FACULTAD DE DERECHO Y CIENCIAS POLÍTICAS

CARRERA DE **DERECHO Y CIENCIAS POLÍTICAS**

"FUNDAMENTOS JURÍDICOS PARA INCORPORAR EL *PHISHING* COMO AGRAVANTE EN EL ARTÍCULO 11° DE LA LEY N.º 30096 – LEY DE DELITOS INFORMÁTICOS EN EL PERÚ"

Tesis para optar al título profesional de:

Abogada

Autor:

Yosselym Marilu Betsabeth Ravines Carrera

Asesor:

Dr. Juan Carlos Tello Villanueva

https://orcid.org/0000-0003-4256-0738

Cajamarca - Perú

2023

JURADO EVALUADOR

Jurado 1 Presidente(a)	**Saúl Alexander Villegas Salazar**	**46865487**
	Nombre y Apellidos	N.º DNI

Jurado 2	**Ramón Omar Muñoz Salazar**	**26732876**
	Nombre y Apellidos	N.º DNI

Jurado 3	**Juan Vargas Carrera**	**26704874**
	Nombre y Apellidos	N.º DNI

INFORME DE SIMILITUD

UNDAMENTOS JURÍDICOS PARA INCORPORAR EL PHISHING COMO AGRAVANTE EN EL ARTÍCULO 11° DE LA LEY N.o 30096 – LEY DE DELITOS INFORMÁTICOS EN EL PERÚ

INFORME DE ORIGINALIDAD

20%	17%	9%	10%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	www.defensoria.gob.pe Fuente de Internet	4%
2	dspace.uniandes.edu.ec Fuente de Internet	1%
3	Submitted to Universidad Privada del Norte Trabajo del estudiante	1%
4	Submitted to Universidad Nacional del Santa Trabajo del estudiante	1%
5	repositorio.usanpedro.edu.pe Fuente de Internet	1%
6	Submitted to Universidad Católica de Santa María Trabajo del estudiante	1%
7	Submitted to Universidad Nacional Jose Faustino Sanchez Carrion Trabajo del estudiante	1%
8	repositorio.unsa.edu.pe	

DEDICATORIA

Esta investigación está dedicada a mi padre, mis hermanas y mi hermano, quienes me han brindado su apoyo y su amor incondicional durante mi carrera universitaria, finalmente, a mi madre quien ha sido mi principal motivación, quien desde el cielo me ha dado la fuerza necesaria para culminar adecuadamente este proyecto.

AGRADECIMIENTO

A Dios, porque es quien me permite lograr este objetivo y es quien me ilumina día a día.

A mi padre, por todo el apoyo tanto moral y la fortaleza que me ha brindado a lo largo de mi vida.

A mi hermano y hermanas, por la confianza, apoyo y ánimo brindado durante todo mi proceso profesional.

A mis docentes, por toda la información y el apoyo académico brindado a lo largo de la carrera profesional.

TABLA DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

La presente investigación tiene por objetivo general determinar los fundamentos jurídicos necesarios para la incorporación del *Phishing* como una agravante del artículo 11° de la Ley N.º 30096 – Ley de delitos Informáticos en el Perú, por lo cual, el tipo de investigación fue básica – descriptiva y con un diseño no experimental, desarrollando un enfoque cualitativo con un alcance correlacional para cumplir con cada objetivo planteado, la población serán todas la principales normas nacionales que se desarrollen en materia penal, tomando como única muestra a la Ley N° 30096 – Ley de delitos informáticos; usando como técnica el análisis de contenido a partir del fichaje, el cual fue usado como instrumento principal, además, del uso de métodos generales y jurídicos que me ayudaron en el análisis de la información obtenida; finalmente, se realizaron los resultados, los cuales brindan una respuesta adecuada a cada uno de los objetivos específicos, desarrollando así la discusión correspondiente de los mismos, para que se pueda resolver la hipótesis planteada, permitiendo así llegar a las conclusiones que hacen referencia a los resultados obtenidos en el presente trabajo de investigación y se recomiende la integración de esta modalidad delictiva como una de las agravante del artículo 11° de la Ley N.º 30096.

PALABRAS CLAVES: Phishing, Delito informático, Agravante, Enlace malicioso.

CAPÍTULO I: INTRODUCCIÓN

1.1. Realidad problemática

En la actualidad, la tecnología ha venido desarrollándose de una forma desmedida y es por esta razón que, la cibercriminalidad también se ha ido incrementado a nivel nacional e internacional, además, desde que se dio la pandemia del COVID – 19 en el año 2020, el uso de plataformas y herramientas tecnológicas hicieron que su aumento sea exponencial hasta la actualidad, es por esta razón que, para cumplir con las restricciones planteadas por el Estado, todas las personas tuvieron que adecuarse al uso de la tecnología enfocadas en los ámbitos educativo, laboral y empresarial, todo esto de acuerdo a las actividades cotidianas que estos realizan y al estilo de vida que llevaban, razón por la cual, en el Perú como en otros países de Latinoamérica, se han tenido que crear y/o modificar regulaciones sobre ciberdelincuencia en sus ordenamientos jurídicos, los cuales les han permitido conocer y delimitar nuevas conductas delictivas.

Estos cambios tecnológicos han traído como consecuencia un incremento en los ataques y modalidades de ciberdelincuencia, siendo el *phishing* una de las modalidades de ciberataque con más incidencia en el mundo, esto de acuerdo al reporte de defensa digital de Microsoft (2020), donde sostiene que el *phishing*, en el contexto empresarial se ha convertido en un factor importante y se ha ido incrementando con el tiempo, pues este se da cuando personas u organizaciones reciben correos electrónicos fraudulentos, los mismos que los hacen ingresar a un enlace que permite que los ciberdelincuentes accedan a un dispositivo en específico y pueda obtener información personal o relevante de las mismas.

Es por esto que, en nuestro país, después de realizar un análisis detallado a la normativa vigente de la Ley N.º 30096 – Ley de Delitos Informáticos, y a su modificatoria

en su artículo 1[1], se debe tener en cuenta que el objetivo principal es sancionar acciones ilícitas que afectan los datos informáticos, por lo que, de acuerdo a la interpretación de Herrera (2016), queda claro que, con la evolución de la tecnología se han ido generado nuevas formas de amenazas en contra de la privacidad de las personas, es decir, que a consecuencia de este avance también se ha creado la necesidad de resguardar los bienes jurídicos que afectan estos tipos de delitos, con la finalidad de proteger los datos personales de las personas, por lo que, es importante tener en cuenta que es necesaria una tipificación que regule el *phishing* como la modalidad más común utilizada por los ciberdelincuentes en la Ley N.º 30096, a través de la cual estos obtienen la información personal de sus víctimas para así poder continuar con la comisión de otros delitos que se encuentran en la presente normativa.

Ante esto, primero es importante entender que es el *phishing*, hace referencia a uno de los métodos más utilizados por los ciberdelincuentes para poder estafar y hacer caer en error a sus víctimas, para obtener información confidencial de forma fraudulenta a través de links o URL, los cuales son distribuidos en su gran mayoría mediante las redes sociales, a fin de poder lograr su cometido (Hidalgo y Solano, 2021).

Como se puede observar el *phishing* es una pieza clave para que se puedan llevar a cabo la mayoría de delitos informáticos que se encuentran dentro de la Ley N.º 30096, esto debido al gran impacto que ha ido generando en la obtención de información personal de sus

[1] La presente Ley tiene por objeto prevenir y sancionar las conductas ilícitas que afectan los sistemas y datos informáticos y otros bienes jurídicos de relevancia penal, cometidas mediante la utilización de tecnologías de la información o de la comunicación, con la finalidad de garantizar la lucha eficaz contra la ciberdelincuencia. (Ley de Delitos Informáticos, 2014, Artículo 1)

víctimas, por lo que sería adecuada su consideración como una de las agravantes que se encuentran tipificadas en el artículo 11°[2] de la misma ley.

Después de todo, en nuestro país, se ha registrado a nivel de fiscalía que desde hace unos años se ha dado un incremento sustancial en cuanto al número de denuncias registradas por delitos informáticos, siendo así que el año 2018, las denuncias por delitos informáticos fueron por un total de 3,851 delitos aproximadamente, mientras que al mes de noviembre del año 2019, se registró un total de 6,906 delitos informáticos, registrando una cifra mayor en un 79.33%; asimismo, en el mismo mes del mismo año se pudo concluir que el delito con mayor incidencia se presenta en aquellos que tienen como bien jurídico protegido el patrimonio generando un 38.24% de delictividad, además, para el año 2020, se registró un total de 8,674 delitos informáticos – Ley N° 30096, en los cuales el mayor porcentaje fueron delitos informáticos contra el patrimonio con un 54.65% (4,741 delitos) (Ministerio Público, 2019, pp. 50 - 59).

En resumen, esto nos deja ver que los ciberataques se van incrementando y que también van surgiendo nuevas modalidades delictivas, las cuales se han visto reprimidas en nuestro ordenamiento jurídico debido a que la Ley de Delitos Informáticos, no fue actualizada desde febrero del año 2014, cuando se promulgó la Ley N.º 30171, la cual realizó

[2] El juez aumenta la pena privativa de libertad hasta en un tercio por encima del máximo legal fijado para cualquiera de los delitos previstos en la presente Ley cuando:

1. El agente comete el delito en calidad de integrante de una organización criminal.
2. El agente comete el delito mediante el abuso de una posición especial de acceso a la data o información reservada o al conocimiento de esta información en razón del ejercicio de un cargo o función.
3. El agente comete el delito con el fin de obtener un beneficio económico, salvo en los delitos que prevén dicha circunstancia.
4. El delito compromete fines asistenciales, la defensa, la seguridad y la soberanía nacionales. (Ley de Delitos Informáticos, 2014, Artículo 11°)

la modificación de algunos artículos integrantes de la Ley N.º 30096, dentro de las cuales no se encontraba el artículo 11° referente a las agravantes, razón por la cual, ante dicha intensificación de este tipo de modalidades delictivas se encuentra al *phishing* como una de las más recurrentes, por lo que su integración como una agravante en la presente ley sería lo más considerable para una adecuada sanción.

De la misma forma se debe tener en cuenta que, de acuerdo al principio de legalidad, no es posible sancionar a ninguna persona por un acto que no se encuentre tipificado en una norma al momento de la comisión del hecho delictivo, por tal motivo, la presente investigación busca realizar un análisis de los fundamentos jurídicos que logren incorporar al *phishing* como una de las agravantes del artículo 11° de la Ley N.º 30096 – Ley De Delitos Informáticos.

1.2. Antecedentes de la investigación.

1.2.1. A nivel internacional

Frente al ámbito internacional se tiene que, para Gonzáles y Peña (2012), en su tesis de pregrado titulada "Estudio del impacto de la ingeniería social – phishing", sustentada en la Universidad Autónoma de México, desarrollaron una tesis cualitativa basada en la ingeniería, el análisis e interpretación de este tipo de método ciberdelictivo que hace que estos autores reconozcan que el *phishing* se ha generalizado con más fuerza en la actualidad, y se ha convertido en el principal delito cometido a través de las redes, convirtiendo así como un fenómeno social muy peligroso que no tiene una tipificación adecuada.

Por otro lado, se pudo encontrar la tesis para obtener el Título de abogado, desarrollada por Herrera (2016), la misma que se titula "El phishing como delito

informático y su falta de tipificación en el Código Orgánico Integral Penal", presentada en la Universidad Central de Ecuador, concluyó que el *phishing* al no encontrarse regulado genera inseguridad e impunidad, pues hace que exista desprotección jurídica en cuanto a las víctimas por la comisión de tales hechos, pues no existe una tutela judicial efectiva de sus derechos, además este delito genera alarma en la sociedad por ser muy peligroso y por violentar el derecho a la intimidad y propiedad de las personas.

También, para Salvi (2019), en su tesis para obtener el Título de Abogado en la Universidad Siglo 21, denominado "El Phishing en la Argentina", como principal objetivo para el desarrollo de su tesis fue analizar los diferentes problemas que abarca el *phishing*, por lo que fue necesario ahondar en la normativa existente, respecto a la competencia territorial y material, y también, en el estudio de la problemática del *phishing* como medio para la comisión de Delitos Informáticos, además, realizó el estudio para determinar si se debe tipificar en el ámbito penal la conducta de obtención de datos personales, finalmente, concluyó que se deben evitar las ambigüedades que puedan surgir del "phishing", pues en vista de esto, puede existir dificultades que impidan aplicar las leyes posiblemente diferentes en un mismo caso en específico.

Así pues, Castillo (2021), en su tesis para obtener el Título de Maestro en la Universidad Externado de Colombia, denominada "Phishing: Día de pesca", analiza el sistema de enjuiciamiento criminal colombiano, particularmente en la modalidad denominada como el *phishing*, para así poder establecer su eficacia y a su vez generar nuevas medidas en esa materia, por lo que, concluye que el *phishing* se da por la falta de buenas prácticas en cuenta a la ciberseguridad, pues no existe un adecuado comportamiento en cuanto a la criminalidad cibernética.

1.2.2. A nivel nacional.

Por otra parte, para el ámbito nacional se realizó la búsqueda en la página oficial de la Red de Investigación de Trabajos de Investigación (RENATI), con el fin de identificar trabajos que aborden el presente tema, teniendo como resultado lo siguiente:

Para Pardo (2018) en su tesis denominada "Tratamiento jurídico penal de los delitos informáticos contra el patrimonio, Distrito Judicial de Lima, 2018", presentada ante la Universidad César Vallejo – Lima, para obtener el grado de Maestro, planteó como objetivo principal analizar el tratamiento jurídico penal de los delitos informáticos contra el patrimonio, dentro del distrito judicial de Lima en el año 2018, desarrollando así una metodología propia y una investigación cualitativa, dentro de un nivel descriptivo explicativo, para lograr su adecuada interpretación y análisis dentro de su investigación, y así poder concluir que el tratamiento jurídico existente es deficiente en cuanto a los delitos informáticos contra el patrimonio, pues al no encontrarse con una regulación adecuada, causa que la interpretación de la norma genere incertidumbre en los operadores de justicia y no permite la adecuada sanción para este tipo de delitos.

