de ataque a los servidores) se basa en redirigir el tráfico en línea hacia un sitio web falso con el fin de perpetrar fraude. Por otro lado, el “vishing” (palabra que surge de la combinación de "voice" y "phishing") es una figura delictiva donde la agraviada recibe correo electrónico donde se le indica llamar a un número telefónico debido a una supuesta emergencia en el banco. Al hacerlo, la persona al otro lado de la línea le solicita a la víctima que brinde sus datos personales, lo cual resulta completamente ilógico.

El autor Cahuasa (2024), señaló que el pharming y phishing están estrechamente relacionados, ya que ambos son tipos de fraudes informáticos que han ganado popularidad en la última década. El objetivo de ambos es obtener los datos personales del usuario (como contraseñas, correos electrónicos, cuentas bancarias) con el fin de causarles un perjuicio económico. No obstante, la principal diferencia radica en el método utilizado para cometer el delito: el pharming introduce un virus en el sistema del usuario mediante el DNS (Domain Name Server), lo que también lo redirige a una página web fraudulenta. En resumen, se puede definir el phishing como un método para obtener información a través de internet, donde el phishing se lleva a cabo a través de correos electrónicos que redirigen al usuario hacia un sitio web falso,

Para Lopez, (2020), argumenta que los tipos de phishing más comunes incluyen: content-injection phishing, spear phishing, pharming, smishing, deceptive phishing, malware-based phishing. El “deceptive phishing” es la forma más frecuente de phishing. Esa figura se basa en enviar masivamente correos electrónicos falsificados que parecen proceder de una entidad legítima, con el objetivo de obtener datos o contraseñas. A nivel mundial, estos correos fraudulentos son extremadamente comunes y cada día miles de usuarios caen en trampas de enlaces engañosos que buscan robarles su dinero.

El malware-based phishing: fue un tipo de virus troyano, donde el procedimiento en primer lugar es mediante un archivo adjunto que infecta la máquina del usuario, posteriormente al usar Google u otro navegador web e ingresa a una página de un banco, se activa de forma inmediata el virus, La credencial que posee cada institución se roban

a través de este malware donde se sustraen los datos de los agraviados quitándole toda la información del banco.

Content-injection phishing. Es una figura delictiva complicada de que se detecte, ya que, el agente que perpetro la operación posee conocimiento de los datos, cuando introdujo el virus donde tiene que transcurrir días o semanas para que se active.

Spear phishing, el spear phishing se asemeja al deceptive phishing. Esta modalidad es más refinada, ya que, conocen a sus objetivos, preferencias y gustos, los correos electrónicos enviados son sofisticados por lo que complican que se detecte, finalmente, la diferencia de que los correos electrónicos que se envían van dirigidos a una determinada persona natural o jurídica.

En estas circunstancias se engaña a la agraviada y aquella va a sufrir un ataque a sus servidores, utilizados para determinar que navegador se usara en el internet, donde es posible su ejecución tanto al servidor estatal y servidor público, En otros términos, cuando la persona desee entrar a sus navegadores se va a redirigir al navegador asignado por el ciberdelincuente para obtener su información personal.

El Smishing, se denomina de ese modo, ya que, el fraude es realizado mediante SMS, con un contenido sugestivo y siendo conciso, de ese modo se logra capturar la atención de la agraviada perjudicando el dinero de la víctima, esta tiene que hacer clic en el link adherido que está en el SMS.

El phishing, en la época digital el phishing, se utilizan los fraudes informáticos donde se incrementó a un grado exponencial en la época de COVID-19. La noticia evidencia el incremento de usuarios que denuncian ser agraviados de estos delincuentes.

No obstante, hasta el momento la ayuda es escasa y el marco jurídico que tenemos respecto a los delitos informáticos es muy general, por ello se genera la siguiente interrogante, ¿qué han hecho las entidades financieras y las instituciones del Estado para prevenir y sancionar estos delitos? (Matos, 2021).

Se tiene algunos consejos como guía para atender a un posible fraude informático:

- a) Informarse respecto a las formas de detectar un SMS de phishing.
- b) No se debe compartir datos, claves, código respecto a nuestras cuentas bancarias.
- c) Desconocer correos o mensajes de remitentes desconocidos.

- d) No aceptar mensajes sospechosos. No se tiene que contestar los correos electrónicos vinculados a cancelar la cuenta de crédito, o un mensaje conexo, se recomienda en primer lugar realizar una consulta adecuada a la entidad bancaria.
- e) En reiteradas oportunidades los falsos mensajes que se reciben no se han personalizado. Contrario sensu, los SMS de los bancos son verídicos ya que, se cuenta con el reconocimiento del remitente.
- f) Instalación de antivirus (actualizado) en laptop, Pc, tablet o cualquier dispositivo.
- g) Tener actualizado el navegador y las aplicaciones de las herramientas tecnológicas, la versión pasada puede que no contenga la medida adecuada de seguridad.
- h) Las contraseñas deben colocarse en entidades financieras.

El otro factor que es la suplantación de identidad, se desarrolla mediante dos formas:

a) Una figura que se emplea para hacer referencia al abuso informático perpetrado por los delincuentes es la suplantación de identidad, utilizada para obtener contraseñas, obtener datos personales y estafar, entre otros. los cibercrimitos el agente aplica el uso de la seguridad informática, suplanta la identidad de una empresa o persona confiable en una comunicación oficial aparente, por ejemplo: las redes sociales, whatsapp, SMS, llamadas telefónicas, email.

Posteriormente al incremento de la cantidad de casos vinculados con la suplantación de identidad, se requiere un método seguro adicional, generando leyes que sancionen el ilícito y una campaña para prevenir y de ese modo socorrer al usuario con la medida técnica del programa.

Secuelas de la Suplantación de Identidad.

- Comercio por Internet.
- Creación cuentas bancarias corrientes.
- Daños financieros: (disponer de tu dinero a su voluntad).
- Daño a la persona.
- Deterioro físico y psicológico.

En numerosas oportunidades, las personas afectadas por la suplantación de identidad no se enteran hasta que el banco detecta movimientos irregulares o sospechosos. Por esta razón, recomendamos que, en caso de perder alguna tarjeta de crédito o identidad, sigas las posteriores recomendaciones.

1. Denunciar: Es la herramienta más eficaz para enfrentarse a los fraudes y las deudas que el atacante pueda haber cometido.
2. Comunicar el robo a tu entidad financiera: Es importante informar a tu entidad financiera lo antes posible y presentar la denuncia correspondiente con la finalidad de determinar las políticas pertinentes

Considerando que los antecedentes de los ilícitos informáticos, en su inicio estaban tipificados en el art. 186. Inc. 3 párrafo dos del Código Penal 1991. Aquella tipificación no era propia de un ilícito autónomo, considerado una agravante del ilícito de hurto. (Bramont- Arias Torres, 2000), actualmente los ilícitos informáticos se regulan en el Capítulo X del Código Penal: los artículos 207-A (interferencia, acceso o copia ilícita contenida en base de datos), 207-B (alteración, daño o destrucción de base de datos), 207-C (circunstancias calificantes agravantes), 207-D (tráfico ilegal de datos), y en las leyes penales especiales.

Respecto a la segunda categoría desarrollamos la criminalidad informática:

Existen normas especiales penales, como la Ley 30096 de delitos Informáticos, la cual se encuentra conformada por 07 capítulos estructurados entre ellos: objeto y finalidad se encuentra en el I capítulo, ilícitos hacia datos y sistemas informáticos II capítulo, ilícitos informáticos de indemnidad y libertad sexual III capítulo, frente a la intimidad y el secreto de las comunicaciones IV capítulo, frente al patrimonio ubicados en el V capítulo, frente a la fe pública VI capítulo, además de disposiciones comunes señalados en el VII capítulo.

Posteriormente, se promulgó la Ley 30171, que modifica la Ley 30096 respecto a ilícitos informáticos. El propósito de esta norma fue alinear la Ley 30096 con los patrones legales del Convenio de Budapest sobre cibercriminalidad. Para ello, se incorporó en los artículos 2, 3, 4, 7, 8 y 10 la posibilidad de cometer delitos de manera deliberada e ilegítima. Las modificaciones introducidas por la Ley 30171 en relación con los delitos informáticos son las siguientes:

Artículo 1º, este artículo introduce modificaciones a los artículos 2º, 3º, 4º, 5º, 7º, 8º y 10º de la Ley 30096, conocida como Ley de Delitos Informáticos. Estos cambios están orientados a actualizar y ajustar las definiciones y sanciones relacionadas con los delitos informáticos, para alinearlas con las nuevas realidades tecnológicas y amenazas cibernéticas.

Artículo 2º, este artículo modifica las disposiciones complementarias finales tercera, cuarta y undécima de la Ley 30096. Estas modificaciones buscan aclarar y especificar mejor las disposiciones finales, asegurando una aplicación coherente y eficaz de la ley en su conjunto.

Artículo 3º, se incorpora el artículo 12 a la Ley 30096. Esta nueva inclusión amplía el alcance de la ley, probablemente introduciendo nuevas categorías de delitos o ajustes procedimentales importantes para fortalecer el marco legal contra la ciberdelincuencia.

Artículo 4º, este artículo realiza cambios en los artículos 158, 162 y 323 del Código Penal. Las modificaciones se centran en ajustar las penas y definir con mayor precisión los delitos relacionados con la actividad informática, reforzando así la capacidad del sistema judicial para responder a los delitos cibernéticos.

Artículo 5º, se incorporan los artículos 154-A y 183-B al Código Penal. Estas nuevas disposiciones probablemente abordan delitos específicos que no estaban claramente definidos en la legislación anterior, proporcionando un marco legal más robusto y completo para enfrentar los crímenes informáticos.

Única disposición complementaria derogatoria, este punto deroga el artículo 6º de la Ley 30096. La derogación puede deberse a la redundancia del artículo con las nuevas modificaciones o a la necesidad de eliminar disposiciones que ya no son aplicables o efectivas bajo el nuevo marco legal.

El perfil del ciberdelincuente en esta modalidad delictiva implica que el agente posea conocimientos y habilidades específicas en el manejo de sistemas informáticos. (Azaola, 2010) Debido a estas cualidades, a menudo se les considera delincuentes de "cuello blanco", quienes presentan las siguientes características:

- a) Contar con amplios conocimientos en informática.
- b) Desempeñar roles clave en su lugar de trabajo, donde se maneja información confidencial (estos se consideran ilícitos ocupacionales, ya que son perpetrados aprovechando el acceso al sistema y el cargo en su centro de trabajo).

Según Marcelo Manson, los delincuentes que cometen ilícitos informáticos no son criminales comunes, sino individuos con conocimientos especializados en informática Manson (2013) Además, señala que quienes perpetran aquellos ilícitos suelen tener

características particulares, como habilidades avanzadas en el manejo de sistemas informáticos, y ocupan posiciones laborales estratégicas donde acceden a información confidencial.

Camacho Losa opina que el perfil de quienes cometen estos delitos no corresponde al de un delincuente común, y describe a los responsables de estas infracciones como trabajadores de confianza de estas instituciones (Camacho, 2020)

De acuerdo a Vives (1996) , el sujeto activo de estos delitos puede ser tanto aquellas personas autorizadas legalmente para ingresar y manejar el sistema (como operadores, programadores u otros), como individuos no autorizados que logran acceder a terminales privadas o públicas.

Gutiérrez y otros, tienen una perspectiva distinta a la anterior y afirman que cualquier individuo puede ser el autor de un delito informático, sin necesidad de tener conocimientos técnicos especializados o cumplir con requisitos personales específicos (Gutierrez, 2019). En nuestra opinión, aunque creemos que el sujeto activo puede ser cualquier persona con conocimientos y habilidades en informática, coincidimos parcialmente en la idea de que el autor del delito debe ocupar un puesto de trabajo que le otorgue acceso a información confidencial. No obstante, no se excluye a aquellos individuos que, aunque no desempeñen un cargo estratégico, puedan ser responsables del delito debido a sus capacidades y conocimientos en informática. Por lo tanto, estos son ilícitos de competencia.

A estos tipos de sujetos se les denomina de diferente manera dependiendo el modo como actúan y que conductas son las que realizan:

- a) **Hackers**; son individuos que, por afición o interés, se especializan en vulnerar programas y sistemas que se consideran clasificados e impenetrables. Se les conoce como delincuentes silenciosos o tecnológicos. Su motivación principal es explorar y entender el funcionamiento de los sistemas informáticos, llevando a cabo estas actividades como un desafío intelectual, sin causar daño alguno, únicamente con el propósito de descifrar y conocer cómo operan dichos sistemas.
- b) Para Siaber (2020), los hackers son individuos que ingresan sin permiso a un sistema de procesamiento de datos de manera remota, sin la intención de manipular, defraudar, espiar o sabotear, sino simplemente como una forma de exploración no

autorizada por placer (Moron, 2019) Según esta definición, un hacker es una persona que accede o interfiere de manera oculta en un sistema informático o en redes de comunicación electrónica, utilizándolos sin autorización o excediendo los límites de acceso permitido.

- c) **Crackers**; son individuos que ingresan a un sistema remoto con el propósito de eliminar datos, interrumpir el servicio a usuarios legítimos y, a groso modo, vulnerar los sistemas, redes informáticas, procesadores, siendo conocidos como piratas cibernéticos.

Analizando los delitos informáticos en la Ley 30096 y su modificación por la Ley 30171, en el Capítulo II se abordan los delitos contra datos y sistemas informáticos. Este capítulo está compuesto por tres principales delitos:

Acceso Ilícito (Artículo 2): Se sanciona a quien accede de manera deliberada e ilegítima a cualquier parte de un sistema informático, vulnerando medidas de seguridad. La pena es de prisión de uno a cuatro años y de treinta a noventa días-multa. La misma sanción se aplica a quien excede lo autorizado en su acceso a un sistema informático.

Atentado a la Integridad de Datos Informáticos (Artículo 3): Este delito penaliza acciones que comprometen la integridad de los datos en un sistema informático.

Atentado a la Integridad de Sistemas Informáticos (Artículo 4): Se castiga a quienes dañan o interfieren con la funcionalidad de sistemas informáticos.

Las modificaciones introducidas por la Ley 30171 refuerzan y clarifican estos delitos, adecuándolos a los estándares internacionales establecidos por el Convenio de Budapest sobre cibercriminalidad, garantizando una mayor protección contra los delitos informáticos.

La violación de la confidencialidad es castigada por esta figura penal de acceso ilícito, que ocurre cuando alguien accede sin permiso a un sistema, infringiendo las medidas de seguridad diseñadas para evitar que personas no autorizadas ingresen a un sistema informático (Española., 2014). El término "acceder" se refiere al acto de entrar o ingresar a un lugar, y en este contexto, implica entrar a un sistema sin la autorización del titular.

Se han realizado diversas reformas en el Código Penal vinculadas con ilícitos informáticos, art. 158, 162, 323 a través del art. 4 de la Ley 30171 (Ley que modifica la Ley de delitos informáticos, Ley N° 30096°) en los posteriores términos:

Artículo 158°, los delitos contemplados en este capítulo son procesables mediante acción privada, excepto el delito señalado en el artículo 154-A. Antes de la modificación, este artículo especificaba que los delitos incluidos en el Capítulo II sobre Violación de la Intimidad se perseguían a través de acción privada. Con la incorporación del artículo 154-A sobre el Tráfico Ilegal de Datos Personales, se establece que la acción penal pública se aplicará únicamente a este nuevo delito.

Artículo 162°, quien, sin justificación, interfiera o escuche una conversación telefónica u otra similar, enfrentará una pena privativa de libertad de tres a seis años. Si el infractor es un funcionario público, la pena será de cuatro a ocho años de prisión, además de la inhabilitación según lo establecido en el artículo 36, incisos 1, 2 y 4.

La pena privativa de libertad será de cinco a ocho años cuando el delito involucre información considerada secreta, reservada o confidencial, según lo establece la Ley 27806 de Transparencia y Acceso a la Información Pública.

Si el delito afecta la defensa, seguridad o soberanía nacionales, la pena será de ocho a diez años de prisión. Además, si el delincuente es parte de una organización criminal, la pena se incrementará hasta un tercio por encima del máximo legal mencionado. Estas modificaciones se realizaron porque la redacción anterior era demasiado general y permitía a los jueces decidir arbitrariamente qué información se consideraba secreta, reservada o confidencial. De ahí la necesidad de especificar las agravantes del delito de interferencia telefónica cuando se trate de información clasificada, según la Ley 27806 de transparencia y acceso a la información pública.

Información Contextual, después de la promulgación de la Ley 30096, (diciembre-2013, se presentó el proyecto de ley 3048/2013-CR, que propone modificaciones al artículo en cuestión. Este proyecto argumenta que la conducta penalizable no ha sido regulada adecuadamente e incluye nuevas agravantes, como las motivaciones detrás de la interceptación.

El artículo 154-A, penaliza a quienes comercializan ilegalmente información privada de cualquier ámbito personal, familiar, patrimonial, laboral, financiero o similar,

con una pena de prisión de tres a cinco años. Si el delito es cometido como parte de una organización criminal, la pena se incrementa hasta en un tercio sobre el máximo legal estipulado. Este análisis pone de manifiesto la intención del proyecto de ley de afinar la legislación existente para abordar de manera más efectiva las conductas delictivas relacionadas con la interceptación y el uso indebido de información personal.

El ilícito de tráfico ilícito de datos personales penaliza el comportamiento (promover, favorecer, facilitar, comercializar, traficar, vender) datos confidenciales, de manera independiente si con estas acciones se generan perjuicios.

Este delito, debido a sus particularidades, tiene una tendencia interna trascendental, ya que incluye un elemento subjetivo que refleja una intención específica de obtener un resultado distinto al normalmente requerido. En efecto, se clasifica como un delito de resultado anticipado, dado que el autor busca un resultado que va más allá de lo estipulado en la tipificación, como lo sería la comercialización, el tráfico, entre otros, de una base de datos. Un ejemplo de esto sería la venta de bases de datos que contienen información personal, como nombres, documentos de identidad, edad, estado civil, dirección, teléfono, ocupación, cargo laboral, salario, entre otros.

Artículo 183-B, este artículo establece que cualquier persona que contacte a un menor de catorce años para solicitar o obtener material pornográfico, o para realizar actividades sexuales con él, será sancionada con una pena privativa de libertad de cuatro a ocho años, además de la inhabilitación conforme a los numerales 1, 2 y 4 del art. 36°.

Suplantación de Identidad (Artículo 9° Ley N.° 30096), en su capítulo VI titulado "Delitos informáticos contra la fe pública", define la suplantación de identidad. Este artículo establece que quien, mediante tecnologías de la información o comunicación, suplante la identidad de una persona natural o jurídica, causando algún perjuicio material o moral, será sancionado con una pena privativa de libertad de tres a cinco años.

En este caso es la identidad digital es el bien jurídico protegido, que se entiende como el conjunto de particularidades que una persona muestra a través de internet, siendo una parte fundamental de su identidad personal, y más específicamente, de sus aspectos psicológicos, sociales y morales. Este delito de suplantación de identidad es falsificado como un ilícito de resultado, ya que no solo es necesario realizar la acción típica, que es suplantar la identidad, sino que además debe seguirse de un resultado distinto que cause un perjuicio. La creación de perfiles falsos en redes sociales sería un ejemplo evidente

(como Twitter, correo electrónico, Facebook) atribuidos a personas físicas o jurídicas con el fin de engañar y dañar a terceros.

Borghello (2020) La identidad se define como el conjunto de atributos y características que distinguen a una persona dentro de la sociedad, ya sea de manera individual o compartida por un grupo o categoría social. Por otra parte, la suplantación de identidad digital puede llevarse a cabo de diferentes modos, aunque siempre con los mismos elementos fundamentales y el mismo objetivo: obtener información personal identificatoria y usarla posteriormente para hacerse pasar por la persona legítima. Estas acciones pueden generar perjuicios tanto personales (como daño al honor, pérdida de reputación, imagen).

La acción del agente pretende en afectar a otra persona, ya sea física o jurídica, lo que significa que tanto individuos como empresas pueden ser perjudicados, siempre que de ese acto se deriven daños materiales. Mientras que el daño material es más fácil de identificar, el daño moral es más complejo, ya que requiere un tipo de valoración diferente.

El ilícito de suplantación de identidad se denomina como suplantación de identidad digital o suplantación de identidad en entornos digitales, ya que aquel ilícito (según el artículo 9 de la Ley N.º 30096) es perpetrado a través tecnologías de la información o de la comunicación. La ley no contempla la suplantación física de una persona, sin embargo; podría ser considerada un delito genérico. Los sujetos son: sujeto activo pudiendo ser cualquier persona natural, y sujeto pasivo viene a ser cualquier persona natural o jurídica.

Según Villavicencio, la tipicidad subjetiva del delito de suplantación de identidad clasifica este crimen como un delito de resultado, ya que no basta con llevar a cabo la conducta típica (suplantar la identidad de una persona, ya sea natural o jurídica), sino que también es necesario que dicha acción resulte en un perjuicio. La pena para este delito es de tres a cinco años de prisión.

Sus agravantes, según el art. 11 de la Ley de Delitos Informáticos (Ley N.º 30096) indica que, si el delito in comento se realiza como perteneciente de organización criminal o haciendo uso de su especial posición de la información en razón de su cargo, con la finalidad de obtener beneficio económico, la pena privativa de la libertad se sitúa por sobre los seis años y medio de pena privativa de la libertad.

IV METODOLOGIA

4.1.- Tipo de Investigación.

Tipo. Es de investigación básica, pues tiene como característica diferencial que genera marco teórico, mediante el desarrollo de categorías de estudio, generando la reproducción de conocimientos respecto a los problemas de la sociedad. Es de tipo básica o sustantiva, también se le denomina de investigación Pura pues quien investiga está interesada por un objetivo crematístico, el interés de conocer y descubrir conocimientos, experiencias; este tipo de investigación es básica pues sirve de fuente a las investigaciones tecnológicas o aplicadas. (Nieto, 2023).

En el presente estudio, se refiere al phishing o suplantación de la identidad digital, y su incidencia dentro de la criminalidad informática en la legislación penal peruana año 2022.

Enfoque cualitativo. – ante una realidad intrínseca, fundamentada en la evaluación y exégesis de quien tiene a cargo el estudio, es imposible la separación de los dos factores primordiales como es conocimiento logrado por el investigador. Siendo el caso de investigación donde el encargado utiliza un procedimiento de análisis de la realidad del problema que se investigó, de manera inductiva mediante la técnica de entrevista e interpretación de los hechos de acuerdo a las experiencias proporcionadas por los colaboradores (Villagómez A. , 2021)

4.2.- Diseño de investigación.

El diseño es fenomenológico, cuya estrategia de desarrollarse es tomando en cuenta los discernimientos o ideas de los colaboradores, partiendo de experiencias habidas y no edificadas por las teorías o saberes, entendiendo otras visiones, sobre una temática en cuestión. (Calle, 2023)

4.3.- Categorías, subcategorías y matriz de categorización.

Categoría uno: El phishing o suplantación de la identidad digital

Categoría dos: Criminalidad informática

Tabla 1: 4.3.- Categorías, subcategorías y matriz de categorización.

Categoría de estudio	Definición conceptual	Subcategoría
Categoría uno: El phishing o suplantación de la identidad digital	Viene a ser una de las técnicas de ingeniería muy conocida en la virtualidad, que puede ser efectuado a través de dos básicas modalidades: la primera es identidad suplantada para conseguir confidencial información.	Orígenes del Phishing Los tipos de Phishing Suplantación de identidad Clases de suplantación Consecuencias Delitos Informáticos Antecedentes Jurisprudencia Tipo penal del phishing El ciberdelincuente Tipos
Categoría dos: Criminalidad informática	La criminalidad informática utiliza diferentes métodos, técnicas de ingeniería social (redes sociales), cuyo fin es capturar información personal o desarrollar actividades fraudulentas en deterioro de bienes jurídicos pluriofensivos gozando protección penal mediante legislación nacional especial Ley N°30096 y su modificatoria N.º 30171.	Delincuencia informática Clases La ley 30096 y su modificación por la ley 30171 Reformas del Código Penal

4.4.- Escenario de estudio.

Tiene la característica de ser accesible, es decir posibilita que mediante negociaciones logre ingresar y obtener la información, con fuentes de información que reúnen las circunstancias que la investigación necesita. (Villavicencio M. L., 2023)

El escenario de estudio está conformado los Juzgados Penales (Poder judicial) de Chiclayo.

4.5.- Participantes

Los participantes, vienen a ser quienes desempeñan una función en determinada investigación, de forma directa o indirecta, haciendo sus aportes mediante acciones o ideas que de alguna manera van posicionando la idea del investigador. (Villagómez A. , 2021)

Los participantes de la presente investigación, serán: el especialista Magister (01) quien valora el instrumento de la entrevista, y 10 abogados profesionales de derecho penal quienes son colaboradoras en desarrollar la entrevista.

4.6.- Técnicas e instrumentos de recolección de datos.

Técnicas

Técnica de Análisis documentales. La más usual en el procedimiento de investigación, utilizada en el análisis de ideas desarrolladas en textos bibliográficos, revistas científicas, periódicos, etc. Se podría decir que viene a ser la técnica precisa orientada a una descripción muy objetiva, ordenada y de calidad. El instrumento es la ficha de análisis documental: la misma que permitirá sistematizar datos, contenidos, comentarios en anotación, para lograr una interpretación adecuada dentro del informe de tesis (Martinez, 2023)

La Técnica de la observación. - La observación una de las principales sistemáticas de indagación social. Es un procedimiento antiguo, pero también confiable, nos ha permitido recoger fichas, datos que luego son verificados en la hipótesis. El instrumento de la técnica de la observación, es la lista de cotejos, la misma que permitirá sostener la secuencia de la investigación; con este instrumento se procura la objetividad, mediante un orden respecto a los acontecimientos que suscitaron o se encontraron dentro de la investigación. (Hernandez, 2021)

Técnica de la entrevista, es una técnica de investigación directa o de campo que se da en una interacción entre el entrevistador y entrevistado, considerada como forma

cotidiana de comunicación y convivencia, siendo necesaria una programación, previsión y su ejecución. La considera como conversación formal entre entrevistador y entrevistado, pudiendo ser estructurada, semiestructurada, no estructurada o grupal. **El instrumento**, es la ficha de entrevista debiendo ser llenada con datos específicos y amplios. Las respuestas se reproducen tal cual las provee el entrevistado, ante ello, se plantean en orden mismo (González, 2022)

4.7.- Procedimientos de recolección de datos e informaciones:

Mediante la observación, se recabaron datos visuales, como son la problemática existente en diferentes sectores, (Comisarías, ver las denuncias respecto a los delitos que se estudian). En el análisis documental, se seleccionaron libros, para revisar la bibliografía y jurisprudencia respecto al tema que se investiga, así mismo se buscaron tesis precedentes, para obtener los antecedentes de estudio que forman parte del desarrollo del presente tema.

En la entrevista, se recopilaban las ideas y conocimientos transcritos en un documento plasmado con un formato, el mismo que luego se analizará, para hacer un estudio general de todas las entrevistas y se realizará una discusión de resultados.

4.8.- Validez y confiabilidad

Este aspecto está desarrollado por el Especialista Magister o maestro al momento de revisar el instrumento y emitir su informe de valoración.

4.9.- Criterios de Rigor científico.

a) Eficacia. – es la exégesis, señalado en columna esencial de una investigación cualitativa, **b) valor de la verdad**, viene a ser indicar las problemáticas y los contextos vividos por los participantes tal cual son expresados por ellos; y **c) Confidencialidad.** - consiente encontrarse en el rol de aquel que realiza la investigación, además permite la identificación de los logros y restricciones. (Fernandez, 2021)

4.10. – Aspectos éticos

Se mencionó diversos criterios, señala Naranjo (2023) las fuentes éticas y normativas para la ejecución de la investigación relaciona con las personas: **a) Justicia** referida a lo imparcial en la distribución de derechos y obligaciones. Discreción para estar atentos respecto a una acción ética o no, observando desde la óptica justa **b) Autonomía.** – representa los niveles de capaz que una persona debe sostener para tener consideración de objetivos individuales respetando y actuando una orientación de las disposiciones que logre decidir.

IV.- RESULTADOS

4.1.- De la entrevista

De acuerdo al objetivo general: Determinar la incidencia del ilícito de Phishing o suplantación de la identidad digital, dentro de la criminalidad informática en la legislación penal peruana año 2022. se formuló la siguiente pregunta: ¿Qué opinión le merece, la incidencia del delito el Phishing o suplantación de la identidad digital, la manera que viene creciendo estos delitos, y las normas penales de nuestro país para hacer frente a este problema?

Tabla 2:
Objetivo general

Entr. 01	Entr. 02	Entr. 03	Entr. 04	Entr. 05
A pesar de que el delito de phishing o suplantación de identidad digital es una preocupación, en Perú se está adaptando progresivamente la legislación conforme a las normas internacionales, con el fin de prevenir, investigar y sancionar estos actos ilícitos y a los responsables. La normativa abarca diversos temas, tales como el uso de tecnologías de la información y comunicación (TIC), las medidas para proteger los datos y sistemas informáticos, la tipificación penal de conductas delictivas y los procedimientos	Uno de los propósitos del phishing es engañar al receptor para que lleve a cabo la acción deseada por el atacante, como proporcionar información financiera, credenciales de acceso al sistema u otros datos estrictamente privados. aumentando cada día debido a la ignorancia digital de la mayor parte de la población, más aún de las personas de edades avanzadas, aprovechando el desconocimiento a la hora de navegar por internet; careciendo de normas estrictas	La ley N.30096 (ley de delitos informáticos) nos permite salvaguardar nuestra identidad de hoy en día que se ve apretada por diversos delitos que se cometen en el ciberespacio, sin embargo, esto no erradica la delincuencia ya que cada día se incrementan los delitos informáticos en nuestro país	El delito de phishing o suplantación de identidad digital es en sí una preocupación significativa, debido a su creciente incidencia y los riesgos asociados para la seguridad y privacidad de las personas en el entorno digital. Este tipo de delito implica el uso de técnicas fraudulentas para obtener información confidencial, como contraseñas, números de tarjetas de crédito o datos personales,	El phishing, también conocido como suplantación de identidad digital, es una de las modalidades delictivas más reportadas, según los registros. Este delito implica la creación de sitios web falsos, especialmente de instituciones bancarias, con el propósito de engañar a los usuarios y obtener sus datos personales y contraseñas de servicios financieros. Los estafadores utilizan esta información para realizar

que deben seguir las autoridades competentes para perseguir y sancionar eficazmente los delitos cibernéticos. Actualmente, existe una ley aprobada que reduce la duración de las condenas.	que paralicen el avance de esta nueva modalidad de estafa, robo	mediante el envío de correos electrónicos, mensajes de texto u otros medios de comunicación falsificados que logran vulnerar la seguridad de que creemos tener en cuanto a los medios en que realizamos transacciones económicas. Asimismo, en nuestro ordenamiento jurídico, existen normas penales que buscan hacer frente a este problema, es así que, la legislación cuenta con disposiciones que penalizan conductas relacionadas con el phishing y la suplantación de identidad digital, principalmente en el marco del Código Penal y otras normativas específicas en materia de delitos	transferencias bancarias ilegales y llevar a cabo fraudes cibernéticos. En cuanto a las normas penales para hacer frente a este delito me parecen que deberían ser más severas ya que realizan diversos perjuicios a las víctimas, obteniendo información personal. En la actualidad la pena privativa de libertad es no menor de tres ni mayor de cinco años.
--	---	---	--

			informáticos, con el propósito de disuadir y sancionar las acciones maliciosas realizadas en el ámbito virtual, como la Ley N.º 30096.	
Entr. 06	Entr. 07	Entr. 08	Entr. 09	Entr. 10
El phishing, o suplantación de identidad digital, ha experimentado un notable crecimiento en los últimos años, especialmente con el aumento de los delitos asociados a fraudes informáticos durante la pandemia del COVID-19. Las normas penales de nuestro país deben contemplar estas diversas modalidades delictivas para poder enfrentar de manera efectiva este problema, aplicando penas acordes a la gravedad del delito y considerando el daño ocasionado a la víctima.	Que, el delito de phishing se viene desarrollando de una manera incontrolable, de modo tal que cuesta trabajo para los especialistas detectarlo. Y si lo hacen cuando ya se ha cometido múltiples robos de identidad como cuentas bancarias, y frente a ello nuestras normas penales deben fortalecerse modificándose y estableciendo penas más drásticas a todas esas personas que cometen este tipo de delitos.	Estos delitos informáticos, en los cuales consiste en la clonación de sitios web, principalmente de los bancos, con la finalidad de obtener información personal de los usuarios como claves, DNI, nombres, etc, en la actualidad están aumentando debido que muchas personas que tienen acceso al internet no saben usarlo adecuadamente, en muchos casos son personas ya adultas que “caen” en la trampa de que ingresen a tal sitio web para ganar un “dinero extra”. En nuestro país tenemos la Ley	Es lamentable, debido que cada vez aumenta los delitos de Phishing o suplantación de identidad, y a pesar de los grandes esfuerzos que el Estado realiza para combatir con dicho delito, los delincuentes buscan como a dé lugar, la manera se seguir optando por nuevas modalidades para llevar a cabo su cometido; no obstante, es rescatable la atención puesta y la dedicación que por hoy brinda el Estado para combatir con este problema que cada día asecha más.	