En la presente tesis se ha desarrollado al *phishing* solamente como un delito informático que afecta directamente al patrimonio en la Ley N.º 30096, lo cual se diferencia de la presente investigación porque aquí el *phishing* es considerado como una modalidad que puede afectar distintos bienes jurídicos protegidos lo mismo que le permite adecuarse a cualquier tipo penal que se desarrolle la presente ley.

Además, Fuentes (2021), en su tesis para obtener el Título de Abogada en la Universidad Señor de Sipán, denominada "Modificación de la Ley N.º 30096 para

incorporar los delitos de Phishing, Pharming y Carding, como delitos penalizados con prisión, para reducir la ciberdelincuencia, Lima 2019", presentó como objetivo general el justificar por qué los delitos de Phishing, Pharming y Carding, deben ser incorporados a la Ley N.º 30096, como delitos que se penalizan con pena privativa de libertad, desarrollando así un tipo de investigación básica con un enfoque cualitativo para poder explicar la importancia de la integración de estas modalidades dentro de la Ley N.º 30096, y así lograr identificar las deficiencias legislativas existentes en la tipificación jurídica de dicha norma, identificando en el *phishing* como sujeto activo a aquel que solicita claves por correo electrónico, y como sujeto pasivo a aquella persona que brinda dicha información, para que pueda cometerse el ilícito penal.

En este caso, la tesis anterior busca integrar en la Ley de Delitos Informáticos al Phishing, Pharming y Carding, como delitos independientes, a diferencia de esta investigación que solo busca integrar en sus agravantes al *phishing*, como la modalidad más utilizada en la actualidad para que se puedan llevar acabo la comisión de algunos delitos que desarrolla la Ley N.º 30096 – Ley de Delitos Informáticos.

Ahora bien, de acuerdo a lo presentado por Ventura (2021), en su tesis para obtener el grado de abogada, en la Universidad Privada del Norte, la misma que se denomina "La tipificación del phishing, smishing y vishing en nuestro sistema penal peruano, para la lucha contra la ciberdelincuencia en lima, 2020", desarrolla la justificación del por qué los delitos del phishing, smishing y vishing, deben ser incorporados en el Sistema Penal como delitos penalizados en el Perú, realizando para ello una investigación básica, con un enfoque cualitativo y multimetódico, para lograrlo tiene como finalidad principal explicar la importancia en la incorporación de estos delitos dentro de la normativa penal.

Por otro lado, el enfoque que desarrolla la tesis anterior es la de tipificar el phishing, smishing y vishing como nuevos delitos, pero dentro del Código Penal, a diferencia de mi investigación que busca integrar el *phishing* en un artículo en específico dentro de la Ley de Delitos Informáticos, teniendo en cuanta que esta ley busca sancionar conductas ilícitas que afectan bienes jurídicos a través del uso de las tecnologías y así reducir el incremento de la ciberdelincuencia en nuestro país.

Finalmente, para Sosa (2022), en su tesis para optar por el Título de abogado, en la Universidad Nacional de Piura, la que se denomina "Phishing como modalidad de delitos informáticos: a propósito de la suplantación y robo a los beneficiarios del bono universal en el Perú", la misma que desarrolla la forma de determinar si el *phishing* es una modalidad de delito informático que se encuentra tipificado de manera expresa en la Ley N.º 30096, además, presenta también la forma de poder determinar si la RENIEC, cuenta con un sistema eficaz que permita la correcta protección y la no vulneración del derecho a la identidad, desarrollando para esto una tesis cualitativa, con un diseño documental y de carácter descriptivo, por lo que se encontraría dentro de una investigación básica, concluyendo así que el delito de *phishing* es un delito informático que cumple con las características de un comportamiento que se aprovecha del uso indebido de tecnologías de la información y de la comunicación para así obtener el acceso ilícito de datos informáticos privados y usarlos en perjuicio de sus víctimas, además, este delito no se encuentra expresamente tipificado en la Ley N.º 30096, por lo que, no goza de una tipificación legal y propicia que continue su impunidad.

De la tesis anterior, si bien es cierto busca integrar al *phishing* como una modalidad de los delitos informáticos, esta solo se enfoca en el delito de suplantación

de identidad que desarrolla la Ley N.º 30096, sin embargo, en la presente investigación se busca integrar el *phishing* en las agravantes, porque este artículo al desarrollar un conjunto de circunstancias específicas, permite que esta modalidad se adecúe al tipo penal que lo considere como necesario para la comisión de ese delito.

1.3. Formulación del problema

¿Cuáles son los fundamentos jurídicos para incorporar el *phishing* como agravante en el artículo 11° de la Ley N.º 30096 – Ley de delitos informáticos en el Perú?

1.4. Objetivos

1.4.1. Objetivo general

Determinar los fundamentos jurídicos para la Incorporación del *phishing* como agravante en el artículo 11° de la Ley N.º 30096 – Ley de Delitos Informáticos en el Perú.

1.4.2. Objetivos específicos

- Identificar y analizar los bienes jurídicos afectados en la Ley N.º 30096 – Ley De Delitos Informáticos en el Perú.
- Identificar y definir las modalidades informáticas más frecuentes en la Ley N.º 30096 – Ley De Delitos Informáticos en el Perú.
- Identificar las agravantes reguladas en la Ley N.º 30096 – Ley De Delitos Informáticos, en base a las agravantes desarrolladas en la dogmática penal peruana.

1.5. Hipótesis

Los fundamentos jurídicos para incorporar el *Phishing* como una agravante en el artículo 11° de la Ley N.º 30096 – Ley De Delitos Informáticos son:

- La mayor gravedad del injusto penal que representa el *Phishing*.
- El incremento de la culpabilidad del autor con la utilización del *Phishing*.

1.6. Justificación

La presente tesis tiene una investigación económica, ya que se trata de abordar un problema que va generando más impacto en la realidad peruana desde el aspecto económico por su incidencia en el mercado, pues el internet ya no es solamente un simple instrumento que es utilizado por personas naturales, sino que también en la actualidad las personas jurídicas hacen uso del mismo a través de sus empresas, las cuales han ido utilizándolo para la realización de diversas transacciones comerciales y financieras, pues es evidente que el internet al ser de fácil acceso y ahorro de tiempo, ha ido generando que la sociedad deje atrás los procedimientos tradicionales, para sumergirse en el mundo tecnológico.

Asimismo, tiene una justificación teórica- jurídica, pues desde este aspecto la presente tesis toma en cuenta que es importante saber que en el internet también existen personas que realizan conductas delictivas, dando así lugar a los ciberdelitos, razón por la cual, el Estado peruano se ha encargado de crear la Ley De Delitos Informáticos – Ley N.º 30096 desde el año 2013, con la finalidad de sancionar aquellas conductas delictivas que sean cometidas en la red por los ciberdelincuentes, no obstante, cabe mencionar que en la presente ley no ha logrado regular adecuadamente todas las conductas delictivas, pues estas han sido presentadas en forma genérica sin establecer las conductas específicas existentes, ni las actuales que se vienen desarrollando a lo largo del tiempo, por lo que, su aplicación resulta inadecuada al momento de aplicar una sanción en determinados ciberdelitos, como es el caso del *phishing*, el cual viene siendo una de las modalidad más relevantes y comunes en nuestro país, y que con el pasar del tiempo se va incrementando en el ámbito informático en cuanto a los ciberdelitos, por lo que, los ciberdelincuentes hacen un uso descomedido de

esta modalidad, ya que existe un vacío legal que no proporciona la sanción adecuada y les permite seguir realizando estos actos sin el control necesario, lo que trae como consecuencia que exista la desprotección legal en esta modalidad, y hace que los bienes jurídicos que vienen siendo afectados por el *phishing*, sigan estando desprotegidos y que su aumento se dé cada día más. Es decir, esta investigación se justifica en analizar la necesidad de tipificar al *phishing* como una agravante más del artículo 11° de la Ley N.º 30096, esto debido a que el *phishing* es una de las modalidades más utilizadas por los ciberdelincuentes en la red, la misma que busca obtener información a través de links que hacen caer en error a sus víctimas, logrando así obtener contraseñas, datos personales, acceso de tarjetas y cuentas bancarias, para la comisión de otros delitos, creando así que las nuevas tecnologías tengan un aumento desmedido en las conductas ilícitas y que así se puedan aprovechar del poco conocimiento que tienen los usuarios en cuanto al uso adecuado de internet y de las seguridad tecnológica que este ofrece.

Finalmente, la presente también tiene una justificación social – práctica, porque ….la adecuada regulación del *phishing* como un delito, permitiría a los operadores de justicia, tanto jueces como fiscales, puedan realizar la persecución penal de este tipo de conductas, que vienen afectando a una gran parte de la población, y así sea más fácil la aplicación de sanciones adecuadas para quienes cometan estos ilícitos, y poder evitar la impunidad de conductas ilícitas, para consecuentemente poder reducir los índices de criminalidad en relación a este tipo de delitos informáticos en nuestro país.

1.7. Marco Teórico

1.7.1. Antecedentes legislativos de la Ley N.º 30096.

Los ciberdelitos iniciaron a finales de los siglos XX, los cuales en sus inicios fueron integrados dentro del Código Penal, pero debido a su constante cambio en

cuanto a su comisión delictiva, se creó una ley especial que pueda desarrollarla adecuadamente, por lo que, de acuerdo a la interpretación de Vega y Arévalo (2022), la cronología correcta sería la siguiente:

a) Hurto Telemático en el Código Penal de 1991: la legislación lo incorporó dentro del artículo 186° que señalaba lo siguiente:

> ***Artículo 186°:*** *el agente será reprimido con pena privativa de la libertad no menor de dos ni mayor de cuatro años, si el hurto es cometido:*
>
> ***(…)*** *Si el agente usa sistemas de transferencia electrónica de fondos, de la telemática en general, o viola el empleo de claves secretas, será reprimido con pena privativa de libertad no menor de tres ni mayo de seis años y con ciento ochenta a trescientos sesenta y cinco días – multa.*

Como se puede observar, originalmente en el delito informático su afectación jurídica era netamente patrimonial y se encontraba tipificada dentro del delito de hurto agravado.

b) Ley N.º 27309 y la incorporación de los artículos 207-A, 207-B y 207-C en el Código Penal: después de la incorporación del internet en nuestro país y el impacto que este generó con sus sistemas informáticos se logró la aprobación de la Ley 27309, el 17 de julio del 2000, la misma que incorporaría los artículos 207-A, 207-B y 207-C en el Código Penal, quedando de la siguiente manera:

> ***Artículo 207º-A. Interferencia, Acceso o copia indebida a base de datos, sistema o red de computadoras.***

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

En este artículo, se buscaba sancionar aquellas conductas que lesionaban, interferían o dañaban los datos, red o computadoras y se encontraban dentro de los delitos contra el patrimonio.

> ***Artículo 207º-B. Alteración, daño o destrucción de base de datos. (Sabotaje Informático)***
>
> *El que utiliza, ingresa o interfiere indebidamente una base de datos, sistema, red o programa de computadoras o cualquier parte de la misma con el fin de alterarlos, dañarlos o destruirlos, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años y con setenta a noventa días multa.*

En este delito, el principal objetivo era cuantificar el valor de la red, datos o sistemas que habrían sido alterados, pues además de la

protección patrimonial, también se buscará la seguridad informática en general.

> ***Artículo 207º-C. Circunstancias agravantes.***
>
> *En los casos de los Artículos 207º-A y 207º-B, la pena será privativa de libertad no menor de cinco ni mayor de siete años, cuando:*
>
> *1. El agente accede a una base de datos, sistema o red de computadoras, haciendo uso de información privilegiada, obtenida en función a su cargo.*
>
> *2. El agente pone en peligro la seguridad nacional.*

Este artículo planteaba las circunstancias agravantes a las conductas delictivas mencionadas anteriormente, buscando así sancionar con mayor pena al sujeto activo, si este se encontraba dentro de los incisos 1 y 2.

c) Ley N. ª 30076 y la incorporación del artículo 207-D en el Código Penal: esta ley tiene como fin principal combatir la inseguridad ciudadana, modificando así 28 artículos del Código Penal y creando 3 delitos adicionales, entre ellos el delito de tráfico ilegal de datos, que establece:

> ***Artículo 207-D. Tráfico ilegal de datos.***
>
> *El que, crea, ingresa o utiliza indebidamente una base de datos sobre una persona natural o jurídica, identificada o identificable, para comercializar, traficar, vender, promover, favorecer o facilitar información relativa a cualquier ámbito de la esfera*

personal, familiar, patrimonial laboral, financiera u otro de naturaleza análoga, creando o no perjuicio, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años.