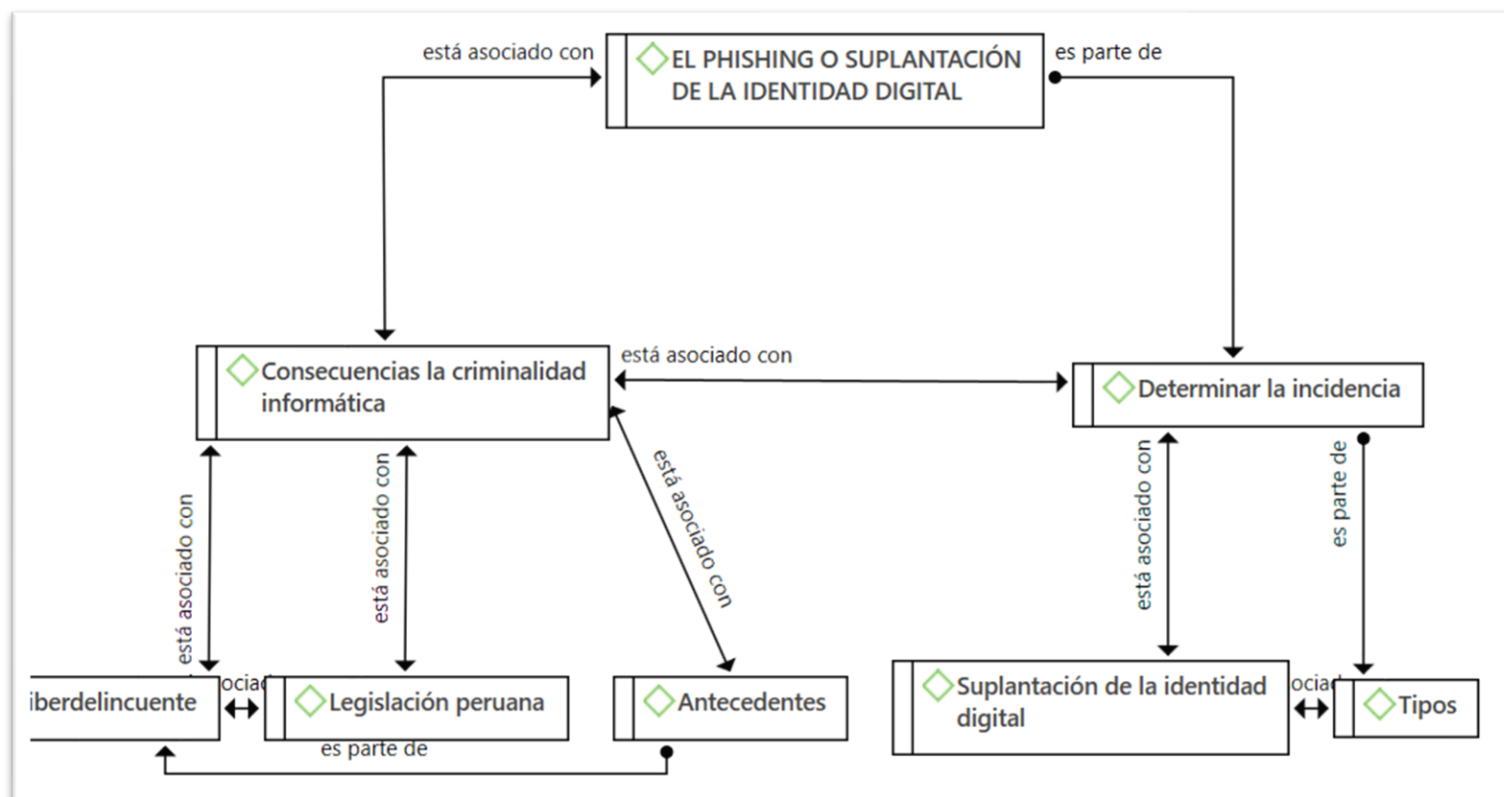
N° 30096 en su
ART. 09 que nos
habla de la
sanción donde
va de 3 hasta 5
años de pena
privativa de
libertad, a
aquellas
personas. Sin
embargo, en la
práctica cuando
uno denuncia
estos tipos de
delitos muchas
veces terminan
siendo
archivados por
falta de pruebas,
es muy
lamentable que
no haya más
información y/o
legislación que
sancione de una
manera eficaz y
efectiva este tipo
de delitos.

De los profesionales en materia penal que han sido entrevistados, se han obtenido de manera global los siguientes datos:

Nueve de los diez entrevistados han indicado desde su conocimiento jurídico en materia penal: que el delito de Phishing está teniendo un evidente crecimiento y desarrollo, además es muy complicado enfrentarlo, inclusive para los especialistas, debido a que el ciberdelincuente aplica técnicas de ingeniería informática con la finalidad de obtener los datos personales de los usuarios con la finalidad de suplantar su identidad. Si bien es cierto, se encuentra vigente la Ley 360096 que sanciona este delito, no ha sido eficaz debido a que no ha conseguido frenarlo.

Resultados de las categorías y subcategorías del objetivo general.

Del objetivo general se han obtenido la relación de categorías de relación, pertenencia y asociación de acuerdo a las entrevistas realizadas, las mismas que han sido llevadas en el aplicativo Atlas ti, arrojando el siguiente esquema:



De acuerdo al objetivo específico primero: Describir los aspectos doctrinales y jurídicos de delitos informáticos en la legislación peruana; se formula la siguiente pregunta: ¿considera usted, que existe suficiente jurisprudencia respecto a delitos informáticos en nuestro país?

Tabla 3:
Objetivo específico uno

Entr. 01	Entr. 02	Entr. 03	Entr. 04	Entr. 05
Considero que, en nuestro país, aun no existe suficiente Jurisprudencia sobre los delitos informáticos, ya que solo establecen muy pocas normas, mucho más en nuestro código	No, actualmente la mayoría de la población carece de conocimiento respecto a las medidas a tomar después de caer en el mencionado Phishing, coadyuvando ello, a la falta de preceptos jurídicos vigentes que hagan referencia al mencionado ciberdelito.	Considero que existe jurisprudencia respecto a los delitos informáticos, pero no la suficiente como para resolver los problemas suficientes de esta índole en el ámbito legal	Considero que actualmente no existe una jurisprudencia suficiente a pesar de los casos que se han venido presentando en cuanto a esta modalidad de delitos informáticos; sin embargo, es importante que las autoridades y entidades competentes en nuestro país continúen fortaleciendo las medidas de prevención, investigación y persecución de los delitos de phishing, así como también la promoción de la educación y concientización sobre la seguridad cibernética entre los ciudadanos. Además, que el desarrollo y actualización	No

constante de la legislación en concordancia con los avances tecnológicos son fundamentales para abordar eficazmente este desafío en el ámbito digital.

Entr. 06	Entr. 07	Entr. 08	Entr. 09
En la legislación peruana, existe suficiente jurisprudencia respecto a delitos informáticos. Verbigracia la Ley N° 30171, Ley de Delitos Informáticos, promulgada en el año 2014. Esta legislación aborda diversas modalidades de delitos informáticos, como fraudes electrónicos, suplantación de identidad, difusión de pornografía infantil a través de medios electrónicos, entre otros. Además, se ha creado la División de Investigación de Delitos de Alta Tecnología (DIVINDAT). Esta unidad especializada se encarga de casos abordados de ciberdelincuencia, incluyendo fraudes electrónicos, difusión de pornografía infantil, entre otros delitos que	al ser delitos que se han desarrollados con mayor fuerza durante los últimos años, no existe jurisprudencia suficiente como para hacer frente a ello y así poder prevenir este tipo de delitos.	En nuestro país no hay mucha jurisprudencia respecto a este delito y menos una legislación donde se sancione aquello.	No, en razón que es un delito “relativamente nuevo”, siendo que hace pocos años ha tomado gran relevancia en nuestra legislación.

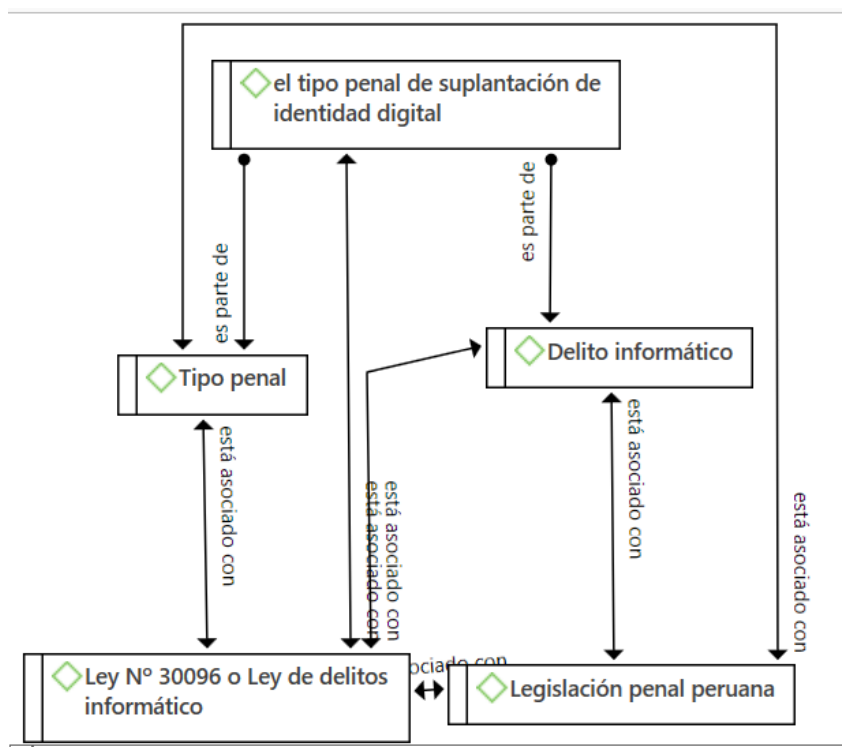
involucran el uso de tecnologías de la información.

De los profesionales en materia penal que han sido entrevistados, se han obtenido de manera global los siguientes datos:

Nueve de los entrevistados consideran que se carece de una de las fuentes más importantes del derecho que es esencial para enfrentar esta problemática, es decir, no contamos con suficiente jurisprudencia respecto al delito de Phishing, otro punto de vista el que han podido coincidir es que la causa de la precaria jurisprudencia se debe a que se están enfrentando a un delito nuevo. Finalmente, la postura de un entrevistado fue que las autoridades y e instituciones competentes no están haciendo un desempeño adecuado de sus funciones para la prevención, investigación y sanción de este delito que se está quebrantando el derecho a la propiedad. Frente a ello, aquella postura concierne con nuestro objetivo que es describir los aspectos doctrinales y jurídicos de delitos informáticos en la legislación peruana, como complemento.

Resultados de las categorías y subcategorías del objetivo general.

Del objetivo específico primero, desde las entrevistas y opiniones de los entrevistados la relación existente entre categorías y subcategorías entre la que se señala son: de pertenencia y asociación, las mismas que han sido llevadas en el aplicativo ATLAS.PI, arrojando el siguiente esquema:



De acuerdo objetivo específico segundo: Desarrollar el tipo penal de suplantación de identidad digital en la legislación penal peruana, se formuló la siguiente pregunta: ¿se encuentra adecuado el tipo penal de suplantación de identidad digital en la legislación penal peruana?

Tabla 4:
Objetivo específico dos

Entr. 01	Entr. 02	Entr. 03	Entr. 04	Entr. 05
Según la Ley N° 30096 o Ley de delitos informáticos, en su artículo 9°, si está establecido, pero como sabemos bien acierto, hay muchos vacíos, que no está especificado claramente.	Si, en parte, ya que la falta de capacitación respecto a la aplicación de las medidas coercitivas frente al mencionado delito informático, no ayudan a la correcta aplicación de sanciones penales.	Si se encuentra adecuado el tipo penal de la legislación peruana, tal y como se indica en el art 9 de la ley N.30096, sin embargo, sería bueno que se concrete más fundamentación jurídica en cuanto a este tema que aún sigue latente para que de esta forma aún se tomen las medidas pertinentes.	Considero que, la legislación penal peruana debería abordar de manera clara y exhaustiva las diversas formas de suplantación de identidad en el entorno digital, contemplando sanciones proporcionales a la gravedad de este delito y medidas específicas para proteger los derechos de las víctimas; por lo que, es importante y necesario que la normativa se mantenga actualizada para adaptarse a los cambios de la realidad tecnológica, pues al tener la Ley N.º 30096, considero que no es suficiente, debido a que hoy en día con los hechos	SI

delictivos que se presentan con ciertas particularidades no resultan ser atendidas para su prevención de manera oportuna y eficaz.			
Entr. 06	Entr. 07	Entr. 08	Entr. 09
El tipo penal de suplantación de identidad digital en la legislación penal peruana se encuentra adecuadamente establecido. La Ley N° 30171, Ley de Delitos Informáticos, contempla disposiciones para sancionar conductas delictivas relacionadas con el uso indebido de tecnologías de la información y comunicación, incluyendo la suplantación de identidad. Esta legislación aborda la usurpación de identidad en el ámbito digital, estableciendo las circunstancias que pueden ser penalizadas por delitos ya establecidos para el uso de falsa	Nuestro ordenamiento lo tipifica dentro de los delitos informáticos, a la suplantación de identidad. Esta lo desarrolla más en la ley 30096, ley publicada el 10 de marzo del 2014.	No, hay poca información tanto para abogados como para la ciudadanía respecto a este nuevo delito, hay una que otra ley, pero terminan siendo letra muerta.	No. En nuestra legislación se encuentra regulado el tipo penal de suplantación de identidad, empero, suplantación de identidad digital, no

identidad.
Asimismo, la
jurisprudencia
existente en el
país ha
contribuido a la
interpretación y
aplicación de las
normas
relacionadas con
la suplantación
de identidad
digital, lo que
brinda un marco
legal
sólido para
abordar este tipo
de delitos
informáticos.

De los profesionales en materia penal que han sido entrevistados, se han obtenido de manera global los siguientes datos:

Siete de los diez entrevistados manifiestan que el delito de suplantación de identidad si se encuentra regulado en la Ley 30096 en el artículo 9, sin embargo, consideran que tienen que abordar de manera más precisa y exhaustiva las diferentes formas de suplantación de identidad.

Dos de los diez entrevistados argumentan que en nuestra legislación se encuentra regulado la suplantación de identidad, mas no, la suplantación de identidad digital, en efecto, nos estamos enfrentando a ese vacío legal que tiene que regularse con celeridad.

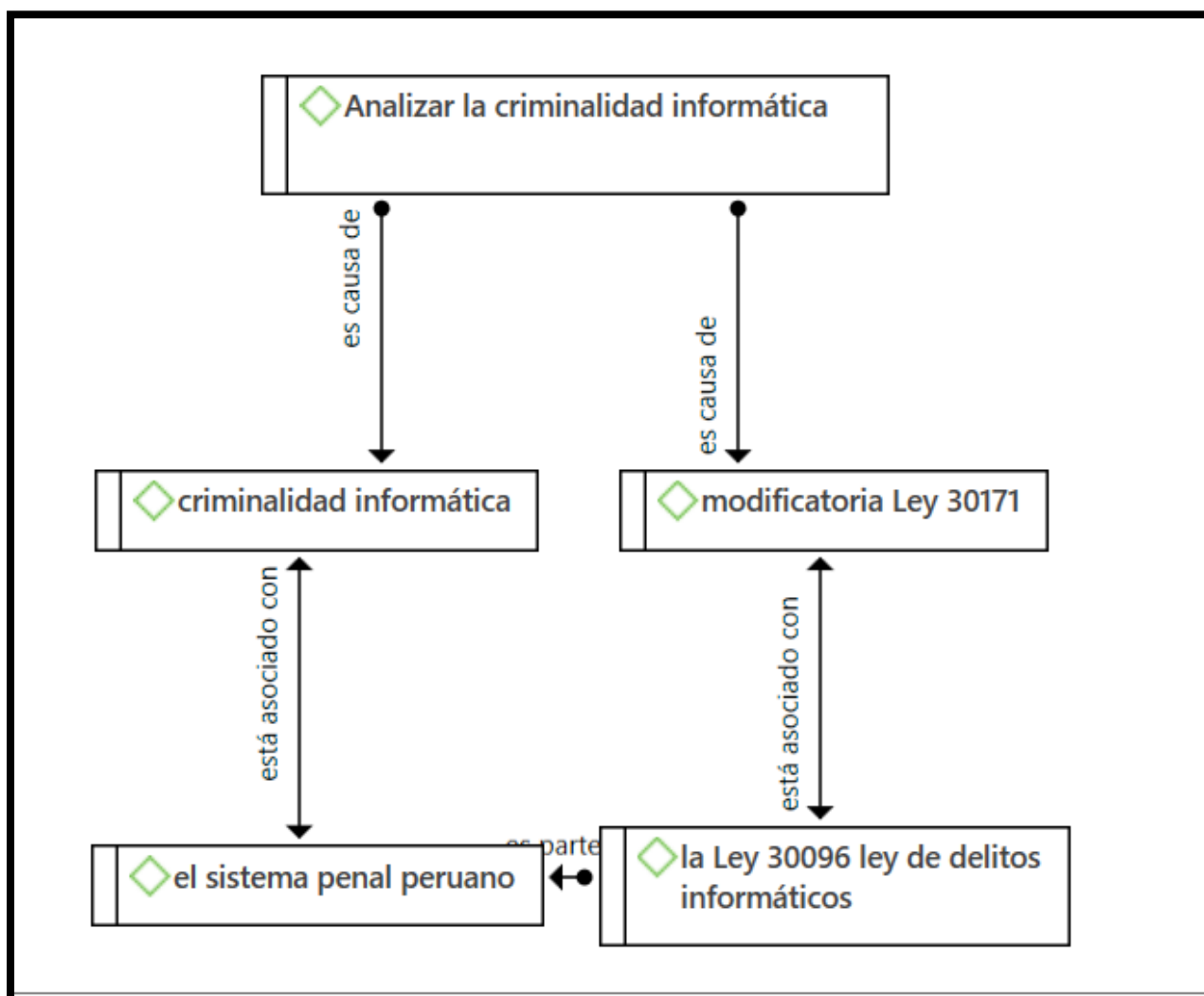
Frente a ello, aquella postura concierne con nuestro objetivo que es Desarrollar el tipo penal de suplantación de identidad digital en la legislación penal peruana.

Un dato esencial para enfrentar este delito, es que, no solamente es tarea de las autoridades crear una ley o modificarla para aumentar su pena, sino, las empresas del rubro de telecomunicaciones deben tener mejores políticas para prevenir este ilícito, por ejemplo: Las empresas dedicadas a la venta de celulares en los últimos años están vendiendo chips con la identidad de otra persona y esto se presta a que de manera más sencilla se apropien de la información personal del usuario. Es por ese motivo El coronel PNP Huamán Santamaría, jefe de la División de Investigación de Delitos de Alta Tecnología (Divindat) de la Policía Nacional del Perú en el periodo 2022 considero necesario que Osiptel, como ente regulador,

ponga mayor énfasis en la verificación de la identidad por parte de los proveedores de telecomunicaciones.

Resultados de las categorías y subcategorías del objetivo general.

Del objetivo específico segundo, desde las entrevistas y opiniones de los entrevistados la relación existente entre categorías y subcategorías entre la que se señala son: de pertenencia y asociación, las mismas que han sido llevadas en el aplicativo ATLAS.PI, arrojando el siguiente esquema:



De acuerdo al Objetivo específico Tercero: c) analizar la criminalidad informática en el sistema penal peruano mediante la ley 30096 ley de delitos informáticos y su modificatoria Ley 30171”, se formuló la siguiente pregunta: ¿Qué señala la Ley 30096 ley de delitos informáticos y su modificatoria Ley 30171, respecto a la criminalidad informática en el sistema penal peruano?

Tabla 5: Objetivo específico tres

Entr. 01	Entr. 02	Entr. 03	Entr. 04	Entr. 05
Que, aunque la Ley 30171 busca alinear de manera más precisa la descripción de las conductas delictivas con el Convenio, que identifica cinco grandes grupos de ciberdelitos según los bienes jurídicos, a saber: los datos y sistemas informáticos, la indemnidad y libertad sexuales, la intimidad y secreto de las comunicaciones, el patrimonio, y la fe pública. Los ciberdelitos contra los datos y sistemas informáticos incluyen el acceso no autorizado, los atentados a la integridad de los datos y sistemas informáticos, y el uso indebido de mecanismos y	Esta ley está diseñada para prevenir y sancionar las actividades ilícitas que comprometen los sistemas y vulneran los datos informáticos confidenciales y otros bienes jurídicos de las personas. Su objetivo principal es prevenir y castigar las conductas ilegales que afectan los sistemas, los datos informáticos y el secreto de las comunicaciones.	Si bien es cierto, es una ley bastante concreta y entendible razón por la cual, cabe precisar que el sistema legal peruano en el peligro que los menores de edad pueden pasar debido a los delincuentes y a sus artimañas, por otro lado, se enfoca en temas bancarios, que es otro tema latente en nuestro país, es por ello que debe indicar que siendo temas de gran importancia merece la atención debida de nuestras autoridades y potenciar la ley respecto al	Señalan y establecen una serie de disposiciones específicas para prevenir, sancionar y perseguir delitos informáticos, incluyendo aspectos como el acceso no autorizado a sistemas informáticos, interceptación de comunicaciones, difusión de virus informáticos, entre otros. También contemplan medidas para proteger la seguridad de la información y para promover la cooperación internacional en la lucha contra los delitos informáticos. Es preciso decir que, esta ley con su modificatoria es un	La ley establece que el simple acceso a Internet puede exponer a los usuarios a una serie de delitos, los cuales se cometen utilizando nuevas tecnologías y avances digitales, violando así la confidencialidad, la integridad y la información. Además, esta normativa ha incluido varios delitos informáticos, como la interceptación de información y la suplantación de identidad, entre otros, asignándoles sanciones penales con el objetivo de prevenir y combatir su ejecución.

dispositivos informáticos.	tema antes mencionado	avance significativo en la legislación penal peruana, ya que reconoce la importancia de regular la criminalidad informática en un entorno tecnológico en constante evolución. Sin embargo, es importante siempre consultar las fuentes oficiales para obtener información actualizada y detallada sobre cualquier disposición legal específica es aplicable a cierto presunto hecho delictivo.	
Entr. 06	Entr. 07	Entr. 08	Entr. 09
La Ley N° 30096, Ley de Delitos Informáticos, y su modificatoria Ley N° 30171, establecen disposiciones específicas para abordar la criminalidad informática en el sistema penal peruano. La Ley N° 30171 modificó varios artículos de la Ley N°	Que cuenta con la finalidad de prevenir y castigar las ilícitas conductas, que perturban los datos y sistemas personales.	La normativa N° 30096 y sus modificaciones en ley N.°30171 señala el agravante y la pena cuando el agente acceda ilegítimamente al informático sistema quebrantando los procedimientos de seguridad.	Señala que son conductas ilegales que afectan los sistemas y datos informáticos, así como otros bienes jurídicos de naturaleza penal, utilizando tecnologías de la información y comunicación, vulnerando así, medidas de seguridad establecidas, tan

30096, ampliando y actualizando el marco legal para abordar de manera más efectiva la criminalidad informática en el país. Estas disposiciones legales brindan un marco sólido para la persecución y sanción de delitos informáticos en el sistema penal peruano.	sólo para obtener ventajas de otros individuos. Por ello, el estado busca a través de ambas normas, proteger y sancionar aquellas conductas realizadas por personas ajenas
---	--

De los profesionales en materia penal que han sido entrevistados, se han obtenido de manera global los siguientes datos: Nueve de los diez entrevistados, manifestaron la siguiente postura “La modificatoria de la Ley 30171 es más específica para adecuar de una mejor manera la descripción de los comportamientos delictivos, estableciendo cinco segmentos de ciber delitos respecto a los bienes, haciendo énfasis en que el delito en cuestión vulnera los datos y el sistema informático, abusa de dispositivos y mecanismos informáticos, viola el secreto de las comunicaciones, y atenta contra patrimonio”. Frente a ello, aquella postura concierne con nuestro objetivo que es analizar la criminalidad informática en el sistema penal peruano mediante la ley 30096, ley de delitos informáticos y su modificatoria Ley 30171. El Análisis de la modificatoria de la Ley es el siguiente: la nueva Ley modifica los artículos 2,3,5,7,8 y 10, incorporando la calidad de ilegítima y deliberada respecto de los ilícitos de acceso ilícito: atentados contra la integridad del sistema de interceptación de datos y fraude informático, además se esclarece el abuso de mecanismos de esta naturaleza especificando delitos interceptación telefónica o interceptación de datos.

Resultados de las categorías y subcategorías del objetivo general.

Del objetivo específico tercero, desde las entrevistas y opiniones de los entrevistados la relación existente entre categorías y subcategorías entre la que se señala son: de pertenencia y asociación, las mismas que han sido llevadas en el aplicativo ATLAS.PI, arrojando el siguiente esquema:

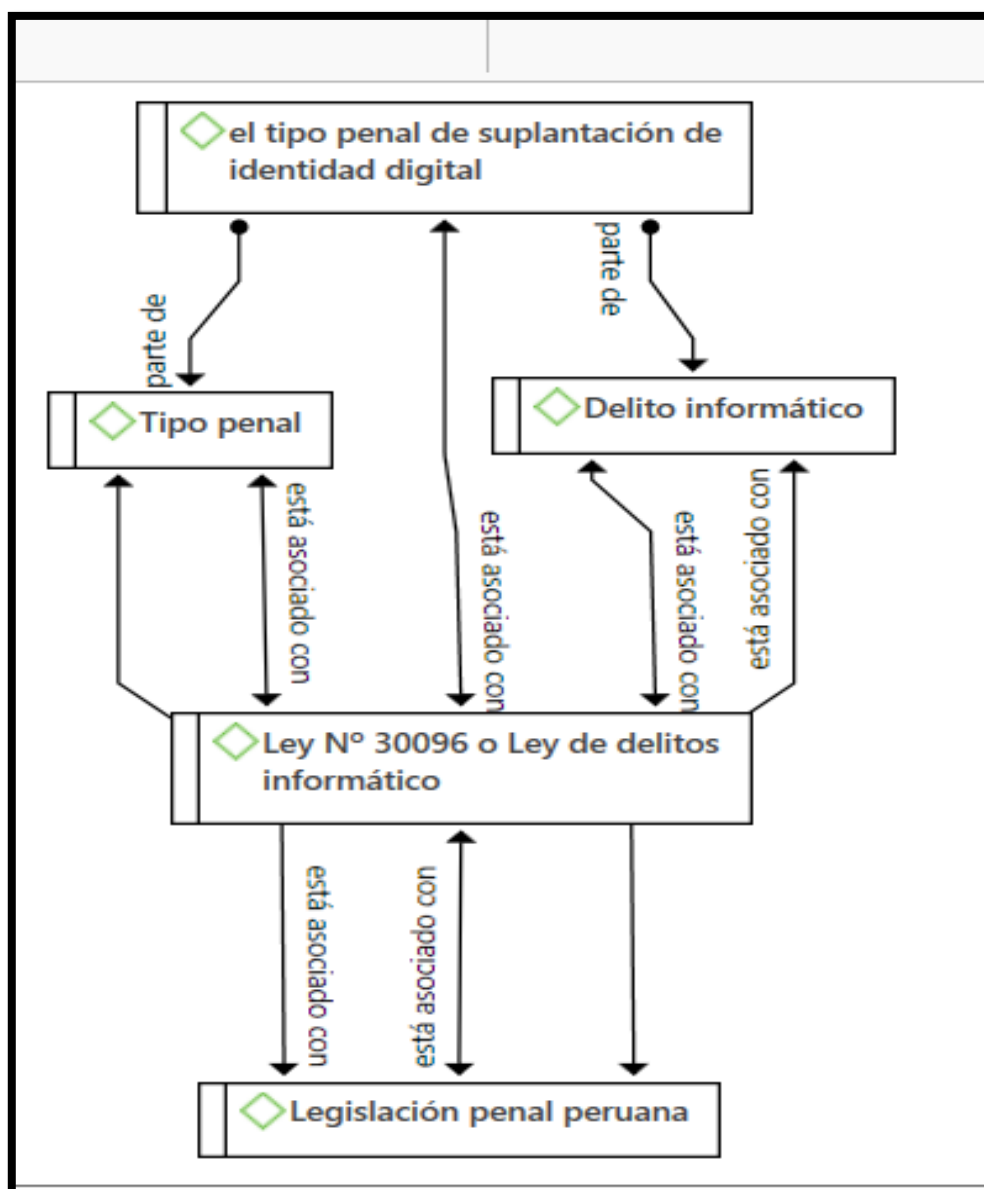
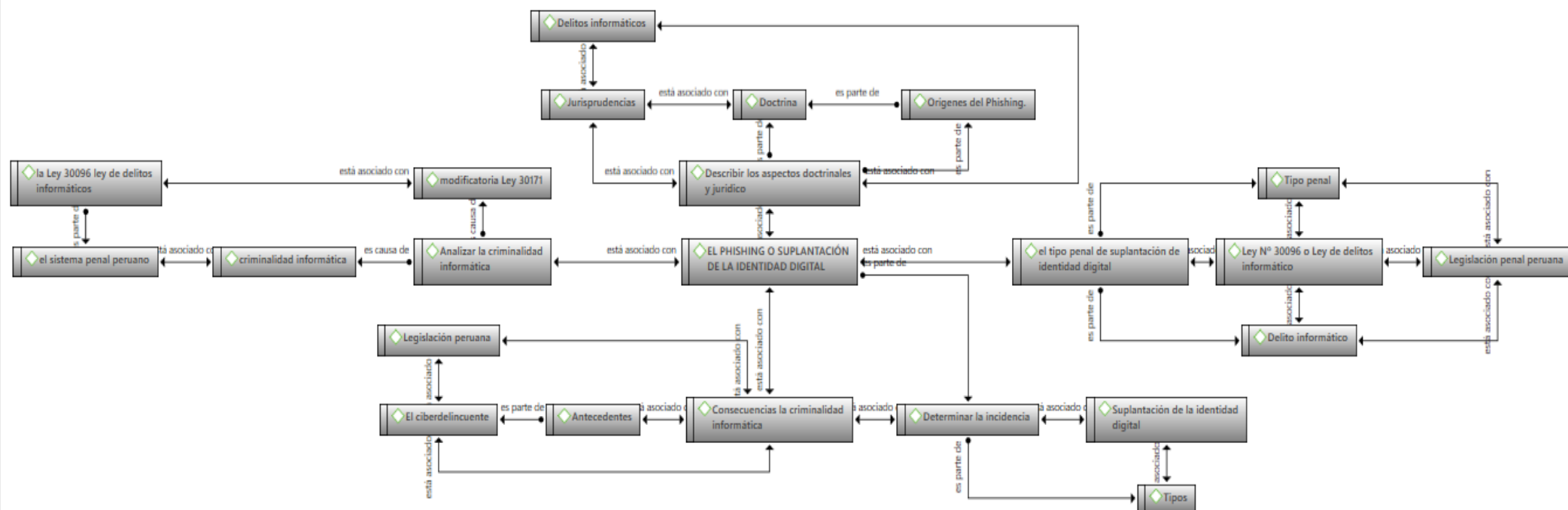


Diagrama global de objetivos:



4.2.- Discusión de resultados

De acuerdo al objetivo general: Analizar el Phishing o suplantación de la identidad digital, y su incidencia dentro de la criminalidad informática en la legislación penal peruana año 2022,

En las entrevistas

se formuló la siguiente pregunta: ¿Qué opinión le merece, la incidencia del delito el Phishing o suplantación de la identidad digital, la manera que viene creciendo estos delitos, y las normas penales de nuestro país para hacer frente a este problema?

Nueve de los diez entrevistados han indicado desde su conocimiento jurídico en materia penal: que el delito de Phishing está teniendo un evidente crecimiento y desarrollo, además es muy complicado enfrentarlo, inclusive para los especialistas, debido a que el ciber delinciente aplica técnicas de ingeniería informática con la finalidad de obtener los datos personales de los usuarios con la finalidad de suplantar su identidad. Si bien es cierto, se encuentra vigente la Ley 360096 que sanciona este delito, no ha sido eficaz debido a que no ha conseguido frenarlo.

Frente a ello, aquella postura concierta con nuestro objetivo que es analizar el Phishing o suplantación de la identidad digital, y su incidencia dentro de la criminalidad informática en la legislación penal peruana año 2022 y para complementar la información recopilada hacemos mención que: una de las figuras en las que se presenta el Phishing es a través de un mensaje de texto a los celulares, aquello se debe a que en la actualidad todas las personas manejamos este objeto en todo momento del día, esto es aprovechado por los ciber delincuentes, donde describen en el SMS promociones de lotería, de premiaciones, entre otros, con la finalidad de emocionar al usuario e ingresen al link que se encuentra en el mensaje y de esa forma apropiarse de su identidad personal.

En los antecedentes

Encontramos la investigación de Solís (2020), que analiza el robo informático en México, como nueva modalidad llamada phishing”, indicando que, esta figura antijurídica es muy incidente y se genera con un modus operandi para robar información bancaria (robo digital), reportando en México un promedio de 71.5% de ilícitos informáticos. Lo que hace concluir

que se debe mejorar las sanciones penales a este delito, en vista que su incidencia se da por que la delincuencia utiliza innovaciones tecnológicas y futuras modalidades delictivas.