El mismo, que busca regular la indebida comercialización de información personal, familiar o patrimonial mediante internet.

d) Proyecto de Ley N.º 034-2011: denominado Ley De Los Delitos Informáticos, presentado el 11 de agosto del 2011 por Juan Calos Eguren Neuenschwander, quien propone una legislación que combata y establezca las conductas delictivas que afectan los bienes jurídicos de los sistemas informáticos mediante el uso de tecnologías.

e) Proyecto de Ley N.º 307-2011: denominado Ley especial sobre delitos cometidos con el uso de las tecnologías de la información y las comunicaciones, presentado el 05 de octubre del 2011 por Octavio Salazar Miranda, quien propone una legislación que combata y establezca las conductas delictivas que afectan los bienes jurídicos de los sistemas informáticos mediante el uso de tecnologías, además de la creación del agente encubierto como nueva figura.

f) Proyecto de Ley N.º 1136-2011: denominado Ley que modifica el artículo 207 – C del Código Penal incorporando el delito de robo de identidad virtual, e incorpora el artículo 207 – D, delito informático agravado, presentado el 17 de mayo del 2012 por Tomás Zamudio Briceño, quien propone la modificación del artículo 207 – C que solo hacía referencia al acceso ilícito y al sabotaje informático como

agravantes, y crea la figura del robo de identidad virtual, la misma que serviría como antecedente al delito de suplantación de identidad, que aún no se encontraba tipificado en esa fecha.

g) **Proyecto de Ley N.º 1257-2011:** denominado Ley que agrava los delitos de violación del secreto de las comunicaciones, presentado el 14 de junio del 2012 por Tomás Zamudio Briceño, quien propone la agravación del delito de violación del secreto de las comunicaciones.

h) **Proyecto de Ley N.º 2112-2012:** denominado Ley que modifica e incorpora diversos artículos del Código Penal sobre uso ilegal del servicio de telecomunicaciones, presentado el 12 de abril del 2013 por Renzo Andrés Reggiardo Barreto, quien propone la modificación de los delitos de receptación y de hurto, además, solicita la incorporación del delito de fraude informático.

i) **Proyecto de Ley N.º 2398-2012:** denominado Ley que modifica el artículo 176 del Código Penal e incorpora el artículo 176 – B, el delito de utilización de los medios informáticos, telefónicos u otras tecnologías de transmisión de datos para ejercer influencia contra un menor para actividades sexuales explícitas o actos de connotación sexual, presentado el 21 de junio del 2013 por Gustavo Bernardo Rondón Fudinaga, quien propone incorporar el delito de uso de tecnologías para ejercer influencia en menores de edad en temas de índole sexual, que sería antecedente del delito de Child Grooming, que sería incorporado.

j) Proyecto de Ley N.º 2482-2012: denominado Ley que incorpora el artículo 175-A en el Código Penal tipificando el delito de acoso sexual infantil, mediante nuevas tecnologías de información y telecomunicaciones, presentado el 17 de julio del 2013 por Julia Tevez Quispe, quien propone la incorporación de este delito para que sea antecedente de la incorporación del delito de Child Grooming.

k) Proyecto de Ley N.º 2520-2012: denominado Ley de prevención de la Cibercriminalidad, presentado el 26 de julio del 2013 por Ollanta Humala Tasso y Juan Jiménez Mayor, quienes proponen una legislación que utiliza por primera vez la Cibercriminalidad como sinónimo de ciberdelincuencia, dejando libre la incorporación de modificaciones a los delitos y a sus términos, los cuales son base importante de la legislación contra la cibercriminalidad.

l) Ley N.º 30096: publicada el 22 de octubre del 2013, la misma que tiene por objeto prevenir y sancionar conductas ilícitas que afecten los sistemas y datos informáticos que sean de relevancia penal, y sean cometidas a través de tecnologías, con el fin principal de garantizar la lucha contra la ciberdelincuencia.

m) Proyecto de Ley N.º 2991-2013: denominado Ley que modifica la Ley N° 30096, Ley de delitos informáticos, presentado el 25 de noviembre del 2013 por Juan Carlos Eguren Neuenschwander, quien propone acoplarnos al contenido del Convenio de Budapest, indicando que varios artículos no cumplían con los parámetros establecidos por lo que no solo debían medicarse sustancialmente, sino también procesalmente.

n) **Proyecto de Ley N.º 2999-2013:** denominado Ley que propone modificar los artículos 2 – 3 – 4 – 5 – 7 – 9 – 10, lo mismo en la tercera y cuartas disposición complementaria modificatoria en su artículo 162 C.P. y derogatoria de los artículos 6 y 8 de la Ley 30096, Ley de delitos informáticos, presentado el 27 de noviembre del 2013 por Mauricio Mulder Bedoya, quien propone la modificación de la ley de delitos informáticos y acoplarnos al Convenio de Budapest, además de evitar la impunidad en los ciberdelincuentes y cerrar espacios vacíos en la legislación.

o) **Proyecto de Ley N.º 3017-2013:** denominado Ley que modifica la Ley N° 30096, Ley de Delitos Informáticos, e incorpora el artículo 183 – B en el Código Penal presentado el 29 de noviembre del 2013 por Alberto Beingolea Delgado, quien propone la modificación de la Ley de delitos informáticos y solicita la incorporación al Convenio de Budapest, además plantea que la conducta del artículo 5 debería ser imputada también cuando las proposiciones se hagan de manera directa, sin necesidad de usar las TIC's para que se considere delito.

p) **Proyecto de Ley N.º 3048-2013:** denominado Ley que modifica la Ley de Delitos Informáticos, presentado el 05 de diciembre del 2013 por José Luna Gálvez, quien propone la modificación del delito de interferencia telefónica, para agregar como verbo rector la conducta prohibida que grava dicho tipo penal.

q) **Proyecto de Ley N.º 3105-2013:** denominado Ley que modifica la Ley de Delitos Informáticos, presentado el 18 de diciembre del 2013 por

Carmen Omonte Durand, quien propone la Ley de delitos informáticos y solicita la incorporación al Convenio de Budapest, en lo relativo a la cooperación internacional y cooperación interinstitucional.

r) **Ley N. ª 30171:** publicada el 10 de marzo del 2014, la misma que tiene por objeto modificar los artículos 2, 3, 4, 5, 7, 8 y 10 de la Ley N.º 30096, Ley de Delitos Informáticos, las cuales fueron consideradas como necesarias para su mejor aplicación en la técnica legislativa.

1.7.2. Glosario de digitalización.

Con respecto al problema planteado se tienen algunos conceptos claves que van a permitir conocer un poco más el tema de investigación; empezando así por los principales términos utilizados en la era de la digitalización, se definen de la siguiente manera:

- **Mula o mulero:** son aquellas personas que, actúan haciendo posible la consumación del hecho, brindando sus cuentas bancarias para transferencias que realizan el perjuicio patrimonial de las víctimas de estos delitos.
- **Ingeniería social:** proceso de la comunicación que busca engañar a un usuario con la finalidad de sacarle dinero o suplantar su identidad, para obtener datos personales del mismo o de terceros (Sain, 2018).
- **Informática:** Jiménez (2017) la define como aquella disciplina que investiga la estructura y la propiedad de la información científica, y a su vez hace posible el tratamiento automático y racional de la información por medio de un ordenador.

- **Delito Informático:** es la acción que reúne las características que delimitan el delito que vulnera los derechos de autor del titular de un elemento informático, ya sea hardware o software (Davara, 1995).
- **Hardware:** según la Real Academia Española, es aquel conjunto de componentes que conforman la parte física de una computadora (Jiménez, 2017).
- **Software:** a diferencia del Hardware, es el conjunto de programas, instrucciones y reglas que se encuentran en la computadora, para entenderlo mejor es aquel equipamiento lógico de un ordenador. (Jiménez, 2017)
- **Spam:** Correo electrónico masivo no solicitado destinado a transmitir publicidad comercial de forma gratuita o engañar a las personas para que visiten páginas web ilegales o sospechosas. (Rojas, 2013)
- **Ciberdelito:** acto ilícito que es cometido mediante el uso de internet, computadora, telemática y uso de las TICs, con el fin de poder acceder a los sistemas informáticos para sustraer datos, dañar programas y suplantar la identidad y así poder causar perjuicio a terceros. (Jiménez, 2017)
- **Ciberespacio:** es el entorno virtual en el cual se realiza un hecho punible, ya que es difícil de ser perseguido por el espacio virtual existente, y en donde se tiene más oportunidad de escape. (Jiménez, 2017)
- **Ciberdelincuencia:** es aquel comportamiento ilícito que se realiza a través de operaciones electrónicas, que atentan la seguridad de los datos personales que se procesan, además, son aquellas acciones ilegales que tienen como objetivo principal destruir y dañar la confidencialidad, integridad y disponibilidad de los sistemas a través del internet. (Jiménez, 2017)

1.7.3. Modalidades para obtener la información en los ciberdelitos.

En este punto se van a desarrollar las diferentes modalidades que utilizan los ciberdelincuentes para poder obtener la información privada de sus víctimas y así poder cometer diferentes ilícitos penales:

i. **Falso bono Estatal**: este tipo de estafa se produce a través de mensajes de texto o redes sociales, en las que solicitan a la víctima el ingreso de su información personal y financiera, además de un depósito de una cantidad exacta de dinero o recargas telefónicas, las cuales estarían dentro del delito de estafa en el artículo 196° del Código Penal. (Espinoza, 2022, p.118)

ii. **Falsa retención bancaria:** esta modalidad se da a través de mensajes en redes sociales, en las cuales el ciberdelincuente envía información al azar y adjunta un link de *phishing* en el cual solicita a sus víctimas el ingreso de sus datos alegando que se le ha realizado una retención bancaria de sus fondos, por lo que, deberá ingresar información obligatoriamente, esta modalidad se configura como el delito de estafa agravada para acceder o sustraer los datos de una tarjeta bancaria, y está tipificado en el artículo 196 – A inciso 5 del Código Penal. (Espinoza, 2022, p.118)

iii. **Falsa oferta de trabajo:** esta modalidad fue más frecuente durante la pandemia del COVID-19, y se produce a través de anuncios en redes sociales mediante convocatorias de trabajo con atrayentes salarios para empresas mineras, constructoras, entre otra, las cuales luego de contactar a su víctima exigen el pago de sumas de dinero para la

realización de capacitaciones, las cuales nunca llegan a producirse, pues después el ciberdelincuente desaparece, está modalidad configura el delito de estafa, y se encuentra dentro del artículo 196° del Código Penal. (Espinoza, 2022, p.118)

iv. **Reposición de chips con fines de fraude informático:** esta modalidad es bastante común y se realiza a través de ciberdelincuentes que tienen como cómplices a empleados de empresas de telefonía, y su forma de cometer estos delitos es la siguiente:

   a. El ciberdelincuente llama a una empresa telefónica suplementando la identidad del titular, para así poder bloquear la línea telefónica seleccionada.

   b. El cómplice, repone dicho chip en un distribuidor de la empresa telefónica.

   c. Se envían mensajes a los bancos del titular, solicitando la reposición de sus claves secretas.

   d. Realizan transferencias bancarias a cuentas de terceras personas, para que estas actúen como *mulas o receptores* de dichas transferencias bancarias que no fueron autorizadas por el titular.

Ante esta modalidad, el Organismo Supervisor de Inversión Privada en Telefonía (Osiptel), dispuso que, desde el 12 de junio del 2022, todas las empresas telefónicas deberán brindar una contraseña única a sus usuarios, para que éstos puedan evitar suplantación de identidad en sus chips, y así se evite el fraude informático, pues este supuesto configura

el delito de suplantación de identidad y fraude informático, en los artículos 8 y 9 de la Ley N.º 30096. (Espinoza, 2022, pp.118 - 119)

v. **Creación de falsa página de red social para solicitar dinero:** esta modalidad es común mediante la creación de perfiles falsos en redes sociales, de personas conocidas, profesionales o empresas, para lo cual el ciberdelincuente utiliza nombres y fotografías de las mismas para hacerse pasar por ellos, y así poder solicitar dinero a sus contactos, este supuesto configura el delito de suplantación de identidad, en el artículo 9° de la Ley N.º 30096. (Espinoza, 2022, p. 119)

vi. **Estafas piramidales y mediante el uso de criptomonedas:** estas estafas son muy frecuentes en la actualidad y aparecen en internet a través de anuncios de inversión informática lucrativa, la cual requiere un pago por derecho de admisión y además, que se reclute a otras posibles víctimas quienes deberán realizar la misma acción del pago del derecho de admisión, para que de este pago una parte sea el gancho para la persona que reclutó y el resto va directo al creador de la pirámide, asimismo, las criptomonedas son inversiones de alto riesgo, debido a la volatilidad que presenta, pues con esto solo se cometen delitos de estafa simple, ya que al no ser una moneda oficial y emitida por una entidad financiera, no se configuraría como un delito de estafa agravada, por lo que, se encuentra como estafa simple dentro del artículo 196° del Código Penal. (Espinoza, 2022, pp. 119 - 120)

vii. **Carta nigeriana:** en esta modalidad se da a través de un correo electrónico en el cual se escribe a la posible víctima y se le hace creer

que ha sido beneficiada con una herencia familiar, un testamento, etc., en los cuales solicitan los datos personales o el envío de una cantidad de dinero para concretar el beneficio, este delito configura estafa simple y está dentro del artículo 196° del Código Penal. (Espinoza, 2022, p.120)

viii. **Sexting:** aquí se da el envío y recepción de imágenes y vídeos de contenido sexual entre dos personas, este envío no configura un delito en sí mismo, pero, si es difundido a través de las redes sociales, páginas web u otro medio electrónico dentro de la red, se estaría cometiendo el delito de difusión de imágenes, materiales audiovisuales o audios con contenido sexual, en el artículo 154 – B del Código Penal. (Espinoza, 2022, p. 120)

ix. **Grooming o Child Grooming:** esto se da cuando un mayor de edad se acerca una persona menor de 14 años, con la finalidad de solicitarle imágenes o vídeos de contenido sexual o para realizar actos de connotación sexual, con él o con otra persona, este delito se considera previo a la pornografía infantil, sin embargo, es un delito independiente, ya que el simple hecho de solicitar material con contenido sexual a una persona menor de 14 años, se encuentra dentro del delito de proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos. (Espinoza, 2022, p. 120)

x. **Revenge porn:** esto se llama a la venganza pornográfica y consiste en la publicación de contenido de connotación sexual no autorizado por la otra persona o víctima que realizó dichas imágenes, en este caso el

sujeto activo de este delito mayormente suelen ser ex's parejas o personas que tienen una rivalidad con la víctima, y su fin principal es vengarse realizando la publicación de vídeos o fotografías de contenido sexual, lo cual está configurado en el delito de difusión de imágenes, materiales audiovisuales o audios con contenido sexual que se encuentra dentro del artículo 154 – B del Código Penal. (Espinoza, 2022, pp. 120 - 121)

xi. **Ciberacoso:** aquí se encuentra el asedio reiterado a una persona sin su consentimiento, lo cual constituye el delito de acoso en el artículo 141 – A del Código Penal. (Espinoza, 2022, p. 121)

xii. **Stalking:** esta modalidad consiste en espiar a una persona acecharla u hostigarla, hasta que se realice la comisión del delito de acoso en el artículo 141 – A del Código Penal. (Espinoza, 2022, p.121)

xiii. **Cyberbullying:** esta modalidad es muy común en las redes sociales y la mayoría de veces se da entre menores de edad, lo cual va generando graves secuelas psicológicas y sociales para las víctimas, pues consiste en una conducta en que los sujetos activos desprecian a sus víctimas marginándolas o tratándolas mal, ya sean por motivos étnicos, religiosos o políticos, lo cual constituye el delito de discriminación e incitación a la discriminación dentro del artículo 323° del Código Penal. (Espinoza, 2022, p.121)