El estudio del investigador Solís, se condice con el presente objetivo que analiza la incidencia del Phishing (que es la suplantación de identidad) pues tanto en la realidad problemática que se expone en México también se presenta en nuestra sociedad peruana, pues los delitos informáticos vienen siendo cometidos de manera más constante. Al igual que la posición de Solís, en su investigación, coincide con la recomendación de buscar que las sanciones penales se analicen y se endurezcan para evitar la incidencia de este delito.

La investigación de Vílchez, (2020), quien señala que la ciberdelincuencia viene en incremento dejando abiertamente los conflictos de investigación y el juicio de estos ilícitos, donde no existe capacitación policial y el no uso de especializadas técnicas, como resultado señala que ante la crisis covid-19 sufridas por los países del mundo, se incrementó el uso de medios tecnológicos, lo que ha sido aprovechado por los ciberdelincuentes para incrementar modos de operar en el delito; por lo tanto, considera que debe existir prioridades en el método legal punitivo es decir corregir las insuficiencias legales que concurren en nuestro país para concurrir con la identificación de autores de los delitos cibernéticos en corto plazo de investigación.

El presente antecedente de al autor Vílchez (2020), tiene coincidencia con el presente objetivo que es la determinación de la incidencia del ilícito de Phishing o suplantación de la identidad digital, dentro de la criminalidad informática en la legislación penal peruana año 2022., pues el autor desarrolla un análisis de la incidencia de los delitos cibernéticos durante la pandemia covid-19, como punto de inicio a su incremento, pues la mayor parte de transacciones se realizaron de manera digital, el investigador analiza la necesidad de implementar prioridades sancionatorias dentro del sistema judicial penal así, como medidas preventivas para lograr identificar autores de los delitos cibernéticos en corto plazo de investigación.

En la doctrina

El phishing viene a ser una de las técnicas de ingeniería muy conocida en la virtualidad, que puede ser efectuado a través de dos básicas modalidades: la primera es la suplantación de identidad para conseguir información confidencial y; la segunda es generada utilizando comunicaciones electrónicas, entre las que son correos y llamadas tecnológicas (Espinoza,2018).

El phishing, en términos simples, es un método en el que el usuario (la víctima) es contactado por el ciberdelincuente mediante correos electrónicos o mensajes de texto. El delincuente se hace pasar por una persona o entidad bancaria confiable para obtener datos confidenciales, como contraseñas y estados de cuenta. Una vez que obtienen esta información de manera fraudulenta, la utilizan indebidamente para acceder a las cuentas personales de la víctima y apropiarse de su patrimonio (Leguizamón, 2015)

La definición de Espinoza, tiene concordancia con el perfil de investigación que se ha realizado al señalar que es la suplantación de identidad que permite conseguir la información confidencial de las personas, para posteriormente ser mal utilizadas aprovechándose de dicha suplantación, siendo ésta una de las dos modalidades.

La definición doctrinal que le da Leguizamón también se considera concordante, al suscribir que es mediante esta modalidad de la suplantación que se permite obtener la información de terceras personas, con la finalidad fraudulenta de utilizar sus datos mediante sistemas electrónicos que causan perjuicios económicos.

Al objetivo específico primero. Describir los aspectos doctrinales y jurídicos de delitos informáticos en la legislación peruana.

En la entrevista

Se formula la siguiente pregunta: ¿considera usted, que existe suficiente jurisprudencia respecto a delitos informáticos en nuestro país? De los profesionales en materia penal que han sido entrevistados, se han obtenido de manera global los siguientes datos: Nueve de los entrevistados consideran que se carece de una de las fuentes más importantes del derecho que es esencial para enfrentar esta problemática, es decir, no contamos con suficiente jurisprudencia respecto al delito de Phishing, otro punto de vista el que han podido coincidir es que la causa de la precaria jurisprudencia se debe a que se están enfrentando a un delito nuevo. Finalmente, la postura de un entrevistado fue que las autoridades y e instituciones competentes no están haciendo un desempeño adecuado de sus funciones para la prevención, investigación y sanción de este delito que se está quebrantando el derecho a la propiedad.

Frente a ello, aquella postura concierne con nuestro objetivo que es describir los aspectos doctrinales y jurídicos de delitos informáticos en la legislación peruana, como complemento dejamos en análisis que no existe la suficiente jurisprudencia de estos delitos modernos que permita una adecuada interpretación legal de estos ilícitos, por lo tanto el congreso de la

república que es conocer de este problema, debe de promulgar normas más amplias que permitan adecuar las acciones delictivas de los ciber espacios.

En los antecedentes

Respecto al presente objetivo señalamos como antecedente que tiene coincidencia a Zeballos (2020), el investigador señala diversas modalidades de estafas informáticas, lo cual en los años últimos vienen perjudicando la economía de diversos usuarios que tienen una tarjeta o alguna dirección electrónica, por eso el autor plantea la necesidad de proteger la infraestructura informática estableciendo se conforme un consejo sobre ciberseguridad, además de colaboración de información tanto en sectores públicos y privados que permitan una estabilidad de los datos e informaciones cibernéticas, denunciar cualquier ataque cibernético.

Esta investigación tiene coincidencia con la posición del presente objetivo, pues en su interpretación se tiene en cuenta que el autor menciona la existencia de diversas modalidades de fraudes informáticos mediante el E-Commerce, el cual consiste en trámites de mercado cibernético (distribuir, vender, comprar, suministro de información, marketing, servicios por internet). Recomendando que se debe interconectar la información de entidades públicas con las empresas privadas para sostener estable los datos e informaciones cibernéticas.

La investigación de Román (2020) quien estudia las modificaciones legislativas de la ley N.º 30096 de “delitos informáticos para su eficacia contra la ciberdelincuencia en la ciudad de Chiclayo” Hace su fundamentación en la teoría del delito informático; estudiando los aspectos principales de los delitos informáticos establecidos en la modificación de la Ley 30096, donde sus resultados demuestran la existencia de diversos tipos de delitos los mismos que en nuestra legislación, no se encuentran regulados por la ley, señalando d forma conceptual que el delito informático se refiere a actividades ilícitas realizadas utilizando una computadora o cualquier dispositivo electrónico conectado a una red conectada, además indica que las características de estos ilícitos es por actos realizados de manera rápida y sencilla, se llevan a cabo mediante medios informáticos, y los perpetradores no necesariamente se encuentran presentes en el lugar de las personas o entidades afectadas, pero no requiere presencia física, por lo que estos delitos la florífera busca identificar y perseguir.

La investigación de Román (2020) se condice con el objetivo específico que describe los aspectos doctrinales y jurídicos de ilícitos informáticos en nuestra legislación, pues analiza

la ley N.º 30096, las mismas que se fundamentan en la teoría del delito informático; diversos tipos de delitos los mismos que en nuestra legislación, no se encuentran regulados por la ley, señalando de forma conceptual que el delito informático se refiere a actividades ilícitas realizadas utilizando un computador o cualquier electrónico dispositivo conectado a una red conectada, además indica que las características de estos ilícitos es por actos realizados de manera rápida y sencilla.

En la doctrina

según la Teoría del derecho penal y delito informático, el "fenómeno informático" se ha convertido en un hecho de nuestras vidas, presente entre nosotros e irrevocablemente integrado en nuestra realidad social y económica. Esto determinó el surgimiento de una serie de derechos en torno a su implementación y uso en aquel momento, que requerían la protección del ordenamiento jurídico. Por lo tanto, la cuestión principal actual es buscar reformas efectivas del control y supervisión penal, ya que el modelo de castigo tradicional no brinda una protección adecuada (Leyva,2011).

Uno de los indicadores de la resistencia a esta nueva realidad es precisamente considerar el ciberespacio, los sistemas informáticos y telemáticos como meros instrumentos ocasionales para la ejecución de cibercrímenes, equiparándolos incluso a delitos computacionales o, según Matellanes (2019), a la conexidad medial con la red para el manejo de datos, información y sistemas informáticos utilizando elementos intangibles.

Estas definiciones establecidas por Leyva (2021) y Matellanes (2000), tienen concordancia en el presente objetivo específico al señalar desde la doctrina la definición de delitos informáticos. Para lo que se necesita buscar reformas efectivas del control y supervisión penal, ya que el modelo de castigo tradicional no brinda una protección adecuada.

De acuerdo objetivo específico segundo: Desarrollar el tipo penal de suplantación de identidad digital en la legislación penal peruana

En las entrevistas:

Se formuló la siguiente pregunta: ¿se encuentra adecuado el tipo penal de suplantación de identidad digital en la legislación penal peruana? b) desarrollar el tipo penal de suplantación de identidad digital en la legislación penal peruana;

De los profesionales en materia penal que han sido entrevistados, se han obtenido de manera global los siguientes datos:

Siete de los diez entrevistados manifiestan que el delito de suplantación de identidad si se encuentra regulado en la Ley 30096 en el artículo 9, sin embargo, consideran que tienen que abordar de manera más precisa y exhaustiva las diferentes formas de suplantación de identidad.

Dos de los diez entrevistados argumentan que en nuestra legislación se encuentra regulado la suplantación de identidad, mas no, la suplantación de identidad digital, en efecto, nos estamos enfrentando a ese vacío legal que tiene que regularse con celeridad.

Frente a ello, aquella postura concierne con nuestro objetivo que es Desarrollar el tipo penal de suplantación de identidad digital en la legislación penal peruana.

Un dato esencial para enfrentar este delito, es que, no solamente es tarea de las autoridades crear una ley o modificarla para aumentar su pena, sino, las empresas del rubro de telecomunicaciones deben tener mejores políticas para prevenir este ilícito, por ejemplo: Las empresas dedicadas a la venta de celulares en los últimos años están vendiendo chips con la identidad de otra persona y esto se presta a que de manera más sencilla se apropien de la información personal del usuario. Es por ese motivo El coronel PNP Huamán Santamaría, jefe de la División de Investigación de Delitos de Alta Tecnología (Divindat) de la Policía Nacional del Perú en el periodo 2022 considero necesario que Osiptel, como ente regulador, ponga mayor énfasis en la verificación de la identidad por parte de los proveedores de telecomunicaciones.

En los antecedentes

La investigación de Flores (2020), Se indica que es necesario adaptarse a las nuevas formas de ciberdelincuencia. Perú se sitúa como el quinto país en América Latina con la mayor cantidad de ataques cibernéticos, afectando principalmente al sector financiero. Por lo tanto, la prioridad actual en Perú es desarrollar mecanismos que mitiguen el alto número de ataques cibernéticos y así asegurar la protección informática.

El presente antecedente de Flores (2020) , tiene concomitancia con nuestro objetivo específico dos que es desarrollar el tipo penal de suplantación de identidad digital en la legislación penal peruana, pues es un estudio nacional que analiza los aspectos doctrinales del tipo penal de suplantación de identidad en la legislación actual peruana que es la ley N.º

30096 de “delitos informáticos; desarrolla diversas características de la tipicidad y antijuridicidad del ilícito, por lo que el investigador recomienda una revisión de los ilícitos ya establecidos, y los nuevo ilícitos que no están reconocidos en nuestra legislación.

En la doctrina

Según Villavicencio (2018), indica: Este delito penaliza la acción de suplantar la identidad de una persona natural o jurídica, utilizando medios engañosos para defraudar y causar perjuicio. La suplantación de identidad se considera un delito de resultado, ya que no solo implica la acción de asumir la identidad de otro, sino que también requiere que esta acción cause un perjuicio. Un ejemplo de este delito es la creación de perfiles falsos en redes sociales como correo electrónico, Facebook o Twitter, atribuidos a personas naturales o jurídicas, con el fin de engañar y dañar a terceros.

Lo que nos enseña Villavicencio(2018) en su doctrina, se condice con el objetivo específico segundo, que habla de desarrollar descripción típica, la doctrina es la descripción típica del delito de suplantación de identidad, las características de delito y su procedimiento, lo cual concluye que no basta con la conducta típica el cual es suplantar la identidad a una persona, además debe de ir acompañado con otra conducta continuada, que es causar un perjuicio, entre ellos ejemplos que se demuestran son suplantar la identidad de alguien para con esa identidad causar daño mediante la creación de espacios cibernéticos como direcciones electrónicas, etc.

De acuerdo al Objetivo específico Tercero: c) analizar la criminalidad informática en el sistema penal peruano mediante la ley 30096 ley de delitos informáticos y su modificatoria Ley 30171”.

En las entrevistas

Se formuló la siguiente pregunta: ¿Qué señala la Ley 30096 ley de delitos informáticos y su modificatoria Ley 30171, respecto a la criminalidad informática en el sistema penal peruano?

De los profesionales en materia penal que han sido entrevistados, se han obtenido de manera global los siguientes datos: Nueve de los diez entrevistados, manifestaron la siguiente postura “La modificatoria de la Ley 30171 es más específica para adecuar de una mejor manera la descripción de los comportamientos delictivos, estableciendo cinco segmentos de ciber delitos respecto a los bienes, haciendo énfasis en que el delito en cuestión vulnera los datos y el sistema informático, abusa de dispositivos y mecanismos informáticos, viola el

secreto de las comunicaciones, y atenta contra patrimonio”. Frente a ello, aquella postura concierne con nuestro objetivo que es analizar la criminalidad informática en el sistema penal peruano mediante la ley 30096, ley de delitos informáticos y su modificatoria Ley 30171. El Análisis de la modificatoria de la Ley es el siguiente: la nueva Ley modifica los artículos 2,3,5,7,8 y 10, incorporando la calidad de ilegítima y deliberada respecto de los ilícitos de acceso ilícito: atentados contra la integridad del sistema de interceptación de datos y fraude informático, además se esclarece el abuso de mecanismos de esta naturaleza especificando delitos interceptación telefónica o interceptación de datos.

En los antecedentes

El antecedente de Román, quien estudia la modificación legislativa de la ley N.º 30096 de delitos informáticos para su eficacia contra la ciberdelincuencia en la ciudad de Chiclayo”, el autor propone cambios legislativos a la Ley N°30096 sobre Delitos Informáticos que permitan combatir de manera eficaz el ciberdelito, fundamentando teóricamente en la teoría del delito informático; diagnostica la situación actual del cibercrimen. Los resultados demostraron que existen diversos tipos de delitos y estos delitos no están debidamente regulados por la ley; el investigador concluye: que los ilícitos informáticos y se concluyó que el delito informático se refiere a actividades ilícitas realizadas utilizando una computadora o cualquier dispositivo electrónico conectado a una red conectada.

La investigación de Fuentes (2021), quien estudia la Modificación de la ley 30096, con el fin de la incorporación de ilícitos como phishing, pharming y carding los mismos que deben ser penalizables con pena efectiva, logrando la reducción de esta la ciberdelincuencia en la ciudad de Lima; el resultado que obtuvo el investigador fue incorporar los delitos del Phishing y Pharming como necesidad para hacer frente a una diversidad de ilícitos dentro del sistema informático. Una de las características para la comisión de las defraudaciones es la sensación de miedo para someter a sus víctimas al engaño y así robarle información personal.

En la doctrina

La doctrina de Manson (2013) Aquellos que violan la ley penal en relación con los delitos informáticos no son delincuentes comunes, sino individuos con especialización en informática. Se destaca que las personas que cometen estos delitos poseen habilidades específicas para manejar sistemas informáticos y suelen ocupar puestos estratégicos donde se gestiona información sensible.

El Autor Manson, hace referencia a las características del sujeto activo, de manera diferenciada sobre otros, cuando se trata de cometer delitos cibernéticos, considerando que puede ser cualquier persona, pero con características especiales como son tener conocimiento de cibernética, habilidades para manejar sistemas informáticos, considerando que gozan un espacio privilegiado en base a lo que conocen en centro de labores y aprovecha de este tipo de ventajas. Por lo tanto, la doctrina de Mason, si se condice con el objetivo específico número tres que nos ayuda a conocer aspectos de la criminalidad informática en el sistema penal.

CONCLUSIONES:

- 1.- El delito de Phishing está teniendo un evidente crecimiento y desarrollo, además es muy complicado enfrentarlo, inclusive para los especialistas, debido a que el ciber delincuente aplica técnicas de ingeniería informática con la finalidad de obtener los datos personales de los usuarios con la finalidad de suplantar su identidad. Si bien es cierto, se encuentra vigente la Ley 360096 que sanciona este delito, no ha sido eficaz debido a que no ha conseguido frenarlo. Esta figura antijurídica es muy incidente y se genera con un modus operandi para robar información bancaria (robo digital), por lo que en base a la doctrina se puede decir que El phishing viene a ser una de las técnicas de ingeniería muy conocida en la virtualidad, mediante esta modalidad de la suplantación que se permite obtener la información de terceras personas, con la finalidad fraudulenta de utilizar sus datos mediante sistemas electrónicos que causan perjuicios económicos.
- 2.- Sobre los aspectos doctrinales y jurídicos de delitos informáticos, se puede concluir que en la actualidad se carece de una de las fuentes más importantes del derecho que es que hay insuficiente jurisprudencia respecto al delito de Phishing. Los legales de los delitos informáticos están establecidos en la modificación de la Ley 30096, donde sus resultados demuestran la existencia de diversos tipos de delitos los mismos que en nuestra legislación, no se encuentran regulados por la ley.
- 3.- El Tipo penal de suplantar identidad, tiene la legislación en la Ley 30096 en el artículo 9º, sin embargo, consideran que tienen que abordar de manera más precisa y exhaustiva las diferentes formas de suplantación de identidad. Este tipo penal castiga el acto de ocupar de manera malintencionada el lugar de alguien, causando defraudación su derecho, trabajo o asistencia del cual hacía disfrute causándole un perjuicio a la persona natural o jurídica. Esta figura penal es clasificada dentro de los ilícitos de resultado.

- 4.- Se concluye que la criminalidad informática en el sistema penal peruano mediante la ley 30096, cuenta con una modificatoria que es la Ley 30171 viene a ser más específica para adecuar de una mejor manera la descripción de los comportamientos delictivos, estableciendo cinco segmentos de ciber delitos respecto a los bienes, haciendo énfasis en que el delito en cuestión vulnera los datos y el sistema informático, abusa de dispositivos y mecanismos informáticos, viola el secreto de comunicación y causa atentado hacia el patrimonio.

RECOMENDACIONES

1. El Estado peruano debe mejorar los medios técnicos de su Unidad de Delitos Informáticos, porque al parecer la tecnología utilizada por quienes cometen actos ilícitos es considerada más avanzada que la utilizada por los responsables de investigar delitos informáticos.
2. La normativa que regula todos los delitos informáticos debe ser analizada anualmente para incorporar plenamente los nuevos patrones que han ido surgiendo a lo largo de los años, de tal manera que estos ilícitos actos, mayormente permanecen impunes, puedan ser sancionados.
3. El Poder Legislativo debe adoptar innovadores lineamientos en la legislación para incorporar plenamente el delito de phishing en la Ley 30096, de manera que quienes cometan estos delitos puedan ser procesados y sancionados penalmente.
4. A la luz de lo dispuesto por la Ley N°30096 y crecimiento de ilícitos actos que se realizan mediante la tecnología, se determinó que la normatividad penal peruana la cual hace regulación a los ilícitos informáticos requiere actualizarse adecuadamente en el nuevo tipo de phishing, ya que es claro que en este La forma en que se han revelado actos ilegales, pero queda impune y no sancionada, afectando directamente a la sociedad sin compensación adecuada ni sanciones penales.

BIBLIOGRAFIA

- Altamirano, A. F. (2010). *Teoría del delito*. Obtenido de <https://derecho.usmp.edu.pe/instituto/novedades/libro-teoria-del-delito-oscar-pena.pdf>
- Arce, J. (2018). *Politica Criminal y delito informatico*. Lima: Gaceta Juridica.
- Avalos, R. Z. (2020). *Informe de análisis n°04 ciberdelincuencia: pautas para una investigación fiscal especializada*. Obtenido de <https://cdn.www.gob.pe/uploads/document/file/1669400/CIBERDELINCUENCIA>
- Azaola, C. L. (2010). *Delitos informáticos y Derecho penal*. México: Ubijus.
- Bajes, S. J. (2020,p.119). *La tentativa en los delitos de peligro abstracto*. Obtenido de <https://www.tesisenred.net/handle/10803/663023>
- Bonilla. (2008). *La evolución de internet como medio de comunicación masivo*. Obtenido de Recuperado de http://biblioteca.usac.edu.gt/tesis/16/16_0599.pdf
- Borghello, C. . (2012). *Suplantación de Identidad Digital como delito informático en Argentina*. Argentina.
- Borghello, C. (2020). *Suplantación de Identidad Digital como delito*. doi:https://www.elderechoinformatico.com/publicaciones/mtemperini/JAIIO_DI_Id entidad_Camera%20Ready.pdf
- Bramont- Arias Torres, L. (2000). Delitos informáticos. . *Revista Peruana de Derecho de la Empresa, Derecho informático Y Teleinformática Jurídica*. No. 51.
- Budapest. (2020). *Convenio sobre la ciberdelincuencia*.
- Cahuasa, P. B. (2024). *“Pharming”: cómo los Ciberdelincuentes pueden suplantarnos para robar nuestros datos*. <https://unifranz.edu.bo/blog/pharming-como-los-ciberdelincuentes-pueden-suplantarnos-para-robar-nuestros-datos/>: UNIFRANZ.
- Calle, M. S. (2023). *Diseños de investigación cualitativa y cuantitativa*. DOI: https://doi.org/10.37811/cl_rcm.v7i4.7016.
- Camacho, L. L. (2020). *El delito informático*. Madrid: Gráficas Cóndor.

- Coello Mazuelos, J. (2020). *El derecho de crédito como objeto de protección penal*. Obtenido de file:///C:/Users/usuario/Downloads/14361-Texto%20del%20art%C3%ADculo57143-1-10-20151117.pdf
- Curio, d. P. (2016). *Delitos informático Generales*. Obtenido de Recuperado de https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf
- De Alfonso, L. D. (2001; pp.110-111). El hackerin blanco. Una conducta ¿punible o impune? En Internet y derecho penal, Cuadernos de Derecho Judicial, Consejo General del poder Judicial. . Madrid.
- Defensoría del Pueblo. (2023). Informe Defensorial N° 001-2023-DP/ADHPD. *La Ciberdelincuencia en el Perú: estrategias y retos del Estado*. doi:<https://www.defensoria.gob.pe/wp-content/uploads/2023/05/INFORME-DEF-001-2023-DP-ADHPD-Ciberdelincuencia.pdf>
- Efe. (2021). *Estafa cibernética, el delito de moda que saca los colores a la víctima 20 minutos*. Obtenido de <https://www.20minutos.es/noticia/4602459/0/estafa-cibernetica-delito-moda-saca-colores-victima/?autoref=true>
- Española., D. d. (28 de marzo de 2014). Obtenido de <http://lema.rae.es/drae/?val=acceder>
- Fernandez, S. (2021). *Metodología de la Investigacion cientifica Cualitativa*. México.
- Flores, M. (2020). *Tecnología y violencia en Perú. En Hiper derecho*. Obtenido de <https://hiperderecho.org/2018/12/tecnologia-y-violencia-en-peru/>
- Fuentes, G. K. (2021). Modificación de la ley 30096 para incorporar los delitos de phishing, pharming y carding como delitos penalizables con prisión, para reducir la ciberdelincuencia Lima 2019. Pimentel - Chiclayo: Universidad Señor de Sipan. Obtenido de <https://repositorio.uss.edu.pe/handle/20.500.12802/8345>
- Gonzales, C. C. (octubre de 2021). Tesis. *Comercio electrónico y los problemas de la ciberdelincuencia en tiempos de Covid-19, Pimentel Udch*. Pimentel, Chiclayo, Lambayeque: UDCH.
- González, V. A. (2022). *La entrevista cualitativa como técnica de investigación en el estudio de las organizaciones*. DOI: <https://doi.org/10.36367/ntqr.14.2022.e571>.
- Gutiérrez, F. M. (1991; p. 76.). *Fraude informático y estafa*. Madrid: Ministerio de Justicia.

- Gutierrez, F. M. (2019). *Fraude informático y estafa*.
- Hernandez, R. (2021). *Metodología de la Investigación*. Bogota- Colombia: Graw Hill.
- Klip, A. (2014; p. 449.). *Internacional de Derecho Penal, Asociación Internacional de Derecho Penal AIDP. Francia*.
- Leguizamón, S. (2015). *El phishing, trabajo final para alcanzar el grado en Criminología y Seguridad*. , Universitat Jaume.
- Leyva, S. C. (2021). *Study of computer crimes and the problem of your typification in the framework of the international agreement* . Lima: Lucerna Iuris Et Investigatio.
- López, J. (2020). *Métodos y técnicas de detección temprana de casos de phishing*. Cataluña: Universitat Oberta de Catalunya.
- Manson, M. (27 de diciembre de 2013). *Legislación sobre delitos informáticos*. . Obtenido de <https://dl.dropbox.com/u//dl.legislacioncomparada.pdf>.
- Marchena, G. M. (2001; p. 356.). *El sabotaje informático: entre los delitos de daños y desordenes públicos*. Madrid: Cuadernos de Derecho Judicial.
- Martinez, C. (2023). *Guía para la revisión y el análisis documental: propuesta desde el enfoque investigativo*. España: Dialnet.
- Mata Barranco, N. Y. (2009). El delito de daños informativos: una tipificación defectuosa. *Revista de Estudios Penales y Criminológicos. Volumen XXIX. España.*, pp. 311-362.
- Matellanes, N. (2019). *“Algunas notas sobre las formas de delincuencia informática en el Código penal”*. Madrid: Colex.
- Matos, E. (2021). *El fraude informatico en la modalidad de Phishing*. Lima: Instituto Pacifico.
- MINJUS, M. d. (2022). *Ciberdelincuencia reporte de información estadística y recomendaciones para la prevención*. MINJUS. doi:<https://cdn.www.gob.pe/uploads/document/file/3562747/Reporte%20de%20Ciberdelincuencia.pdf>

- Monchiero, L. (2022). La suplantación de identidad creció un 50 por ciento en Argentina. *Clarín*, https://www.clarin.com/tecnologia/suplantacion-identidad-crecio-50-ciento-argentina-operan-ciberdelincuentes_0_WRq_pT7l4.html.
- Morant, V. J. (2002; p. 44). *Protección penal de la intimidad frente a las nuevas tecnologías*. Valencia: Práctica de derecho.
- Morant, Vidal Jesús. (2003; pp. 46- 47). *Protección penal de la intimidad frente a las nuevas tecnologías*. Valencia: Práctica de Derecho.
- Moron, L. E. (2019). *Internet y Derecho Penal: hacking y otras conductas ilícitas en la red*. 2da edición. Navarra: Aranzadi.
- Naranjo, L. E. (2023). *Revisión sistemática para propuesta de calidad metodológica en la docencia a las ciencias jurídicas*. Dialnet-RevisionSistematicaParaPropuestaDeCalidadMetodolog-9107695.pdf: ISSN electrónico: 1683-8947 .
- Neyra, F. J. (2020). *Novedades en el desarrollo y tipificación de delitos informáticos vinculados a criminalidad informática*. Lima: Gaceta Jurídica.
- Nieto, N. T. (2023). *Tipos de Investigación*. <https://core.ac.uk/download/pdf/250080756.pdf>.
- OEA, O. E. (2023). *Ciberdelitos y Criminalidad Informática*. FIADI file:///C:/Users/Rolando/Downloads/CIBERDELITOS+Y+CRIMINALIDAD+INFORM%C3%81TICA%20(1).pdf.
- 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.*, <https://scielo.conicyt.cl/pdf/rdpucv/n41/a07.pdf>.
- Oxman, N. (2021). *Estafas informáticas a través de internet. Acerca de la imputación penal del phishing y el pharming*. Valparaíso: Pontificia Universidad Católica de Valparaíso.
- Ricra, E. (2020). *Hacker y Cracker*. https://es.slideshare.net/EnmerGenaroLeandroRi?utm_campaign=profiletracking&utm_medium=sssite&utm_source=ssslideview.

- Roldan, Á. J. (2023). *El principio de confianza en el derecho penal*. Trujillo: UTC.
- Romero, C. M. (2018). *Introducción a la seguridad informática y el análisis de vulnerabilidades*. Obtenido de <https://www.3ciencias.com/wp-content/uploads/2018/10/Seguridad-inform%C3%A1tica.pdf>
- Roxin, C. (2014). *Autoría y dominio del hecho en derecho penal*, Tomo 2, . España: Editorial Civitas.
- Sánchez, C. (2018). *Bienes Jurídicos*. Obtenido de <file:///C:/Users/usuario/Downloads/DialnetLesividadEnLosBienesJuridicosColectivosYDelitosDeP-5235020.pdf>
- Schwartz, M. (2020). *Reporte ciberseguridad riesgos, avances y el camino a seguir en américa latina y el caribe*. Obtenido de [file:///C:/Users/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe%20\(1\).pdf](file:///C:/Users/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe%20(1).pdf)
- Sieber, U. (2020). *Criminalidad informática: peligro y prevención*.
- Stern, E. (No. 21; p. 187.). *El sentido de la privacidad, la intimidad y la seguridad en el mundo digital: ámbito y límites*. Eguzkilore.
- Unión Europea, P. P. (2021). *“Apoyo a la creación de una Fiscalía Especializada en Ciberdelito en Perú”*. <https://busquedas.elperuano.pe/dispositivo/NL/1916745-1>.
- Vallejos, A. (2018,p.284). *Delitos de peligro abstracto*. Obtenido de <https://www.tesisenred.net/handle/10803/663023#page=1>
- Vílchez, L. R. (2020). *La ciberdelincuencia en el contexto de la pandemia del coronavirus. Una aproximación desde el marco convencional*. Obtenido de [file:///C:/Users/usuario/Downloads/25688-Texto%20del%20art%C3%ADculo88341-1-10-20210209%20\(1\).pdf](file:///C:/Users/usuario/Downloads/25688-Texto%20del%20art%C3%ADculo88341-1-10-20210209%20(1).pdf)
- Villagómez, A. (2021). *"Metodología de la Investigacion Cuantitativa - Cualitativa"*. Bogotá: Ediciones de la U.
- Villagómez, A. (2021). *Metodología de la Investigacion Cuantitativa - Cualitativa*. Bogotá: Ediciones de la U.

- Villavicencio, M. L. (2023). *La Investigación Descriptiva con Enfoque Cualitativo*. Lima: PUCP.
- Villavicencio, T. F. (2013,p.354). *Derecho Penal. Parte general*. . Lima: Grijley.
- Villavicencio, t. F. (2020). *Delitos informáticos, en Ius et Veritas, n.º 49*. Obtenido de <https://revistas.pucp.edu.pe/index.php/iusetveritas/article/view/13630/14253>
- Vives Antón, T. y. (1996). *.Comentarios al código Penal 1995*. Valencia:: Tiront Blanch.
- Zea, C. (2022). Suplantación de identidad, un flagelo que está al alza . *Semana*, <https://www.semana.com/economia/macroeconomia/articulo/suplantacion-de-identidad-un-flagelo-que-esta-al-alza/202214/>.
- Zevallos Padro, O. (2020). *Delitos informáticos: ¿Cuáles son los principales fraudes informáticos que se pueden cometer a través del E-Commerce?* . Obtenido de <https://ius360.com/delitos-informaticos-cuales-son-los-principales-fraudes-informaticos-que-se-pueden-cometer-a-traves-del-e-commerce-oscar-zevallos-prado/>

ANEXOS

Anexo 01: Guía de entrevista



CARTA PARA VALIDACIÓN DEL INSTRUMENTO

Chiclayo, 19 de junio del 2023.

Magister: José Dolores Orrego Díaz.

Asunto: Evaluación de entrevista

Sirva la presente para expresarle nuestro cordial saludo e informarle que estoy elaborando mi tesis cuyo título es “El phishing o suplantación de la identidad digital, y su incidencia dentro de la criminalidad informática en la legislación penal peruana año 2022” con la finalidad de obtener el título de abogado.

Por ello, estoy desarrollando un estudio en el cual se incluye la aplicación de un instrumento de recolección de información denominado: entrevista.

Por tanto, le solicito tenga a bien realizar la validación del instrumento de investigación, que adjunto, para cubrir con el requisito de “Juicio de expertos”.

Esperando tener la acogida a esta petición, hago propicia la oportunidad para renovar nuestro aprecio y especial consideración.

Atentamente

Helfer Jairo Valdez Hernández

Adjunto:

- Título de investigación.
- Formulación del problema, objetivos generales y específicos
- Tabla de Categorización
- Instrumento


Mg. José Dolores Orrego Díaz
ABOGADO
José Dolores Orrego Díaz
C.A. Ab. Chiclayo 4° 1016
Magister.

a.- TÍTULO DE TRABAJO DE INVESTIGACIÓN:

La teoría de imputación de regreso en el ilícito de falsedad genérica que involucra a transportistas de carga de la provincia de Chiclayo”

b.- FORMULACIÓN DEL PROBLEMA:

¿De qué manera el Phishing o suplantación de la identidad digital, viene incidiendo dentro de la criminalidad informática en la legislación penal peruana en el año 2022?

c.- OBJETIVO GENERAL:

Analizar el Phishing o suplantación de la identidad digital, y su incidencia dentro de la criminalidad informática en la legislación penal peruana año 2022.

d. OBJETIVOS ESPECÍFICOS:

- a) describir los aspectos doctrinales y jurídicos de delitos informáticos en la legislación peruana;
- b) desarrollar el tipo penal de suplantación de identidad digital en la legislación penal peruana;
- c) analizar la criminalidad informática en el sistema penal peruano mediante la ley 30096 ley de delitos informáticos y su modificatoria Ley 30171 .