xiv. **Phishing:** esta modalidad consiste en el envío de links a través de correos electrónicos o mensajes en redes sociales, los cuales las víctimas al ingresar a estos links enviados van a recolectar los datos de

las tarjetas bancarias de sus titulares para realizar transferencias de dinero no autorizadas esta modalidad está dentro del delito de estafa agravada y el delito de fraude informático. en el artículo 196 – A en el Código Penal y artículo 8° de la Ley N.º 30096. (Espinoza, 2022, p. 121)

xv. **Smishing:** es una modalidad de phishing ya que se da a través de enlaces, pero estos se remiten a través de mensajes de texto y se configuran en el delito de estafa agravada y delito informático en el artículo 196° del Código Penal y la Ley N.º 30096. (Espinoza, 2022, p. 121)

xvi. **Vishing:** en esta modalidad el sujeto activo es un suplantador, y se hace pasar por otra persona para poder conseguir la información personal y financiera de sus víctimas y así poder usarlas en el delito de fraude informático, el que configura el delito de suplantación de identidad y fraude informático, en los artículos 9° y 8° de la Ley N.º 30096. (Espinoza, 2022, p. 122)

xvii. **Pharming:** esta modalidad consiste en crear páginas falsas de entidades bancarias u otras, con el fin de apoderarse de los datos de cuentas bancarias de usuarios para cometer el delito de abuso de mecanismos y fraude informático en los artículos 10° y 8° de la Ley N.º 30096. (Espinoza, 2022, p. 122)

xviii. **Skimming:** esta modalidad es la clonación o fotos de tarjetas bancarias, para utilizar datos en el fraude informático, y son colocados en los cajeros automáticos o en los agentes, para que la víctima al momento

de pasar su tarjeta se almacene dicha información en un dispositivo electrónico. (Espinoza, 2022, p. 122)

xix. **Keylogging:** esto se produce cuando se introduce un virus malicioso en la computadora o celular, que registra todo lo que se teclea y estaría dentro del delito de acceso ilícito. (Espinoza, 2022, p. 122)

xx. **Ransomware:** se trata de un secuestro de los datos informáticos que se encuentran en un determinado computador, a través del cual los ciberdelincuentes buscan conseguir con el pago de un dinero para poder acceder a dicha información y se configura el delito de acceso ilícito. (Espinoza, 2022, p. 122)

1.7.4. ¿Qué es el Phishing?

En primer lugar, es importante analizar a que se le denomina *phishing*, ya que no tiene un concepto en específico, pues aún no existe una definición que lo reconozca como tal, y esto es debido a que las conductas que utilizan los ciberdelincuentes son distintas y se realizan en toda la red, sin embargo, dichas conductas suelen presentar características en particular que las permiten ubicarlas dentro del *phishing*, y poder diferenciarlas de otros métodos informáticos delictivos.

Usualmente, esta palabra es utilizada para calificar a uno de los métodos más utilizados por los ciberdelincuentes, los cuales lo utilizan para estafar y obtener la información de sus víctimas de forma fraudulenta, requiriendo información detallada como: contraseñas, información de tarjetas o entidades bancarias a las que pertenecen, a través de links enviados en internet, haciéndolas caer en error.

Por otro lado, este término se deriva de la palabra *"fishing",* haciendo referencia al intento que se hace para que las víctimas muerdan un anzuelo. Además,

mayormente los hackers reemplazan la letra *"f"* con las letras *"ph"*, haciendo referencia a la antigua forma de hacking telefónico conocida como "phreaking".

En este sentido, se puede decir que en las últimas décadas surgió una nueva forma de comportamiento, que consistía en el envío masivo de correos electrónicos, en la actualidad, se utilizan links o enlaces los mismos que simulan una comunicación de carácter oficial con la empresa o persona suplantada, con el fin de obtener información confidencial, por parte de los usuarios que se convierten en sus víctimas y quienes son los seleccionados para recibir este tipo de mensajes.

Ante esto, es importante reconocer al sujeto activo que realiza el *Phishing*, quien es un estafador, que conoce técnicas de ingeniería social e informática, a través de la cual se gana la confianza de sus víctimas haciéndose pasar por una persona o empresa de confianza emitiendo un comunicado oficial a través de sus redes sociales en internet, mayormente mediante correos electrónicos, mensajes de difusión, links entre otros, los mismos tienen como función principal obtener información de carácter confidencial por parte de los receptores de este tipo de mensajes.

Finalmente, Leguizamón (2015) define al phishing como el proceso por el cual una persona es contactada por email o por teléfono por alguien que simula ser una institución legítima para obtener datos privados, tales como datos bancarios, contraseñas, datos personales, etc. para que luego esta información obtenida de forma fraudulenta sea utilizada para acceder a las cuentas personales de las víctimas y causar pérdidas económicas o suplantación de identidad.

1.7.5. Bien jurídico del Phishing

Es necesario saber que, al momento de identificar el bien jurídico protegido por el *phishing*, la mayoría de veces este se relaciona directamente con el ámbito bancario,

pues en la mayoría de veces el phisher utiliza esta modalidad para obtener información financiera de sus víctimas, y así luego poder utilizarlas para realizar transferencias bancarias a sus cuentas o a las de un tercero, por lo que, es un error común considerar que el *phishing* afecta únicamente al patrimonio, pues en la realidad, el *phishing* es un proceso que tiene como fin principal obtener la información confidencial de sus víctimas, sin la necesidad de que esta contenga un valor económico, ya que a veces, a través del *phishing,* una persona puede acceder a las redes sociales, email, one drive u otros servicios virtuales de su víctima, para solo mantener su información personal y así poder utilizarla posteriormente, lo cual nos permite evidenciar que el bien jurídico afectado por el *phishing,* solamente dependerá del tipo de uso que realice el phisher con la información personal que obtuvo de su víctima, y para qué tipo de delito busca aplicarlo posteriormente, por lo que, resulta importante poder identificar la confidencialidad de la información sensible como bien jurídico, pues típicamente este tipo de conducta vulnera la información obtenida para poder ser usada para otros fines.

1.7.6. Etapas del phishing

El *phishing*, al ser una conducta compleja y al presentar diversas etapas, hace que se complique su tratamiento jurídico, lo que dificulta el poder determinar cuándo es que se produce la afectación de un bien jurídico, por eso es importante reconocer las seis fases de ataque que presenta el *phishing***,** de acuerdo al análisis realizado por Valle (2013), siendo las siguientes:

- **Planificación:** Aquí el phisher, tiene que tomar las decisiones de lo que va a realizar, teniendo en cuenta a quién va dirigido el ataque, cómo, cuándo y dónde se va a realizar el ataque, qué tipo de truco va a utilizar,

qué medios utilizará y cuál es su objetivo principal, por lo que, en este caso se define también el nivel de aporte por parte de la víctima.

- **Preparación:** En esta fase, los ciberdelincuentes deben conseguir un software, que les permita obtener los datos de contacto, localizar el destino de ataque, preparar sus equipos y construir o diseñar las páginas web en las que realizarán el fraude, todo esto de acuerdo al tipo de delito que plantean ejecutar.
- **Ataque:** En este momento, el phisher requiere la actuación de sus víctimas, pues necesita que estas interactúen con los medios informáticos utilizados o creados, para que la comisión del delito se lleve a cabo.
- **Recolección:** Como su propio nombre lo dice, aquí se recogen los datos obtenidos mediante la fase anterior referente al ataque, pues aquí se llevó a cabo la interacción entre la víctima y los medios utilizados por el *phisher*, para la obtención de la información confidencial de su víctima, permitiéndole también obtener sus datos personales.
- **Fraude:** Una vez que ya se obtuvieron los datos personales de su víctima, sigue la comisión del delito, y es que en este caso los ciberdelincuentes realizan la estafa de forma directa o indirecta, vendiendo la información robada a otros phishers para que estos puedan cometer el delito.
- **Post - ataque:** Al ser la última fase, esto tiene como finalidad principal que el ciberdelincuente elimine las pistas que hayan quedado durante

toda la ejecución y así todos los implicados en el ataque pueden ser considerados como susceptibles durante el proceso.

1.7.7. Tipos de Phishing

Cuando hablamos de los tipos de *phishing*, no solo hablamos de su finalidad por la que se comete, sino en el procedimiento realizado por el phisher para obtener la información confidencial de sus víctimas, esto desarrollado bajo el análisis planteado por Valle (2013), de la siguiente manera:

- **Phishing engañoso:** es el envío de un correo electrónico engañoso en el que se suplanta a una empresa o institución de confianza, donde el receptor pulsa en el enlace contenido en el mensaje y es desviado de manera inconsciente a un sitio web fraudulento (Belisario, 2014).
- **Phishing basado en software malicioso – malware – based Phishing**: este refiere a cualquier tipo de ejecución de un software malicioso en el ordenador de la víctima, el mismo que se puede dar a través de cualquier acción que permita la ejecución del malware en su máquina, estas técnicas sociales buscan conseguir que el usuario interactúe con el contenido ofrecido para la obtención de su información. (Leguizamon, 2015).
- **Phishing basado en el DNS o Pharming**: Aquí se da la interferencia del proceso de búsqueda del nombre de dominio (la traducción de la dirección introducida en el navegador a la dirección IP). Y es que el pharming, supone un peligro mayor que algunas de las otras variantes que se han mencionado, ya que la colaboración de la víctima es aún

menor y, además, la careta empleada por los ciberdelincuentes es más real.

- **Phishing mediante introducción de contenidos:** Esta modalidad consiste en introducir contenido malicioso en un sitio web legítimo, en donde este contenido puede tener diversas modalidades, ya sea, redirigir a los visitantes a otra página, instalar algún tipo de malware en el ordenador de los usuarios, entre otros.
- **Phishing mediante la técnica del intermediario:** Esta técnica implica el posicionamiento del *phisher* entre el ordenador del usuario y el servidor web legítimo, siendo así que el delincuente cuenta con la capacidad de filtrar, leer, e incluso modificar la información que se transfiere desde el servidor atacado y viceversa, sin que las partes sean conscientes de la violación de su seguridad, siendo el principal objetivo el robo de información confidencial, ya sea para su uso, para una venta posterior, o para el secuestro de la sesión (session hijacking), en cuyo caso podrá mantener esa información.
- **Phishing de motor de búsqueda:** Aquí se crean páginas web para productos o servicios falsos, las mismas que introducen en los índices de los motores de búsqueda, en la cual esperan que los usuarios visiten estas páginas para realizar sus compras y proporcionen información confidencial, o directamente realicen transferencias bancarias, normalmente, las falsas ofertas suelen ser mejores que las ofrecidas por empresas legítimas, con el objetivo de atraer a más víctimas posibles.

- **Spear Phishing:** Esta es una técnica donde el phisher elige cuidadosamente a su víctima, la estudia, y luego realiza el engaño mediante medios informáticos, aquí el phisher usa un tipo de información personal de la víctima para elaborar un engaño convincente y así poder vulnerar su ciberseguridad.

1.7.8. Formas para detectar el Phishing

Finalmente, siguiendo la interpretación de Valle (2013), para poder detectar el *phishing*, es importante tener en cuenta las características más comunes que presenta este tipo de modalidad, las cuales son:

- **El uso de nombres de compañías conocidas,** pues los ciberdelincuentes actúan mediante una imagen corporativa la misma que debe ser conocida en el mercado, para que así generen confianza en los usuarios.
- **Uso del nombre real de un empleado que pertenece a la empresa**, con el fin de que este aparezca como responsable original del correo enviado, pues así el usuario al comunicarse con la empresa para confirmar la veracidad del correo, este brindará el nombre del remitente del correo, para que se pueda confirmar que dicha persona labora en su empresa.
- **Direcciones web con apariencia oficial**, en este caso, la mayoría de veces el correo electrónico de una empresa o tienda redirige a la página oficial de la misma, en este caso, el correo fraudulento lleva al usuario a un sitio web aparente de la empresa, el mismo que están funcionando solamente como pantalla para poder robar su información.

- **Factor miedo,** esto se da cuando la empresa comunica a sus clientes que se están dando una nueva modalidad de fraude o de actos informáticos delictivos, lo cual pone en alerta a los usuarios y evita que estos ingresen a determinados sitios web o correos electrónicos maliciosos, por lo que, en este caso el phisher amenaza a los usuarios indicándoles que pueden sufrir una posible pérdida económica, la cual afecta directamente a su cuenta como cliente, razón por la cual, el usuario en un momento de pánico accede a las indicaciones que el phisher le indica y se convierte en victima brindando la información necesaria para la comisión de otros delitos.

CAPÍTULO II: METODOLOGÍA

2.1. Tipo de investigación según la finalidad

El tipo de investigación fue básico, ya que como se indica en la doctrina, este tipo de investigación tiene como objetivo principal la obtención y recopilación de información para construir una base de conocimiento con el cual formular nuevas teorías o modificar las existentes y así poder incrementar los conocimientos teóricos, científicos o filosóficos, que forman parte de la investigación, pero sin buscar contrastarlos con algún aspecto práctico existente (Ingenium, 2020).

Siendo así que, en la presente investigación, fue básico porque si bien, en principio se buscó responder a la pregunta de investigación referida a ¿cuáles son los fundamentos jurídicos para incorporar el *phishing* como agravante en el artículo 11° de la ley N.º 30096 – Ley de delitos informáticos?, con ello, a su vez, se tuvo a bien lograr desde la perspectiva metodológica un aporte al desarrollo de mayor conocimiento en la rama del derecho penal y para que otros investigadores jurídicos tengan cierta base para emprender futuras investigaciones relacionadas a la presente y así generar nuevos argumentos que ayuden al desarrollo de más teorías o teorías más completas sobre el tema que se ha analizado.

2.2. Diseño de la investigación

El diseño fue no experimental, ya que como en la doctrina se indica, este diseño se caracteriza, porque en este la investigación el investigar emprende la búsqueda de datos sin la necesidad de hacer alguna maniobra con las variables (Hernández, Fernández y Baptista, 2016).