Dr. José Dolores Chusillo Díaz
MAGISTER
José Dolores Chusillo Díaz
La Jota, Chiclayo 2019
Magister:

INFORME SOBRE VALIDACIÓN DE EXPERTO

I. DATOS GENERALES

Apellidos y nombres del experto: José Dolores Orrego Diaz.
 Institución donde labora: Abogado
 Especialidad: Derecho.
 Instrumento de evaluación: Entrevista.
 Autor del instrumento: Helfer Jairo Valdez Hernández.

II. ASPECTOS DE VALIDACIÓN

EXCELENTE (1), BUENO (2), ACEPTABLE (3), DEFICIENTE (4), MUY DEFICIENTE (5)

CRITERIOS	INDICADORES	1	2	3	4	5
CLARIDAD	Los ítems están redactados con lenguaje apropiado y libre de ambigüedades acorde con los sujetos muestrales.		X			
OBJETIVIDAD	Las instrucciones y los ítems del instrumento permiten recoger la información objetiva sobre la variable, en todas sus dimensiones en indicadores conceptuales y operacionales.		X			
ACTUALIDAD	El instrumento de muestra vigencia acorde con el conocimiento científico, tecnológico, innovación y legal inherente a la variable: Variación de prisión efectiva.		X			
ORGANIZACIÓN	Los ítems del instrumento reflejan organicidad lógica entre la definición operacional y conceptual respecto a la variable, de manera que permiten hacer inferencias en función a la hipótesis, problema y objetivos de la investigación.		X			
SUFICIENCIA	Los ítems del instrumento son suficientes en cantidad y calidad acorde con la variable, dimensiones e indicadores.		X			
INTENCIONALIDAD	Los ítems del instrumento son coherentes con el tipo de investigación y responden a los objetivos, hipótesis y variable del estudio: Variación de prisión efectiva.			X		
CONSISTENCIA	La información que se recoja a través de los ítems del instrumento, permitirá analizar, describir y explicar la realidad, motivo de la investigación.			X		
COHERENCIA	Los ítems del instrumento expresan relación con los indicadores de cada dimensión de la variable: Variación de prisión efectiva.			X		
METODOLOGÍA	La relación entre la técnica y el instrumento propuestos responden al propósito de la investigación, desarrollo tecnológico e innovación.		X			
PERTINENCIA	La relación de los ítems concuerda con la escala valorativa del instrumento.		X			
PUNTAJE TOTAL						

(Nota: Tener en cuenta que el instrumento es válido cuando se tiene un puntaje mínimo de 41 "Excelente", sin embargo, un puntaje menor al anterior se considera al instrumento no válido ni aplicable)


 Mg. José Dolores Orrego Diaz
 Abogado
 Lic. Adm. Empresas
 Mg: José Dolores Orrego Diaz



Magister:

Objetivo específico Tercero: c) analizar la criminalidad informática en el sistema penal peruano mediante la ley 30096 ley de delitos informáticos y su modificatoria Ley 30171 .

¿Qué señala la Ley 30096 ley de delitos informáticos y su modificatoria Ley 30171, respecto a la criminalidad informática en el sistema penal peruano?



APROBADO
José Dolores Chuspa Díaz
11-Año: 2018
Magister:
Magister:

Anexo 02: Matriz de categorización.

Categoría de estudio	Definición conceptual	Subcategoría	Instrumento
Categoría uno: El phishing o suplantación de la identidad digital	Viene a ser una de las técnicas de ingeniería muy conocida en la virtualidad, que puede ser efectuado a través de dos básicas modalidades: la primera es la suplantación de identidad del personal bancario para conseguir información confidencial y; la segunda es generada utilizando comunicaciones electrónicas, entre las que son correos y llamadas tecnológicas	Definición del Phishing.	Análisis documental Entrevista
		Orígenes del Phishing	Análisis documental Entrevista
		Los tipos de Phishing	Análisis documental Entrevista
		Suplantación de identidad	Análisis documental Entrevista
		Clases de suplantación	Análisis documental Entrevista
		Consecuencias	Análisis documental Entrevista
		Antecedentes	Análisis documental Entrevista
		El ciberdelincuente	Análisis documental Entrevista
Categoría dos: Criminalidad informática	La criminalidad informática utiliza diferentes métodos, técnicas de ingeniería social (redes sociales), cuyo fin es capturar información personal o desarrollar actividades fraudulentas en deterioro de bienes jurídicos pluriofensivos gozando protección penal mediante legislación nacional especial Ley N°30096 y su modificatoria N.º 30171.	Tipos	Análisis documental Entrevista
		Clases	Análisis documental Entrevista
		La situación de las personas jurídicas	Análisis documental Entrevista
		La ley 30096 y su modificación por la ley 30171	Análisis documental Entrevista
		Reformas del Código Penal	Análisis documental Entrevista
			Análisis documental Entrevista

Anexo 03: entrevistas



Entrevista

I. Datos generales:

Edad: 31..... Cargo: Abogada independiente N.º Colegiatura: 7473
Condición laboral: Nombrado () Contratado ()

II. Instrucciones:

Estimado(a) colaborador, mediante esta entrevista cuya finalidad, es analizar “El Phishing o suplantación de la identidad digital, y su incidencia dentro de la criminalidad informática en la legislación penal peruana año 2022” me permite sugerir que sus respuestas sean de manera adecuada, a cada una de las preguntas formuladas. Siendo así, agradecemos su aporte en cada interrogante en la presente entrevista:

Objetivo general:

Analizar el Phishing o suplantación de la identidad digital, y su incidencia dentro de la criminalidad informática en la legislación penal peruana año 2022.

Que opinión le merece, la incidencia del delito el Phishing o suplantación de la identidad digital, la manera que viene creciendo estos delitos, y las normas penales de nuestro país para hacer frente a este problema.

Que, si bien cierto el delito el Phishing o suplantación de la identidad digital; en el Perú, vienen adecuando progresivamente su legislación en concordancia con la normatividad internacional, con el objeto de prevenir, investigar y sancionar esta clase de actos ilícitos y a sus responsables. La producción normativa abarca la regulación de diferentes asuntos, como es, el uso de las TIC, las medidas a implementarse para cautelar y proteger los datos y sistemas informáticos, la tipificación penal de actos y conductas delictivas y los procedimientos a seguir por las autoridades que resulten competentes al respecto, para perseguir y sancionar de forma eficaz a quienes delinquen en el ciberespacios. Que actualmente existe una Ley aprobada donde beneficia las condenas de menos años.

Objetivo específico Primero. - describir los aspectos doctrinales y jurídicos de delitos informáticos en la legislación peruana;

Considera usted, que existe suficiente jurisprudencia respecto a delitos informáticos en nuestro país:

Considero que, en nuestro país, aun no existe suficiente Jurisprudencia sobre los delitos informáticos, ya que solo establecen muy pocas normas, mucho más en nuestro código.

Objetivo específico Segundo: Desarrollar el tipo penal de suplantación de identidad digital en la legislación penal peruana.

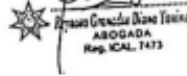
¿Se encuentra adecuado el tipo penal de suplantación de identidad digital en la legislación penal peruana?

Según la Ley N° 30096 o Ley de delitos informáticos, en su artículo 9°, si esta establecido, pero como sabemos bien acierto, hay muchos vacíos, que no está especificado claramente.

Objetivo específico Tercero: c) analizar la criminalidad informática en el sistema penal peruano mediante la ley 30096 ley de delitos informáticos y su modificatoria Ley 30171 .

¿Qué señala la Ley 30096 ley de delitos informáticos y su modificatoria Ley 30171, respecto a la criminalidad informática en el sistema penal peruano?

Que si bien es cierto la Ley 30171 es para adecuar de mejor manera la descripción de sus conductas delictivas al Convenio donde establece cinco grandes grupos de ciberdelitos en función a los bienes jurídicos, a saber, los datos y los sistemas informáticos, la indemnidad y la libertad sexuales, la intimidad y el secreto de las comunicaciones, el patrimonio y, por último, la fe pública. Los ciberdelitos contra los datos y los sistemas informáticos comprenden el acceso ilícito, los atentados a la integridad de los datos informáticos y de los sistemas informáticos, y el abuso de mecanismos y dispositivos informáticos.

Patricia Encarnación Díaz Torres
ABOGADA
Reg. ICAL 1473

Abogado:

Entrevista

I. Datos generales:

Edad: 30 Cargo: ABOGADA GRH- MPL N.º Colegiatura: 6820
Condición laboral: Nombrado () Contratado (X)

II. Instrucciones:

Estimado(a) colaborador, mediante esta entrevista cuya finalidad, es analizar “El Phishing o suplantación de la identidad digital, y su incidencia dentro de la criminalidad informática en la legislación penal peruana año 2022” me permite sugerir que sus respuestas sean de manera adecuada, a cada una de las preguntas formuladas. Siendo así, agradecemos su aporte en cada interrogante en la presente entrevista:

Objetivo general:

Analizar el Phishing o suplantación de la identidad digital, y su incidencia dentro de la criminalidad informática en la legislación penal peruana año 2022.

Qué opinión le merece, la incidencia del delito el Phishing o suplantación de la identidad digital, la manera que viene creciendo estos delitos, y las normas penales de nuestro país para hacer frente a este problema.

Se conoce que uno de los objetivos de la modalidad del Phishing es la de engañar al destinatario para que realice la acción esperada por el atacante, como obtener información financiera confidencial, credenciales de acceso al sistema u otra información estrictamente privada; aumentando cada día debido a la ignorancia digital de la mayor parte de la población, más aún de las personas de edades avanzadas, aprovechando el desconocimiento a la hora de navegar por internet; careciendo de normas estrictas que paralicen el avance de esta nueva modalidad de estafa, robo.

Objetivo específico Primero. - describir los aspectos doctrinales y jurídicos de delitos informáticos en la legislación peruana;

Considera usted, que existe suficiente jurisprudencia respecto a delitos informáticos en nuestro país:

No, actualmente la mayoría de la población carece de conocimiento respecto a las medidas a tomar después de caer en el mencionado Phishing, coadyuvando ello, a la falta de preceptos jurídicos vigentes que hagan referencia al mencionado ciberdelito.

Objetivo específico Segundo: Desarrollar el tipo penal de suplantación de identidad digital en la legislación penal peruana.

¿Se encuentra adecuado el tipo penal de suplantación de identidad digital en la legislación penal peruana?

Si, en parte, ya que la falta de capacitación respecto a la aplicación de las medidas coercitivas frente al mencionado delito informático, no ayudan a la correcta aplicación de sanciones penales.

Objetivo específico Tercero: c) analizar la criminalidad informática en el sistema penal peruano mediante la ley 30096 ley de delitos informáticos y su modificatoria Ley 30171 .

¿Qué señala la Ley 30096 ley de delitos informáticos y su modificatoria Ley 30171, respecto a la criminalidad informática en el sistema penal peruano?

La presente Ley tiene por objeto prevenir y sancionar las conductas ilícitas que afectan los sistemas y vulnerando los datos informáticos confidenciales y otros bienes jurídicos de las personas. Estableciendo que la finalidad de la ley es prevenir y sancionar las conductas ilícitas que afectan los sistemas, las datos informáticos, el secreto de las comunicaciones.



Mg. Abg. Leydi Vanessa Santamaría Torres

ICAL 6820

Entrevista**I. Datos generales:**Edad: 29 Cargo: Independe N.º Colegiatura: 9804

(Abogado)

Condición laboral: Nombrado () Contratado () – Independiente

II. Instrucciones:

Estimado(a) colaborador, mediante esta entrevista cuya finalidad, es analizar "El Phishing o suplantación de la identidad digital, y su incidencia dentro de la criminalidad informática en la legislación penal peruana año 2022" me permite sugerir que sus respuestas sean de manera adecuada, a cada una de las preguntas formuladas. Siendo así, agradecemos su aporte en cada interrogante en la presente entrevista:

Objetivo general:

Analizar el Phishing o suplantación de la identidad digital, y su incidencia dentro de la criminalidad informática en la legislación penal peruana año 2022.

Que opinión le merece, la incidencia del delito el Phishing o suplantación de la identidad digital, la manera que viene creciendo estos delitos, y las normas penales de nuestro país para hacer frente a este problema.

La Ley N° 30096 (Ley de Delitos Informáticos), nos permite salvaguardar nuestra identidad que hoy en día se ve afectada por los diversos delitos que se cometen en el ciberespacio y sin embargo esta no erradica la delincuencia ya que cada día incrementan los delitos informáticos en nuestro país.

Objetivo específico Primero. - describir los aspectos doctrinales y jurídicos de delitos informáticos en la legislación peruana;

Considera usted, que existe suficiente jurisprudencia respecto a delitos informáticos en nuestro país:

Considero que existe jurisprudencia respecto a delitos informáticos, pero no la suficiente como para resolver problemas de esta índole en el ámbito legal.

Objetivo específico Segundo: Desarrollar el tipo penal de suplantación de identidad digital en la legislación penal peruana.

¿Se encuentra adecuado el tipo penal de suplantación de identidad digital en la legislación penal peruana?

Sí se encuentra adecuado el tipo penal en la legislación peruana, tal y como se indica en el Art. 9 de la Ley N° 30096, sin embargo sería buena que se concrete más fundamentación jurídica en cuanto a éste tema que aún sigue latente para de ésta forma se tomen las medidas pertinentes.

Objetivo específico Tercero: c) analizar la criminalidad informática en el sistema penal peruano mediante la ley 30096 ley de delitos informáticos y su modificatoria Ley 30171.

¿Qué señala la Ley 30096 ley de delitos informáticos y su modificatoria Ley 30171, respecto a la criminalidad informática en el sistema penal peruano?

Si bien es cierto, es una ley bastante concreta y entendible razón por la cual, cabe precisar que el sistema penal peruano se enfoca mucho en el peligro que los menores de edad ~~sean~~ pueden pasar debido a los cibercriminales y sus artimañas, por otro lado se enfoca en temas bancarios que es otro tema latente en nuestro país, es por ello que deba indicar que siendo temas de gran importancia merece la atención



debida de nuestras autoridades y potenciar la ley respecto al tema antes mencionado.

Abogado: Katherine Córdova García.
Ical: 9804

Entrevista

I. Datos generales:

Edad: 29 Cargo: Abogado Litigante N.º Colegiatura: 9482

Condición laboral: Nombrado () Contratado ()

II. Instrucciones:

Estimado(a) colaborador, mediante esta entrevista cuya finalidad, es analizar “El Phishing o suplantación de la identidad digital, y su incidencia dentro de la criminalidad informática en la legislación penal peruana año 2022” me permite sugerir que sus respuestas sean de manera adecuada, a cada una de las preguntas formuladas. Siendo así, agradecemos su aporte en cada interrogante en la presente entrevista:

Objetivo general:

Analizar el Phishing o suplantación de la identidad digital, y su incidencia dentro de la criminalidad informática en la legislación penal peruana año 2022.

¿Qué opinión le merece, la incidencia del delito el Phishing o suplantación de la identidad digital, la manera que viene creciendo estos delitos, y las normas penales de nuestro país para hacer frente a este problema?

El delito de phishing o suplantación de identidad digital es en sí una preocupación significativa, debido a su creciente incidencia y los riesgos asociados para la seguridad y privacidad de las personas en el entorno digital. Este tipo de delito implica el uso de técnicas fraudulentas para obtener información confidencial, como contraseñas, números de tarjetas de crédito o datos personales, mediante el envío de correos electrónicos, mensajes de texto u otros medios de comunicación falsificados que logran vulnerar la seguridad de que creemos tener en cuanto a los medios en que realizamos transacciones económicas. Asimismo, en nuestro ordenamiento jurídico, existen normas penales que buscan hacer frente a este problema, es así que, la legislación cuenta con disposiciones que penalizan conductas relacionadas con el phishing y la suplantación de identidad digital, principalmente en el marco del Código Penal y otras normativas específicas en materia de delitos informáticos, con el propósito de disuadir y sancionar las acciones maliciosas realizadas en el ámbito virtual, como la Ley N.º 30096.

Objetivo específico Primero. - describir los aspectos doctrinales y jurídicos de delitos informáticos en la legislación peruana;

Considera usted, que existe suficiente jurisprudencia respecto a delitos informáticos en nuestro país:

Considero que actualmente no existe una jurisprudencia suficiente a pesar de los casos que se han venido presentando en cuanto a esta modalidad de delitos informáticos; sin embargo, es importante que las autoridades y entidades competentes en nuestro país continúen fortaleciendo las medidas de

prevención, investigación y persecución de los delitos de phishing, así como también la promoción de la educación y concientización sobre la seguridad cibernética entre los ciudadanos. Además, que el desarrollo y actualización constante de la legislación en concordancia con los avances tecnológicos son fundamentales para abordar eficazmente este desafío en el ámbito digital.

Objetivo específico Segundo: Desarrollar el tipo penal de suplantación de identidad digital en la legislación penal peruana.

¿Se encuentra adecuado el tipo penal de suplantación de identidad digital en la legislación penal peruana?

Considero que, la legislación penal peruana debería abordar de manera clara y exhaustiva las diversas formas de suplantación de identidad en el entorno digital, contemplando sanciones proporcionales a la gravedad de este delito y medidas específicas para proteger los derechos de las víctimas; por lo que, es importante y necesario que la normativa se mantenga actualizada para adaptarse a los cambios de la realidad tecnológica, pues al tener la Ley N.º 30096, considero que no es suficiente, debido a que hoy en día con los hechos delictivos que se presentan con ciertas particularidades no resultan ser atendidas para su prevención de manera oportuna y eficaz.

Objetivo específico Tercero: c) analizar la criminalidad informática en el sistema penal peruano mediante la ley 30096 ley de delitos informáticos y su modificatoria Ley 30171 .

¿Qué señala la Ley 30096 ley de delitos informáticos y su modificatoria Ley 30171, respecto a la criminalidad informática en el sistema penal peruano?

Señalan y establecen una serie de disposiciones específicas para prevenir, sancionar y perseguir delitos informáticos, incluyendo aspectos como el acceso no autorizado a sistemas informáticos, interceptación de comunicaciones, difusión de virus informáticos, entre otros. También contemplan medidas para proteger la seguridad de la información y para promover la cooperación internacional en la lucha contra los delitos informáticos. Es preciso decir que, esta ley con su modificatoria es un avance significativo en la legislación penal peruana, ya que reconoce la importancia de regular la criminalidad informática en un entorno tecnológico en constante evolución. Sin embargo, es importante siempre consultar las fuentes oficiales para obtener información actualizada y detallada sobre cualquier disposición legal específica es aplicable a cierto presunto hecho delictivo.


YERKA Y. DÍAZ CAMPOS
ABOGADO
Reg. ICAL. N° 9482



Entrevista

I. Datos generales:

Edad: 32..... Cargo: ABOGADA..... N.º Colegiatura: 8414

Condición laboral: Nombrado () Contratado (x)

II. Instrucciones:

Estimado(a) colaborador, mediante esta entrevista cuya finalidad, es analizar "El Phishing o suplantación de la identidad digital, y su incidencia dentro de la criminalidad informática en la legislación penal peruana año 2022" me permite sugerir que sus respuestas sean de manera adecuada, a cada una de las preguntas formuladas. Siendo así, agradecemos su aporte en cada interrogante en la presente entrevista:

Objetivo general:

Analizar el Phishing o suplantación de la identidad digital, y su incidencia dentro de la criminalidad informática en la legislación penal peruana año 2022.

Que opinión le merece, la incidencia del delito el Phishing o suplantación de la identidad digital, la manera que viene creciendo estos delitos, y las normas penales de nuestro país para hacer frente a este problema.

El delito el Phishing o suplantación de la identidad digital. Es una modalidad la cual es la más denunciada y se refleja en los registros. Consiste en la clonación de sitios web, especialmente de entidades bancarias, para engañar a los usuarios y obtener sus datos personales y claves de servicios financieros. Con esta información, los estafadores realizan transferencias bancarias ilegales y cometen el fraude cibernético.

En cuanto a las normas penales para hacer frente a este delito me parecen que deberían ser más severas ya que realizan diversos perjuicios a las víctimas, obteniendo información personal. En la actualidad la pena privativa de libertad es no menor de tres ni mayor de cinco años.

Objetivo específico Primero. - describir los aspectos doctrinales y jurídicos de delitos informáticos en la legislación peruana;

Considera usted, que existe suficiente jurisprudencia respecto a delitos informáticos en nuestro país:

No

Objetivo específico Segundo: Desarrollar el tipo penal de suplantación de identidad digital en la legislación penal peruana.

¿Se encuentra adecuado el tipo penal de suplantación de identidad digital en la legislación penal peruana?

SI

Objetivo específico Tercero: c) analizar la criminalidad informática en el sistema penal peruano mediante la ley 30096 ley de delitos informáticos y su modificatoria Ley 30171 .

¿Qué señala la Ley 30096 ley de delitos informáticos y su modificatoria Ley 30171, respecto a la criminalidad informática en el sistema penal peruano?

La ley describe que, con tan solo tener acceso a Internet, muchos de los usuarios están expuestos a una cadena de delitos que se cometen incorporando las nuevas tecnologías y avances digitales, según la ley violando la confidencialidad, integridad y la información; asimismo, la citada norma incorporó una serie de delitos informáticos, dentro de los que se encuentran interceptación de información, suplantación de identidad, entre otros, a estos tipos penales se les establecieron sanciones penales con la finalidad de contrarrestar su consumación.



Abg: Mariela Vallejos Terrones

REG. ICAL: N° 8414

Entrevista

I. Datos generales:

Edad: 27 Cargo: Defensa libre N.º Colegiatura: 9982

Condición laboral: Nombrado () Contratado ()

II. Instrucciones:

Estimado(a) colaborador, mediante esta entrevista cuya finalidad, es analizar “El Phishing o suplantación de la identidad digital, y su incidencia dentro de la criminalidad informática en la legislación penal peruana año 2022” me permite sugerir que sus respuestas sean de manera adecuada, a cada una de las preguntas formuladas. Siendo así, agradecemos su aporte en cada interrogante en la presente entrevista:

Objetivo general:

Analizar el Phishing o suplantación de la identidad digital, y su incidencia dentro de la criminalidad informática en la legislación penal peruana año 2022.

Que opinión le merece, la incidencia del delito el Phishing o suplantación de la identidad digital, la manera que viene creciendo estos delitos, y las normas penales de nuestro país para hacer frente a este problema.

El phishing, o suplantación de identidad digital, ha experimentado un notable crecimiento en los últimos años, especialmente con el aumento de los delitos asociados a fraudes informáticos durante la pandemia del COVID-19. Esta práctica consiste en el uso de técnicas de ingeniería social por parte de ciberdelincuentes para obtener información confidencial de los usuarios de forma fraudulenta y apropiarse de su identidad. Las normas penales de nuestro país deben contemplar estas diversas modalidades delictivas para poder enfrentar de manera efectiva este problema, aplicando penas acordes a la gravedad del delito y considerando el daño ocasionado a la víctima.

Objetivo específico Primero. - describir los aspectos doctrinales y jurídicos de delitos informáticos en la legislación peruana;

Considera usted, que existe suficiente jurisprudencia respecto a delitos informáticos en nuestro país:

En la legislación peruana, existe suficiente jurisprudencia respecto a delitos informáticos. Verbigracia la Ley N° 30171, Ley de Delitos Informáticos, promulgada en el año 2014. Esta legislación aborda diversas modalidades de delitos informáticos,

como fraudes electrónicos, suplantación de identidad, difusión de pornografía infantil a través de medios electrónicos, entre otros. Además, se ha creado la División de Investigación de Delitos de Alta Tecnología (DIVINDAT). Esta unidad especializada se encarga de casos abordados de ciberdelincuencia, incluyendo fraudes electrónicos, difusión de pornografía infantil, entre otros delitos que involucran el uso de tecnologías de la información.

Objetivo específico Segundo: Desarrollar el tipo penal de suplantación de identidad digital en la legislación penal peruana.

¿Se encuentra adecuado el tipo penal de suplantación de identidad digital en la legislación penal peruana?

El tipo penal de suplantación de identidad digital en la legislación penal peruana se encuentra adecuadamente establecido. La Ley N° 30171, Ley de Delitos Informáticos, contempla disposiciones para sancionar conductas delictivas relacionadas con el uso indebido de tecnologías de la información y comunicación, incluyendo la suplantación de identidad. Esta legislación aborda la usurpación de identidad en el ámbito digital, estableciendo las circunstancias que pueden ser penalizadas por delitos ya establecidos para el uso de falsa identidad. Asimismo, la jurisprudencia existente en el país ha contribuido a la interpretación y aplicación de las normas relacionadas con la suplantación de identidad digital, lo que brinda un marco legal sólido para abordar este tipo de delitos informáticos.

Objetivo específico Tercero: c) analizar la criminalidad informática en el sistema penal peruano mediante la ley 30096 ley de delitos informáticos y su modificatoria Ley 30171 .

¿Qué señala la Ley 30096 ley de delitos informáticos y su modificatoria Ley 30171, respecto a la criminalidad informática en el sistema penal peruano?

La Ley N° 30096, Ley de Delitos Informáticos, y su modificatoria Ley N° 30171, establecen disposiciones específicas para abordar la criminalidad informática en el sistema penal peruano. La Ley N° 30171 modificó varios artículos de la Ley N° 30096, ampliando y actualizando el marco legal para abordar de manera más efectiva la criminalidad informática en el país. Estas disposiciones legales brindan

un marco sólido para la persecución y sanción de delitos informáticos en el sistema penal peruano.



Abogado:

Entrevista

I. Datos generales:

Edad: 32..... Cargo: ...abogado... N.º Colegiatura: 10172_____
Condición laboral: independiente Nombrado () Contratado ()

II. Instrucciones:

Estimado(a) colaborador, mediante esta entrevista cuya finalidad, es analizar “El Phishing o suplantación de la identidad digital, y su incidencia dentro de la criminalidad informática en la legislación penal peruana año 2022” me permite sugerir que sus respuestas sean de manera adecuada, a cada una de las preguntas formuladas. Siendo así, agradecemos su aporte en cada interrogante en la presente entrevista:

Objetivo general:

Analizar el Phishing o suplantación de la identidad digital, y su incidencia dentro de la criminalidad informática en la legislación penal peruana año 2022.

Qué opinión le merece, la incidencia del delito el Phishing o suplantación de la identidad digital, la manera que viene creciendo estos delitos, y las normas penales de nuestro país para hacer frente a este problema.

Que, el delito de phishing se viene desarrollando de una manera incontrolable, de modo tal que cuesta trabajo para los especialistas detectarlo. Y si lo hacen cuando ya se ha cometido múltiples robos de identidad como cuentas bancarias, y frente a ello nuestras normas penales deben fortalecerse modificándose y estableciendo penas más drásticas a todas esas personas que cometen este tipo de delitos.

Objetivo específico Primero. - describir los aspectos doctrinales y jurídicos de delitos informáticos en la legislación peruana;

Considera usted, que existe suficiente jurisprudencia respecto a delitos informáticos en nuestro país: al ser delitos que se han desarrollados con mayor fuerza durante los últimos años, no existe jurisprudencia suficiente como para hacer frente a ello y así poder prevenir este tipo de delitos.

Objetivo específico Segundo: Desarrollar el tipo penal de suplantación de identidad digital en la legislación penal peruana.

¿Se encuentra adecuado el tipo penal de suplantación de identidad digital en la legislación penal peruana

Nuestro ordenamiento lo tipifica dentro de los delitos informáticos, a la suplantación de identidad. Esta lo desarrolla mas en la ley 30096, ley publicada el 10 de marzo del 2014.

Objetivo específico Tercero: c) analizar la criminalidad informática en el sistema penal peruano mediante la ley 30096 ley de delitos informáticos y su modificatoria Ley 30171 .

¿Qué señala la Ley 30096 ley de delitos informáticos y su modificatoria Ley 30171, respecto a la criminalidad informática en el sistema penal peruano?

Que tiene por objetivo prevenir y sancionar las conductas ilícitas, que afectan los sistemas y datos personales.

A handwritten signature in black ink, appearing to be 'Andrés B.', written over a horizontal line.

Abogado:

Entrevista

I. Datos generales:

Edad: ...33..... Cargo: ...ABOGADA N.º Colegiatura: ____7353____

Condición laboral: Nombrado () Contratado () Independiente (X)

II. Instrucciones:

Estimado(a) colaborador, mediante esta entrevista cuya finalidad, es analizar “El Phishing o suplantación de la identidad digital, y su incidencia dentro de la criminalidad informática en la legislación penal peruana año 2022” me permite sugerir que sus respuestas sean de manera adecuada, a cada una de las preguntas formuladas. Siendo así, agradecemos su aporte en cada interrogante en la presente entrevista:

Objetivo general:

Analizar el Phishing o suplantación de la identidad digital, y su incidencia dentro de la criminalidad informática en la legislación penal peruana año 2022.

Que opinión le merece, la incidencia del delito el Phishing o suplantación de la identidad digital, la manera que viene creciendo estos delitos, y las normas penales de nuestro país para hacer frente a este problema.

Estos delitos informáticos, en los cuales consiste en la clonación de sitios web, principalmente de los bancos, con la finalidad de obtener información personal de los usuarios como claves, dni, nombres, etc, en la actualidad están aumentando debido que muchas personas que tienen acceso al internet no saben usarlo adecuadamente, en muchos casos son personas ya adultas que “caen” en la trampa de que ingresen a tal sitio web para ganar un “dinero extra”.

En nuestro país tenemos la Ley N° 30096 en su ART. 09 que nos habla de la sanción donde va de 3 hasta 5 años de pena privativa de libertad, a aquellas personas 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.

Sin embargo en la práctica cuando uno denuncia estos tipo de delitos muchas veces terminan siendo archivados por falta de pruebas, es muy lamentable que no haya más información y/o legislación que sancione de una manera eficaz y efectiva este tipos de delitos.

Objetivo específico Primero. - describir los aspectos doctrinales y jurídicos de delitos informáticos en la legislación peruana;

Considera usted, que existe suficiente jurisprudencia respecto a delitos informáticos en nuestro país:

En nuestro país no hay mucha jurisprudencia respecto a este delito y menos una legislación donde se sancione aquello.

Objetivo específico Segundo: Desarrollar el tipo penal de suplantación de identidad digital en la legislación penal peruana.

¿Se encuentra adecuado el tipo penal de suplantación de identidad digital en la legislación penal peruana?

No, hay poca información tanto para abogados como para la ciudadanía respecto a este nuevo delito, hay una que otra ley pero terminan siendo letra muerta.

Objetivo específico Tercero: c) analizar la criminalidad informática en el sistema penal peruano mediante la ley 30096 ley de delitos informáticos y su modificatoria Ley 30171 .

¿Qué señala la Ley 30096 ley de delitos informáticos y su modificatoria Ley 30171, respecto a la criminalidad informática en el sistema penal peruano?

La ley N° 30096 y su modificatoria Ley N° 30171 señala el agravante y la pena cuando el agente acceda ilegítimamente al sistema informático vulnerando los sistema de seguridad.


María Mercedes Olascoaga
ABOGADO
ICAL N° 7553

Entrevista

I. Datos generales:

Edad: 31 Cargo: Inspector auxiliar de trabajo de Sunafil N.º Colegiatura: 7129

Condición laboral: Nombrado (X) Contratado ()

II. Instrucciones:

Estimado(a) colaborador, mediante esta entrevista cuya finalidad, es analizar “El Phishing o suplantación de la identidad digital, y su incidencia dentro de la criminalidad informática en la legislación penal peruana año 2022” me permite sugerir que sus respuestas sean de manera adecuada, a cada una de las preguntas formuladas. Siendo así, agradecemos su aporte en cada interrogante en la presente entrevista:

Objetivo general:

Analizar el Phishing o suplantación de la identidad digital, y su incidencia dentro de la criminalidad informática en la legislación penal peruana año 2022.

Que opinión le merece, la incidencia del delito el Phishing o suplantación de la identidad digital, la manera que viene creciendo estos delitos, y las normas penales de nuestro país para hacer frente a este problema.

Es lamentable, debido que cada vez aumenta los delitos de Phishing o suplantación de identidad, y a pesar de los grandes esfuerzos que el Estado realiza para combatir con dicho delito, los delincuentes buscan como a dé lugar, la manera se seguir optando por nuevas modalidades para llevar a cabo su cometido; no obstante, es rescatable la atención puesta y la dedicación que por hoy brinda el Estado para combatir con este problema que cada día asecha más.

Objetivo específico Primero. - describir los aspectos doctrinales y jurídicos de delitos informáticos en la legislación peruana;

Considera usted, que existe suficiente jurisprudencia respecto a delitos informáticos en nuestro país:

No, en razón que es un delito “relativamente nuevo”, siendo que hace pocos años ha tomado gran relevancia en nuestra legislación.

Objetivo específico Segundo: Desarrollar el tipo penal de suplantación de identidad digital en la legislación penal peruana.

¿Se encuentra adecuado el tipo penal de suplantación de identidad digital en la legislación penal peruana?

No. En nuestra legislación se encuentra regulado el tipo penal de suplantación de identidad, empero, suplantación de identidad digital, no.