En base a ello, se puede decir que, en la presente investigación sólo se limitó a observar los hechos tal y como ocurrieron en su ambiente natural, sin que estos hayan sufrido

manipulación alguna por parte nuestra, es así que solamente se enfocó en lograr responder a la pregunta de investigación, alcanzar los objetivos y comprobar la hipótesis planteada, sobre la base del recojo y análisis de datos provenientes de distintas fuentes que tenían relaciona directa con las variables o categorías jurídicas de la presente tesis, como se diría en Derecho; pero, sin realizar algún experimento con aquellas, sino, tan solo se las abordo desde un aspecto abstracto, así pues una premisa fue explicar cómo es que la falta de una regulación legal sobre el *phishing* en nuestro ordenamiento jurídico, puede provocar que dicha conducta en nuestro país no pueda ser objeto de persecución penal y que dichos actos ilícitos puedan quedar impunes hasta la actualidad.

Pues, frente a dicha problemática, se busca dar solución mediante la integración del *phishing* como una agravante en el artículo 11° de la Ley de Delitos Informáticos – Ley N.º 30096, para que de este modo dicha conducta no siga siendo impune y que se permita a los operadores de justicia poder actuar apropiadamente frente a este tipo de fenómenos social tecnológico, teniendo como base las adecuadas normas legales, que le garanticen la correcta investigación penal.

2.3. Enfoque de la investigación

Esta investigación tuvo un enfoque cualitativo, el cual de acuerdo a Jaramillo, Valarezo y Astudillo (2014) consiste en que, en este tipo de investigaciones se emprende un análisis de los datos con el fin de categorizarlos, clarificarlos, sintetizarlos y compararlos, para así arribar a una visión más amplia respecto a la situación de lo estudiado.

Es así, que en esta investigación se analizaron los datos provenientes de fuentes como la doctrina, la ley y la jurisprudencia, en el sentido de identificar sus principales cualidades o características para ver el panorama real y completo del problema de investigación referido

a ¿cuáles son los fundamentos jurídicos para incorporar el *phishing* como agravante en el artículo 11° de la ley N.º 30096 – Ley de delitos informáticos?; de tal forma que eso permita encontrar las teorías jurídicas que ayuden a responder a esta pregunta de investigación, y se brinde recomendaciones y un aporte.

2.4. Alcance de investigación

El alcance de esta investigación fue descriptiva, ya que como lo indica Monje (2011) este señala que: "se propone este tipo de investigación describir de modo sistemático las características de una población, situación o área de interés. (…) busca únicamente describir situaciones o acontecimientos (p. 26)".

Es por esto que, esta investigación buscó describir la realidad problemática del phishing y su necesidad de integrarlo como una agravante más del artículo 11° de la Ley N.º 30096 – Ley de Delitos Informáticos en el Perú; por lo que, después de la búsqueda de la información, se logró definir e identificar al phishing dentro de la Ley de delitos informáticos, teniendo en cuenta, la interpretación de la noma, la identificación del verbo rector, el sujeto activo, el sujeto pasivo y el bien jurídico afectado por este delito, finalmente, se buscó conseguir conclusiones favorables que ayuden a confirmar la hipótesis planteada y así también poder brindar posteriormente una propuesta normativa para que el phishing sea considerado como una agravante más del artículo 11° de la Ley N.º 30096 – Ley de delitos informáticos en el Perú.

2.5. Población y muestra (Materiales, instrumentos y métodos)

2.5.1. Población

Esto se conoce como el grupo de personas, seres vivos, objetos, casos, situaciones, etc. sobre los cuales los investigadores están interesados en estudiar para comprobar la hipótesis planteada al respecto de ellos. Este conjunto posee una o más características, propiedades, atributos los cuales deben ser precisados en el tiempo y el espacio para que tenga un carácter inequívoco (Urquiaga, 2018).

2.5.2. Muestra

Esto es visto como una parte de la población, que tienen características que devienen de la misma, por lo cual, los resultados obtenidos en la muestra ayudan a generalizar a la población, según lo dice Carrasco (2005).

En función a lo expuesto, en la presente se planteo como muestra y población lo expuesto en la siguiente tabla.

Tabla 1

Población y muestra de la investigación

Población	**Muestra**
Principales normas nacionales en materia penal.	Ley N. ª 30096 – Ley De Delitos Informáticos en el Perú.
Principales autores en la doctrina internacional especializada en derecho penal	Vidal (2022). Dexia abogados (2022).
Principales autores en la doctrina nacional especializada en derecho penal	Jiménez (2017) Espinoza (2022) Vega y Arévalo (2022)

Principales casos de jurisprudencia nacional en derecho penal	RN 1960-2019, Lima Sur. RN 2134-2016, Callao.

Fuente. Elaboración propia

Como se aprecia, en la Tabla 1 se indica que la población estuvo referida a distintas fuentes del derecho principalmente normativa, doctrina y jurisprudencia, de las cuales se obtuvo una muestra, en base a muestreo de tipo no probabilístico o no aleatorio, porque se eligió de una manera intencionada haciendo uso de criterios de inclusión y exclusión.

Ahora bien, explicando los criterios de inclusión y exclusión usados en la presente, se tiene la siguiente tabla.

Tabla 2

Criterios de inclusión y exclusión de la tesis

Criterios de inclusión	**Criterios de exclusión**
Se relacionen a la pregunta de investigación.	Que no sea información de libre acceso.
Se relacionen a los objetivos de investigación.	Que no sea información jurídica sino de otras carreras distintas a Derecho.
Ayuden a verificar la hipótesis.	Que sean en idiomas extranjeros de poco uso.
Provengan de bases de datos de revistas indexadas y RENATI.	Que sea información de hace más de 20 años**.**

Fuente. Elaboración propia.

En la Tabla 2 se aprecia que se usaron criterios de inclusión y exclusión, referidos a diversos aspectos relacionados a la tesis que ayuden a lograr lo propuesto, además como otros aspectos en la exclusión referidos a aspectos meramente formales de la información.

2.5.3. Técnica

Es la ejecución de los medios auxiliares del método. El investigador utilizará una serie de procedimientos y acciones que permitan recolectar estructuradamente la información. Es necesario que este enuncie y describa las técnicas y rutas que utilizará (observación, entrevista, análisis casos, etc.), cómo y cuándo los aplicará (Urquiaga, 2018).

La técnica a emplearse en la presente investigación fue la que destacó los documentos relevantes, los mismos que fueron analizados minuciosamente con la información doctrinaria y legislativa sobre el tema de investigación, la cual fue la de **análisis de contenido.**

Para Andréu (2018) indica que el análisis de contenido en un sentido amplio, es una técnica de interpretación de textos, ya sean escritos, grabados, pintados, filmados u otra forma diferente, donde puedan existir toda clase de registros de datos, trascripción de entrevistas, discursos, protocolos de observación, documentos, etcétera, en donde el denominador común de todos estos materiales es su capacidad para albergar un contenido que leído e interpretado adecuadamente nos abre las puertas a los conocimientos de diversos aspectos y fenómenos de la vida social.

Esta técnica ayudó a fortalecer los puntos principales que forman parte del desarrollo del presente trabajo de investigación; aplicándolo de la siguiente forma: realizando recopilación de información, respecto al phishing, cómo se da, sus modalidades, el bien jurídico protegido, sus tipos y la falta de regulación en el sistema jurídico peruano; por lo que se recurrió a diversos medios para obtener la bibliografía necesaria, tales como libros, artículos, revistas, legislación nacional e internacional,

doctrina comparada en modalidad física y virtual, y noticias y páginas web nacionales e internacionales para conocer más sobre el tema.

2.5.4. Instrumentos

Es un recurso que utiliza el investigador para registrar información o datos sobre las variables que tiene en mente (Hernández, 2014), por lo que, en la presente investigación los instrumentos que se empleó fue **la ficha.**

Este instrumento permitió obtener la información necesaria (libros, revistas jurídicas, artículos online) para el desarrollo del marco teórico, se define como: "Documento donde el investigador recopila, con criterio selectivo y siguiendo ciertas normas técnicas, toda información sustancial referida a un tema específico, que luego le sirva para la sustentación teórica" (Rojas, 2002, p.29).

Este instrumento ayudó en la presente investigación al momento de la obtención de recolección de la información, la cual era necesaria para identificar y almacenar la información que fue utilizada en el desarrollo de la introducción, además, este instrumento se utilizó para realizar las síntesis de las ideas o conceptos básicos que se consideran de mayor importancia para la investigación, en las cuales se extrajeron información relevante de un texto extenso, para obtener conceptos que contengan ideas propias, a partir de datos que proporcionan los autores.

2.6. Procedimiento de recolección de datos

Primero, se buscó información en bases datos como RENATI y revistas indexadas donde se encontró información jurídica respecto al tema y problema de investigación, con base en ello, se estableció la población y muestra, y en concordancia con el problema de investigación planteado y los objetivos.

Luego, en función a la población y muestra se identificó las técnicas e instrumentos que se iban a usar para recoger los datos respecto a la muestra identificada. Así, se utilizó como instrumento la ficha y para analizar los datos recogidos de este instrumento se usó la técnica de análisis de contenido. Con el cual, se pudo obtener solo aquellos datos de documentos relevantes para la tesis, proveniente de normas nacionales, doctrina internacional y nacional y jurisprudencia nacional.

Con los resultados de lo obtenido en base a lo anterior, recién se pudo pasar a lo siguiente, que fue la discusión de los resultados, para lo cual se usaron los métodos de análisis de datos, siendo primero se usaron los métodos inductivo y comparativo. Ello, permitió arribar a una discusión de los resultados bajo una perspectiva metodológica más general. Pero, como la presente investigación se asienta en el campo del Derecho, entonces se usaron otros métodos de análisis de datos como el histórico, hermenéutico y dogmáticos, con ello se pudo desarrollar una discusión más específica para el campo del Derecho, según se detalla más adelante. Y así, se pudo generar las conclusiones y recomendaciones alineadas a la presente tesis.

En todo el procedimiento de la presente tesis, se usaron herramientas para almacenar y procesar los datos como: una computadora, un USB, un celular y programas informáticos como Microsoft, Word, Excel y PowerPoint.

2.7. Método de análisis de datos

Es el conjunto de procedimientos lógicos ordenados que se utilizan para investigar y obtener nuevos conocimientos (Urquiaga, 2018). Por otro lado, para Yañes (2014), es el procedimiento en donde el investigador tamiza los datos más relevantes de la información

procesada, para aplicar el método de la hermenéutica de forma clara y definitiva, por lo que, para el presente trabajo se utilizaron los métodos jurídicos y científicos:

2.7.1. Métodos de análisis científicos o generales.

- **Inductivo:** En la presente investigación se usó el método inductivo, ya que es característico de las investigaciones cualitativas, donde en lugar de iniciar con una teoría y luego dirigirse al mundo empírico para confirmar estos datos y resultados, el investigador ahora deberá comenzar examinando los hechos en sí y durante el proceso desarrolla una teoría coherente para representar lo que se está observando (Hernández, Fernández y Baptista, 2014).

  Este método al dirigirse desde lo particular hasta lo general, hace que se observe, se describa y se analice la realidad problemática para posteriormente desembocar en conclusiones y teorías, por lo que, en la presente investigación se analizaron los datos obtenidos de los informes emitidos por el Ministerio Público a nivel nacional a fin de conocer el porcentaje de delitos informáticos en el Perú, y poder reconocer cuantos se desarrollaron en materia del *phishing,* para así poder llegar a la conclusión de la necesidad de tipificación de dicha conducta para erradicar su impunidad.

- **Comparativo:** se aplica a las investigaciones cualitativas, la cual permite conocer la totalidad de los hechos y fenómenos de la realidad estableciendo sus semejanzas y diferencias en forma comparativa, dejando así que los resultados de las comparaciones metodológicas nos llevan lógicamente a encontrar la verdad. Este método se usó en la presente investigación para establecer las semejanzas y diferencias que presentan los ordenamientos jurídicos de otros

países con el nuestro, de acuerdo a la regulación establecida en los delitos informáticos, y específicamente sobre el *phishing*.

2.7.2. Métodos jurídicos

Al estar en el campo del Derecho, en la tesis se hizo necesario recurrir a métodos más de esta disciplina a fin de tener datos mas relevantes para la tesis. Así, se usaron estos:

- **Histórico:** Este método fue necesario porque ayudó a realizar un análisis de la normativa vigente, a fin de determinar si se regula o no la conducta delictiva materia de estudio conforme a la Ley N.º 30096 – Ley de Delitos Informáticos.
- **Hermenéutico:** es aquel método básico del conocimiento científico que implica la observación de los hechos o fenómenos fácticos y su interpretación, para determinar su significado y sentido. (Aranzamendi, 2013).

  En la presente investigación este método fue útil, porque ayudó a demostrar que el *phishing* es un fenómeno social que cobra mayor relevancia en la sociedad conforme los avances tecnológicos y a través de la actualidad, haciendo uso de la interpretación de jurisprudencia que permitió poder analizar los fundamentos jurídicos que se encuentran como problemática de la presente investigación y demostrar la necesidad de integración en nuestra normativa.
- **Dogmático:** Para Ramos (2000): Se inscribe en el ámbito de pensamiento que ubica al Derecho como una ciencia o técnica formal y, por consiguiente, como una variable independiente de la sociedad, dotada de autosuficiencia metodológica y técnica, ya que, una tesis de grado que se inspira en el método dogmático visualizará el problema jurídico solo a la luz de las fuentes formales.

En ese sentido, este método permitió que en la presente investigación se pueda recurrir a las fuentes formales del derecho como doctrina nacional e internacional y la normativa nacional, que nos brindó información necesaria para el adecuado análisis del *phishing*, y así poder confirmar la postura planteada respecto a la existencia de una regulación que permita sancionar las conductas punibles que no están correctamente reguladas en nuestro ordenamiento jurídico.

CAPÍTULO III: RESULTADOS

3.1. Objetivo específico 1: Identificar y analizar los bienes jurídicos afectados en la Ley N.º 30096 – Ley De Delitos Informáticos en el Perú.

Con respecto a este objetivo, los resultados a nivel normativo son los siguientes:

Tabla 3

Principales elementos de los tipos penales regulados en los artículos de la Ley N.º 30096 – Ley de Delitos Informáticos y del Phishing como delito a nivel normativo.

Tipos Penales Informáticos	***Sujeto Activo***	***Sujeto Pasivo***	***Verbo Rector***	***Modalidades***	***Bien Jurídico Protegido***
Artículo 2: Acceso ilícito	"El que"	Persona natural o jurídica	Acceder	Vulnera las medidas de seguridad.	Integridad Informática
Artículo 3: Atentado a la integridad de datos informáticos	"El que"	Persona natural o jurídica	Daña; Introduce: Borra; Deteriora; Altera; Suprime; Hace inaccesibles.	Usa un verbo rector para aplicar a los datos informáticos.	Integridad informática
Artículo 4: Atentado a la integridad de sistemas informáticos	"El que"	Persona natural o jurídica	Inutiliza; Impide; Entorpece; Imposibilita.	Afecta el funcionamiento de estos servicios.	Integridad y mantenimiento de los datos informáticos.
Artículo 5: Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos	"El que"	Persona natural, menor de 14 años y menor de edad de 28 a 14 años.	Contactar	Solicita u obtiene material pornográfico para proponerle llevar a cabo actos de connotación sexual con él o un tercero.	Libertad sexual e Indemnidad sexual.
Artículo 6: Tráfico ilegal de datos	**(*)** Artículo **derogado** por la Única Disposición Complementaria Derogatoria de la Ley N° 30171, publicada el 10 marzo 2014.				
Artículo 7. Interceptación de datos informáticos	"El que"	Persona natural o jurídica	Interceptar	Obtiene datos informáticos en transmisiones no públicas.	Integridad informática; Intimidad y Secreto de las comunicaciones.

Artículo 8: Fraude informático	"El que"	Persona natural o jurídica	Provecho ilícito.	Interfiere o manipula el funcionamiento de un sistema informático	Integridad informática, y Patrimonio
Artículo 9: Suplantación de identidad	"El que"	Persona natural o jurídica	Suplantar la identidad	Sustituye a una persona natural o jurídica, para generar un perjuicio, material o moral.	Fe pública y Patrimonio
Artículo 10: Abuso de mecanismos y dispositivos informáticos	"El que"	Persona natural o jurídica	Fabrica; Diseña; Desarrolla; Vende; Facilita; Distribuye; Importa; Obtiene.	Mediante mecanismos, programas u otros métodos informáticos, cometen delitos previstos en la presente Ley.	Integridad informática; Intimidad y Secreto de las comunicaciones

Fuente: Elaboración propia.

En la Tabla 3, se puede apreciar la identificación de los principales elementos de los tipos penales regulados en los artículos de la Ley N.º 30096 – Ley de Delitos Informáticos a nivel normativo, el mismo que permitió diferenciar al sujeto activo; sujeto pasivo; verbo rector; modalidad; y bien jurídico protegido, lo que va a permite que se pueda entender de forma general el tipo de conducta especifica que se deberá desarrollar en cada artículo para que se lleve a cabo el ilícito penal sancionado.

Con respecto a este objetivo, los resultados a nivel doctrinario son los siguientes:

Tabla 4

Principales elementos de los tipos penales regulados en los artículos de la Ley N.º 30096 – Ley de Delitos Informáticos a nivel de la doctrina.

Tipos penales informáticos	***Autor***	***Sujeto Activo***	***Sujeto Pasivo***	***Verbo Rector***	***Tipicidad Subjetiva***	***Bien Jurídico Protegido***
Artículo 2: Acceso ilícito	**Jiménez (2017)**	Cualquier persona con conocimientos informáticos.	Persona natural o jurídica y empresas.	Acceder	Dolo	Seguridad Informática

	Espinoza (2022)	Cualquier persona con conocimientos informáticos	Páginas estatales y personas jurídicas.	Acceder	Dolo	Ciberseguridad Confidencialidad Integridad
Artículo 3: Atentado a la integridad de datos informáticos	**Jiménez (2017)**	Cualquier persona con conocimientos informáticos	Persona natural o jurídica y empresas.	Dañar; Introducir: Borrar; Deteriorar; Alterar; Suprimir; inaccesibilidad.	Dolo	Integridad Confidencialidad Informatización de datos.
	Espinoza (2022)	Cualquier persona con conocimientos informáticos.	Personas jurídicas y páginas del Estado.	Dañar; Introducir: Borrar; Deteriorar; Alterar; Suprimir; inaccesibilidad.	Dolo	Ciberseguridad Intangibilidad informática.
Artículo 4: Atentado a la integridad de sistemas informáticos	**Jiménez (2017)**	Cualquier persona con conocimientos informáticos.	Persona natural o jurídica y empresas.	Inutilizar; Impedir; Entorpecer; Imposibilitar.	Dolo	Integridad Confidencialidad Disponibilidad de sistemas informáticos.
	Espinoza (2022)	Cualquier persona con conocimientos informáticos.	Páginas estatales y personas jurídicas.	Inutilizar; Impedir; Entorpecer; Imposibilitar.	Dolo	Intangibilidad informática.
Artículo 5: Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos	**Jiménez (2017)**	Cualquier persona mayor de edad con conocimientos informáticos	Menores de 18 años de edad.	Contactar	Dolo	Libertad sexual Indemnidad
	Espinoza (2022)	Cualquier persona mayor de edad con conocimientos informáticos.	Menor de 14 años de edad. Menor de 18 a 14 años de edad.	Contactar	Dolo	Indemnidad Libertad sexual
Artículo 6: Tráfico ilegal de datos	**(*)** Artículo **derogado** por la Única Disposición Complementaria Derogatoria de la Ley N° 30171, publicada el 10 marzo 2014.					
Artículo 7: Interceptación de datos informáticos	**Jiménez (2017)**	Cualquier persona con conocimientos informáticos.	Persona natural o jurídica y empresas.	Interceptar	Dolo	Secreto de las comunicaciones
	Espinoza (2022)	Cualquier persona con conocimientos informáticos.	Páginas estatales y personas jurídicas.	Interceptar	Dolo	Privacidad Intimidad

						Secreto de las comunicaciones.
Artículo 8: Fraude informático	**Jiménez (2017)**	Cualquier persona con conocimientos informáticos.	Persona natural o jurídica y empresas.	Provecho ilícito.	Dolo	Patrimonio Integridad Confidencialidad Informatización de datos.
	Espinoza (2022)	Cualquier persona con conocimientos informáticos.	Persona natural o jurídicas.	Provecho ilícito.	Dolo	Patrimonio
Artículo 9: Suplantación de identidad	**Jiménez (2017)**	Cualquier persona	Persona natural o jurídica y empresas.	Suplantar la identidad	Dolo	Fe pública
	Espinoza (2022)	Cualquier persona natural.	Cualquier persona natural o jurídica.	Suplantar la identidad	Dolo	Identidad en el entorno digital.
Artículo 10: Abuso de mecanismos y dispositivos informáticos	**Jiménez (2017)**	Cualquier persona con conocimientos informáticos.	Persona natural o jurídica y empresas.	Fabricar; Diseñar Desarrollar; Vender; Facilitar; Distribuir; Importar; Obtener.	Dolo	Varios bienes jurídicos protegidos de acuerdo al tipo de dispositivo.
	Espinoza (2022)	Cualquier persona con conocimientos informáticos.	Páginas estatales y personas jurídicas.	Fabricar; Diseñar Desarrollar; Vender; Facilitar; Distribuir; Importar; Obtener.	Dolo	Varios bienes jurídicos protegidos de acuerdo al tipo de dispositivo.

Fuente: Elaboración propia.

En la Tabla 4, se puede apreciar la identificación de los principales elementos de los tipos penales regulados en los artículos de la Ley N.º 30096 – Ley de Delitos Informáticos a nivel doctrinario, el mismo que diferencia al sujeto activo; sujeto pasivo; verbo rector; tipicidad subjetiva; y al bien jurídico protegido, lo que va a permite que se pueda entender de forma general la interpretación de ambos autores respecto a la normativa existente tipificada por la Ley N.º 30096, evidenciando las semejanzas en algunos elementos en cuanto

a la interpretación, y a las diferentes perspectivas en cuanto a los bienes jurídicos protegidos por cada delito.

3.2. Objetivo específico 2: Identificar y definir las modalidades informáticas más frecuentes en la Ley N.º 30096 – Ley De Delitos Informáticos en el Perú, de conformidad con datos reales obtenidos sobre la criminalidad informática en el Perú.

Con respecto a este objetivo, los resultados a nivel normativo son los siguientes.

Tabla 5

Modalidades informáticas más frecuentes en la Ley N.º 30096 – Ley De Delitos Informáticos en el Perú a nivel normativo.

Artículo	***Modalidad identificada en la norma***
Artículo 2: Acceso ilícito	Stalking Keylogging Ransomware
Artículo 5: Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos.	Sexting Grooming O Childgrooming
Artículo 8: Fraude informático	Falsa Retención Bancaria Carta Nigeriana Vishing Pharming Skimming Phishing
Artículo 9: Suplantación de identidad	Creación De Falsa Página De Red Social Para Solicitar Dinero Smishing Vishing Phishing
Artículo 10: Abuso de mecanismos y dispositivos informáticos.	Pharming

Fuente: *Elaboración propia.*

En la tabla 5, se hace referencia a las Modalidades informáticas más frecuentes en la Ley N.º 30096 – Ley De Delitos Informáticos en el Perú a nivel normativo, dejando ver que tipo de modalidades actuales se integran a artículos específicos, de acuerdo al tipo penal que estos desarrollan.

Con respecto a este objetivo, los resultados a nivel doctrinario son los siguientes:

Tabla 6

Modalidades informáticas más frecuentes en la Ley N.º 30096 – Ley De Delitos Informáticos en el Perú según lo definido en la doctrina.

Artículo	***Modalidad***	***Autor***	***Definición***
Artículo 8: Fraude Informático	FALSA RETENCIÓN BANCARIA	**Espinoza (2022)**	Esta modalidad se da a través de mensajes en redes sociales, mediante el envío de un link de *phishing*, el cual solicita el ingreso de datos personales, alegando que se le ha realizado una retención bancaria de sus fondos, por lo que, deberá ingresar información obligatoriamente.
		Vega y Arévalo (2022)	Estos ciberdelincuentes se basan en primero sustrae la identidad de sus víctimas para luego realizar fraudes con tarjetas de crédito en la red.
Artículo 9: Suplantación de Identidad	CREACIÓN DE FALSA PÁGINA DE RED SOCIAL PARA SOLICITAR DINERO	**Espinoza (2022)**	Esta modalidad es común mediante la creación de perfiles falsos en redes sociales, para lo cual se utiliza nombres y fotografías de las mismas a suplantar para hacerse pasar por ellos, y así poder solicitar dinero a sus contactos.
		Vega y Arévalo (2022)	Robo o fraude de identidad con la que se busca suplanta la identidad de un usuario en redes sociales, para luego cometer acciones fraudulentas.
Artículo 8: Fraude Informático	CARTA NIGERIANA	**Espinoza (2022)**	Esta modalidad se da a través de un correo electrónico en el cual se escribe a la posible víctima y se le hace creer que ha sido beneficiada con una herencia familiar, un testamento, etc., en los cuales solicitan los datos personales o el envío de una cantidad de dinero para concretar el beneficio.

		Vega y Arévalo (2022)	Son correos electrónicos enviados por el estafador para engañar al usuario, tratando de llama la atención de la víctima con un potencial beneficio patrimonial otorgado, para que este sea finalmente quien realice la disposición patrimonial al ciberdelincuente.
Artículo 5: Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos.	SEXTING	**Espinoza (2022)**	Esta modalidad se da mediante el envío y recepción de imágenes y vídeos de contenido sexual entre dos personas, lo que no configura delito, pero, si estas son difundidas a través de las redes sociales, páginas web u otro medio electrónico dentro de la red, se estaría cometiendo delito.
		Vega y Arévalo (2022)	Esta modalidad es un tipo de grooming online, el cual contiene fotografías propias de desnudos de menores de edad, para luego ser enviadas por sus teléfonos móviles con mensajes obscenos, de amor u odio, con la finalidad de conocer a nuevas personas en internet.
Artículo 5: Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos.	GROOMING O CHILDGROOMING	**Espinoza (2022)**	Esto se da cuando un mayor de edad se acerca una persona menor de 14 años, con la finalidad de solicitarle imágenes o vídeos de contenido sexual o para realizar actos de connotación sexual, con él o con otra persona.
		Vega y Arévalo (2022)	Esta modalidad se basa en contactar a menores de edad a través de las redes sociales, para acercarse a ellos y posteriormente logar un contacto sexual.
Artículo 2: Acceso ilícito	STALKING	**Espinoza (2022)**	Esta modalidad consiste en espiar a una persona acecharla u hostigarla.
		Vega y Arévalo (2022)	Considerado también como ciberacoso continuado, pues se utiliza del internet para seguir, hostigar y perseguir a la víctima, además, también se usa para amenazar, insultar y dejar mal la imagen de una persona.
Artículo 9: Suplantación de identidad	SMISHING	**Espinoza (2022)**	Esto es una modalidad de phishing y se da a través de un enlace, los cuales se remiten solamente a través de mensajes de texto.

		Vega y Arévalo (2022)	En este tipo se hace uso de técnicas de ingeniería social mediante equipos celulares para que la víctima ingrese a un hipervínculo, llame a un número telefónico, o responda un mensaje de texto.
Artículo 8: Fraude informático **Artículo 9:** Suplantación de identidad	VISHING	**Espinoza (2022)**	En esta modalidad el sujeto activo es un suplantador, y se hace pasar por otra persona para poder conseguir la información personal y financiera de sus víctimas y así poder usarlas después.
		Vega y Arévalo (2022)	Este tipo de practica se da en los mensajes de voz a través de teléfono móvil, haciendo uso de una IP, para obtener información, persona, financiera o confidencial.
Artículo 8: Fraude informático **Artículo 10:** Abuso de mecanismos y dispositivos informáticos.	PHARMING	**Espinoza (2022)**	Esta modalidad consiste en crear páginas falsas de entidades bancarias u otras, con el fin de apoderarse de los datos de cuentas bancarias de usuarios.
		Vega y Arévalo (2022)	Esta modalidad cambia el contenido de la página original por una página muy parecida o iguala a la original, la misma que hace caer en error a los usuarios.
Artículo 8: Fraude informático	SKIMMING	**Espinoza (2022)**	Esta modalidad es la clonación o fotos de tarjetas bancarias, para utilizar los datos en el fraude informático, y así sean colocados en los cajeros automáticos o en los agentes, para que la víctima al momento de pasar su tarjeta se almacene dicha información en un dispositivo electrónico.
		Vega y Arévalo (2022)	Modalidad de clonación de tarjetas, a través de engaños a sus víctimas bandas magnéticas de clonación para que el usuario no sospeche al momento de realizar su operación que su tarjeta está siendo clonada.
Artículo 2: Acceso ilícito	KEYLOGGING	**Espinoza (2022)**	Aquí se produce cuando se introduce un virus malicioso en la computadora o celular, para que registre todo lo que se teclea.
		Vega y Arévalo (2022)	Tipo de hardware que registra las pulsaciones que hace el teclado para memorizarlas y después enviarlas al ciberdelincuente para que este ingrese a la información de la víctima o a su patrimonio.

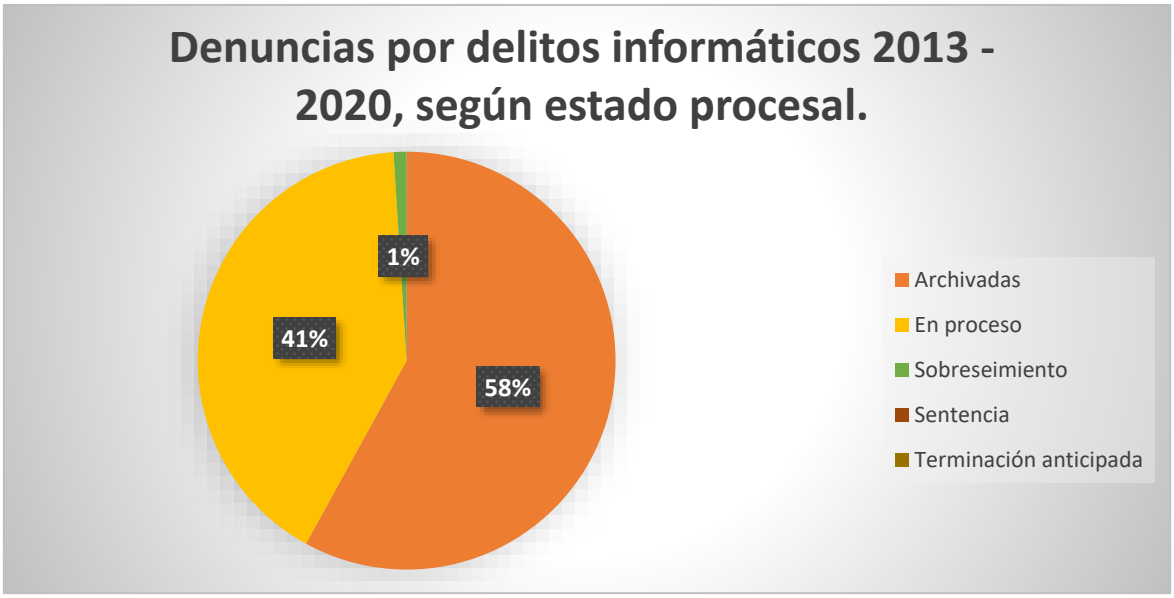
Artículo 2: Acceso ilícito	RANSOMWARE	**Espinoza (2022)**	Esta modalidad se trata de un secuestro de los datos informáticos que se encuentran en un determinado computador, a través del cual los ciberdelincuentes buscan conseguir con el pago de un dinero para poder acceder a dicha información.
		Vega y Arévalo (2022)	Esta modalidad contiene un tipo de malware que impide que los usuarios accedan a sus archivos personales o sistemas, y exige el pago de un rescate de información para poder acceder a ellos.
Artículo 8: Fraude informático **Artículo 9:** Suplantación de identidad	PHISHING	**Espinoza (2022)**	Esta modalidad consiste en el envío de links a través de correos electrónicos o mensajes en redes sociales, para que las víctimas al ingresar a estos links enviados y brindaran información personal que será recolectada para luego acceder a las tarjetas bancarias sin inconvenientes.
		Vega y Arévalo (2022)	Esta modalidad es un mecanismo que se desarrolla dentro de la ingeniería social para robar los datos de la identidad de personal de sus consumidores, y luego acceder a sus tarjetas de crédito y cuentas propias.

Fuente: Elaboración propia.

Respecto a la tabla 6, se hace referencia a las modalidades informáticas más frecuentes en la Ley N.º 30096 – Ley De Delitos Informáticos en el Perú, dejando ver que entre los 13 tipos de modalidades desarrollados, de acuerdo a la interpretación de ambos autores, se debe tener en cuenta que en su gran mayoría, y de acuerdo a su definición, hacen referencia al *phishing* y se consideran como tipos o parte integrante del phishing, lo cual deja en evidencia que si se considera analizar detalladamente cada modalidad antes descrita, la gran mayoría de modalidades tienen como base la forma de actuar del phishing, para así poder desarrollar lo mismo en un tipo de conducta en específico para la comisión de esos delitos.

Figura 1

Denuncias por delitos informáticos en el Perú durante 2013 – 2020, según estado procesal.

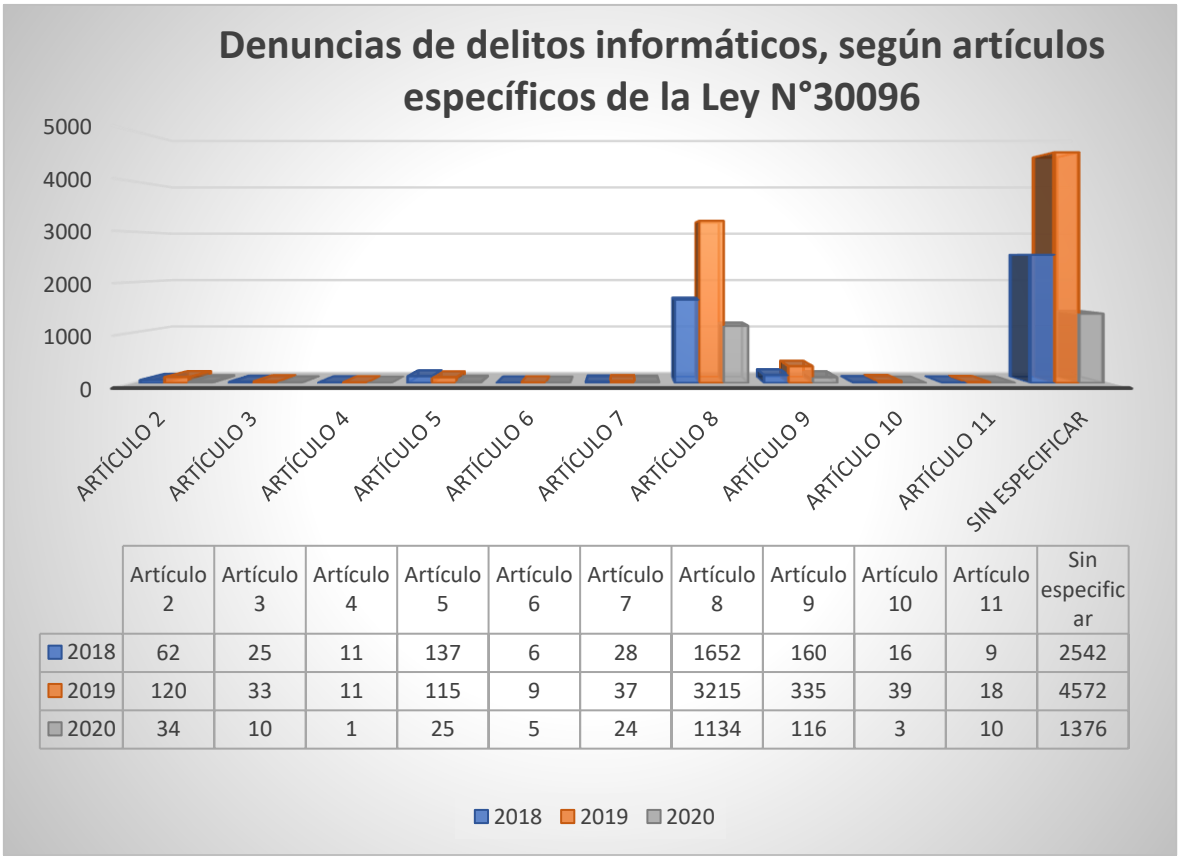


Fuente: Adaptado de "Denuncias registradas por la división de delitos de alta Tecnología" (p. 26)**,** por Oficina De Análisis Estratégico Contra La Criminalidad, 2021, *Ciberdelincuencia: pautas para una investigación fiscal especializada,* Informe de análisis N° 04.

De acuerdo al a Figura 1, se puede evidenciar que en el estudio realizado por el Ministerio Público, desde el año 2013 se han cometido delitos informáticos en el Perú, dejando ver que en la actualidad el 58% de las denuncias han sido archivadas por falta de adecuación en el tipo penal de algún artículo que integra la Ley de Delitos Informáticos, por otro lado, el 41% se encuentran en proceso de investigación y juzgamiento, de las cuales la gran mayoría fueron sobreseídas y un menor número de estas se acogió a la terminación anticipada, finalmente, son menos del 1% aquellos casos que llegaron a sentencia, datos que nos permiten conocer el incremento de delitos informáticos durante este tiempo, teniendo en cuenta que, durante la pandemia hasta la actualidad se dio un aumento desenfrenado en este tipo de delitos, por el nuevo estilo de vida tecnológico al que tuvieron que adaptarse las personas en este periodo para la realización de sus actividades cotidianas.

Figura 2

Denuncias de delitos informáticos, según artículos específicos de la Ley N.º 30096.



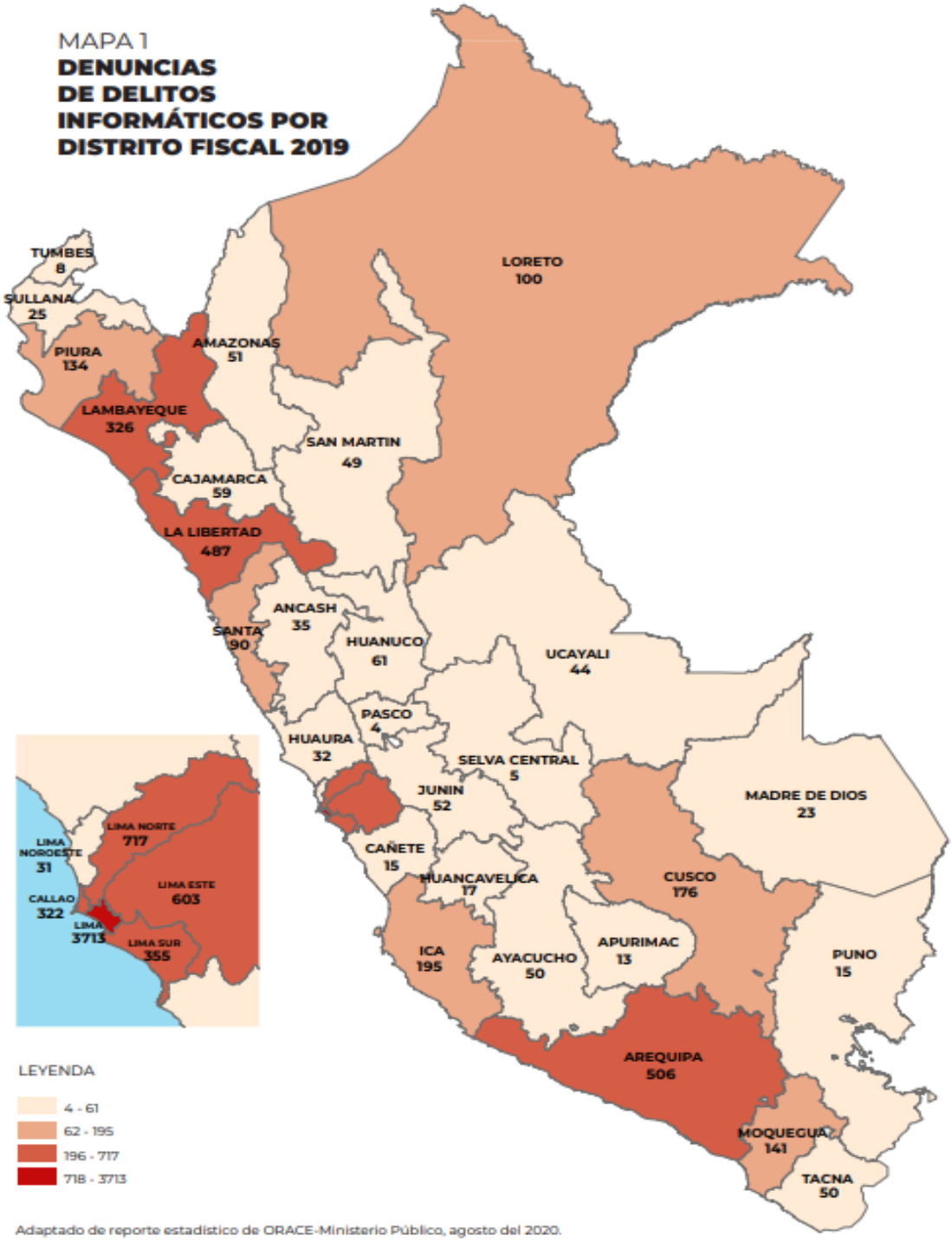
	Artículo 2	Artículo 3	Artículo 4	Artículo 5	Artículo 6	Artículo 7	Artículo 8	Artículo 9	Artículo 10	Artículo 11	Sin especificar
2018	62	25	11	137	6	28	1652	160	16	9	2542
2019	120	33	11	115	9	37	3215	335	39	18	4572
2020	34	10	1	25	5	24	1134	116	3	10	1376

Fuente: Adaptado de "Denuncias registradas por la división de delitos de alta Tecnología" (p. 26)**,** por Oficina De Análisis Estratégico Contra La Criminalidad, 2021, *Ciberdelincuencia: pautas para una investigación fiscal especializada,* Informe de análisis N° 04.

Tomando como referencia la figura anterior, se puede evidenciar que, en el periodo del 2018 a julio del 2020, se registraron un total de 15890 denuncias, en todos los artículos de la Ley de Delitos informáticos, dejando ver también que el año con más registro de denuncias fue el año 2019 en el cual el delito de fraude informático registro un total de 3215 denuncias ese año, sin embargo, ese mismo año se registraron 4572 denuncias sin especificar un delito en especial, esto debido a que la Ley N° 30096, tiene muchos vacíos legales que no permiten una adecuada interpretación de los hechos, para que se puedan identificar estos tipo de actos en un solo delito, generando así que su comisión sea más recurrente por falta de legislación aplicable a los mismos.

Figura 3

Denuncias de delitos informáticos por distrito fiscal año 2019.



Fuente: Adaptado de "Denuncias registradas por la división de delitos de alta Tecnología" (p. 23)**,** por Oficina De Análisis Estratégico Contra La Criminalidad, 2021, *Ciberdelincuencia: pautas para una investigación fiscal especializada,* Informe de análisis N° 04.

Figura 4

Denuncias de delitos informáticos por distrito fiscal año 2020.

Fuente: Adaptado de "Denuncias registradas por la división de delitos de alta Tecnología" (p. 24)**,** por Oficina De Análisis Estratégico Contra La Criminalidad, 2021, *Ciberdelincuencia: pautas para una investigación fiscal especializada*, Informe de análisis N° 04.

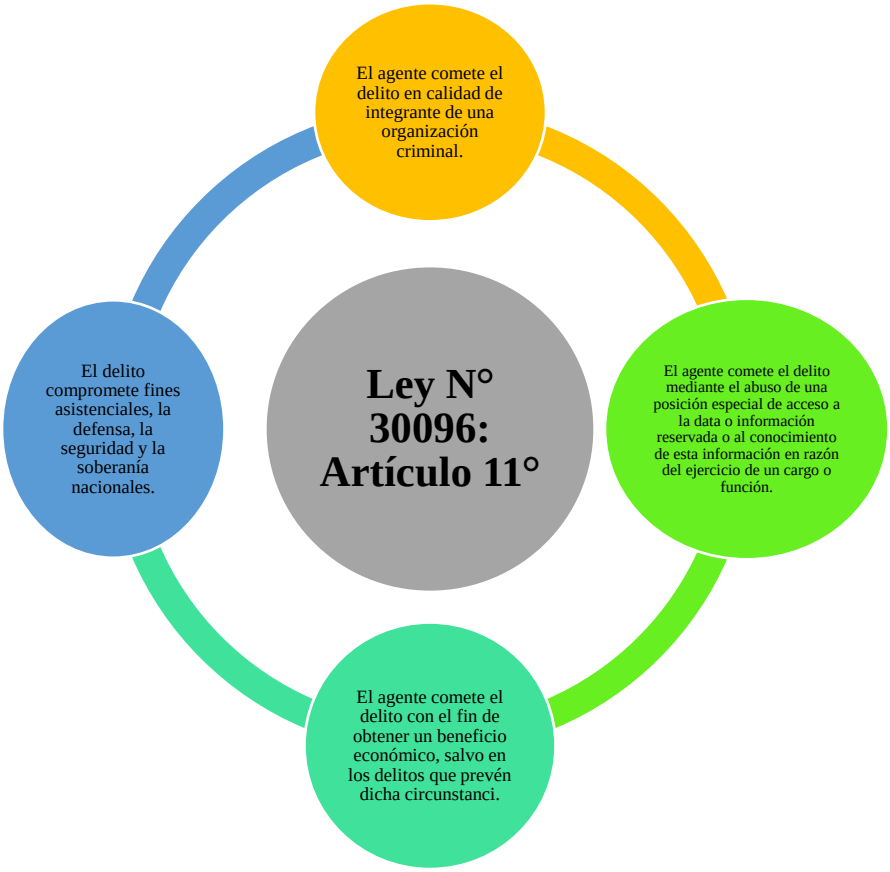
Como se pueden observar en la Figura 3 y Figura 4, estas imágenes nos permiten ver el número de delitos informáticos que se han cometido en cada Distrito Fiscal a nivel del Perú, teniendo en cuenta que, son solo delitos informáticos durante el año 2019 – 2020, lo cuales ingresaron de forma indistinta a Fiscalías Penales, Fiscalías Penales Especializadas y Fiscalías Mixtas a nivel nacional, todo esto de acuerdo al Sistema de Gestión Fiscal (SGF) y al Sistema Integrado de Apoyo de Trabajo Fiscal (SIATF) del Ministerio Público, las cuales registraron el aumento masivo de dichos delitos en cada ciudad, permitiendo así que se pueda llevar un monitoreo respecto a los incrementos constantes que se dan en este tipo de delitos en nuestro país, siendo importante que se tenga en cuenta dicho incremento para tener una regulación adecuada y que se encuentre con la tipificación específica para que estos delitos se puedan adecuar a la normativa vigente y puedan tener una sanción proporcional de acuerdo a la afectación al bien jurídico protegido que dicha acción genere.

3.3. Objetivo específico 3: Identificar las agravantes reguladas en la Ley N.º 30096 en base a las agravantes desarrolladas en la dogmática penal peruana.

Con respecto a este objetivo, los resultados a nivel normativo son los siguientes.

Figura 5

Identificación de las agravantes en la Ley N.º 30096 – Ley de Delitos Informáticos.



Fuente: Elaboración propia.

La Figura 5, contiene información respecto a las agravantes que se desarrollan en el artículo 11° de la Ley N.º 30096 – Ley de Delitos Informáticos, las mismas que desarrollan el aumento de la pena hasta un tercio por encima del máximo cuando los delitos previstos en la presente ley constituyan cualquiera de los supuestos redactados en el presente artículo, para determinar el tipo de agravante que va a presentar.

Con respecto a este objetivo, los resultados a nivel doctrinario son los siguientes.

Figura 6

Identificación de las agravantes en la dogmática penal.

Fuente: *Elaboración propia.*

La Figura 6, contiene información respecto al tipo de agravantes existentes en el Derecho Penal, permitiendo poder identificarlas a nivel nacional e internacional, y en la normativa correspondiente, pudiendo concluir que existen 3 tipos de agravantes, siendo genéricas, específicas y cualificadas, en cuanto al primer tipo de agravantes se tiene que, son aquellas que no están destinadas para un solo tipo penal en específico, sino que su actuación puede ser aplicada a todos los delitos existentes; en el segundo tipo de agravantes, las especificas solo se regulan en la parte especial, por lo que se estas se desarrollan en un párrafo adicional y dentro de determinados delitos; como tercer tipo de agravante se tienen a las cualificadas, las que su eficacia incide solamente en la estructura de la pena conminada, lo que significa que sus efectos pueden alterar o modificar los límites máximos o mínimos previstos en cada delito, creando así un nuevo marco penal conminada; finalmente, de acuerdo al análisis de los conceptos obtenidos en la figura se concluye que las agravantes que desarrolla la Ley N.º 30096, son agravantes genéricas, toda vez que pueden aplicarse a todos los artículos de la presente ley, siempre y cuando cumplan con las condiciones descrita en el artículo correspondiente.

CAPÍTULO IV: DISCUSIÓN Y CONCLUSIONES

4.1. Discusión

Con el transcurso del tiempo, la tecnología ha ido desarrollando nuevas formas de atentado contra la ciberseguridad a través de nuevas modalidades digitales que hoy en día no se encuentran reguladas por un ordenamiento jurídico peruano, si bien es cierto el Perú cuenta con la Ley N.º 30096 – Ley de Delitos Informáticos, la misma que busca sancionar este tipo de conductas, hasta la fecha no ha tenido ninguna modificación, lo que ha ido generando que estas nuevas modalidades delictivas no se encuentren reguladas, como lo es en el caso del *phishing.*

4.1.1. Objetivo 1: respecto a este objetivo es necesario describir los elementos del tipo penal que desarrolla esta ley, teniendo en cuenta que:

- **Primero:** al hablar del sujeto activo, se hace referencia a un delito común, pues al no describir con características especiales para este sujeto, permite que dicha conducta pueda ser cometida por cualquier persona que cuente con conocimientos promedios o avanzados sobre temas de informática, ya que es el espacio donde se desarrollan este tipo de delitos.
- **Segundo:** al mencionar al sujeto pasivo, la presente ley considera como posibles agraviados a cualquier persona natural o jurídica, salvo el artículo 5 que desarrolla el delito de **Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos,** el mismo que identifica como agraviado a los menores de edad, para que encajen dentro de esta figura delictiva, pues el objetivo principal de estos delitos es afectar la ciberseguridad de las plataformas virtuales que contienen

la información personal y reservada de sus víctimas, para que así puedan realizar diversos delitos informáticos.

- **Tercero:** al hablar del verbo rector, estamos haciendo referencia a la acción que debe cometer el ciberdelincuente para que este configure el delito en especifico que desarrolla cada artículo, por lo que, de acuerdo a lo desarrollado en la tabla 3 se pudo evidenciar que ningún verbo rector se repite en los artículos que desarrolla la Ley N.º 30096, pues cada uno muestra conductas independientes que permiten identificar al sujeto activo en un solo tipo penal para su adecuada sanción aplicable.
- **Cuarto:** en cuanto a las modalidades, estas describen las particularidades en las que se desarrollaran las conductas de los ciberdelincuentes para que se pueda consumar el delito en específico, pues se va refiriendo a las características y medios utilizados que debe aplicar el ciberdelincuente para la obtención de la información reservada, para posteriormente cometer el delito, dejando ver también que cada artículo cumple con modalidades distintas para cada tipo penal descrito.
- **Quinto:** finalmente, al hablar del bien jurídico protegido en la Ley de Delitos Informáticos, se pudo evidenciar que el bien jurídico más afectado en esta ley es la Integridad Informática, la misma que hace referencia a la información privada que se registra en una base de datos de la red, la cual es el punto más buscado por los ciberdelincuentes para la comisión de distintos ilícitos penales de esta ley, por otro lado, el patrimonio y la fe pública, son otros bienes jurídicos que se ven

afectados al momento de la comisión de estos delitos, pues la mayoría de veces que el ciberdelincuente obtiene la información personal de su victima con el fin principal de obtener un beneficio económico posterior, sin tener en cuenta la afectación a la fe pública que este puede generar en sus víctimas.

Es por esta razón que, al haber identificado correctamente todos los elementos del tipo penal, puedo concordar en parte con lo planteado por Hidalgo y Solano (2021), pues si bien es cierto, el phishing afecta la confidencialidad de la información sensible de sus víctimas para después perjudicarlas económicamente, por lo que, se debe tener en cuenta que, de acuerdo a los resultados obtenidos en el Objetivo 1, el *phishing* actúa como una conducta pluriofensiva, lo que nos permite evidenciar que esta figura también afecta a más de un bien jurídico protegido, lo que demuestra la necesidad de que este tipo de conducta sea tipificada como parte de las agravantes que contiene la Ley N.º 30096, además, de acuerdo con la interpretación presentada por los autores que analizaron la Ley N.º 30096 – Ley de delitos informáticos, pues consideramos también que el *phishing* es una modalidad consistente en la actualidad, y que al contar con todos los elementos más relevantes que componen a un tipo penal, le permite ser sancionada penalmente.

4.1.2. Objetivo 2: para hablar del segundo objetivo, es importante tener en cuenta los resultados obtenidos en la Tabla 5, esto debido a que su contenido tenia como fin principal el demostrar la existencia de nuevas modalidades informáticas delictivas

que se vienen desarrollando a lo largo del tiempo, para luego poder definirlas y demostrar así la necesidad e importancia de regularlas y así evitar su impunidad legislativa.

- Por otro lado, las definiciones obtenidas en la Tabla 6, nos permitieron identificar a varias modalidades que se consideran como subtipos del *phishing* para su adecuada identificación, dejando ver así que el *phishing* es modalidad delictiva más reconocida a nivel mundial, por el uso y accesibilidad que tienen los delincuentes para poder engañar a sus víctimas, obteniendo la información necesaria para luego cometer otros delitos con lo obtenido, asimismo, se tiene en cuenta que de acuerdo a las otras definiciones de estas nuevas modalidades, se pudo identificar que en su gran mayoría se dan a través de las redes sociales como lo son: Facebook, Instagram y Twitter, y en los medios de mensajería instantánea que son, Gmail, Outlook, Hotmail y los Mensajes de texto, mediante los cuales los ciberdelincuentes usan estas plataformas virtuales para hacer llegar mensajes didácticos a los usuarios de internet de forma aleatoria, y así poder llamar la atención de sus víctimas, con mensajes que contienen información convincente mediante un URL malicioso al cual los usuarios pueden acceder y los hacen caer en error para que de forma voluntaria estos brinden la información necesaria para que los ciberdelincuentes puedan cometer otros delitos que se encuentran integrantes en la misma ley.
- Por esta razón, concuerdo totalmente con lo planteado por Ventura (2020), quien indica que las modalidades del *phishing, smishing y*

vishing, al no encontrarse reguladas en nuestra legislación, presentan muchos problemas a pesar de demostrar que son las formas más comunes de defraudación que se usan para engañar a los usuarios en internet; además, para Solano e Hidalgo (2021), de acuerdo a su resultado 4, la conducta del *phishing* es compleja, y el problema es que los tipos penales vigentes no abordan de manera específica el *phishing*, sino que solo pretenden subsumirlo dentro de otras conductas que no las tipifican adecuadamente y no dan solución a la complejidad de los delitos informáticos; finalmente, para Sosa (2022), en una de sus conclusiones considera que el delito de *phishing*, cumple con las características necesarias de un comportamiento que busca aprovecharse del uso indebido de tecnologías de la información y de la comunicación, para obtener el acceso ilícito a datos informáticos privador y posteriormente usarlos en perjuicio de los sujetos pasivos del delito.

- Es decir, después de la interpretación presentada por los autores mencionados anteriormente, el *phishing* cuenta con todos los aspectos necesarios para poder configurarlo como una agravante de esta ley, ya que se puede evidenciar que esta modalidad se puede integrar directamente con los delitos de fraude informático y suplantación de identidad, los cuales muestran la necesidad de esta modalidad para que estos delitos se puedan llevar a cabo.
- Finalmente, teniendo en cuenta las cifras del Ministerio Público, durante el periodo 2013 – 2020, se recibieron un total de 23,657

denuncias por delitos informáticos, siendo un 58% (12608) de denuncias archivadas y un 41% (8842) de denuncias en proceso de investigación, dejando ver que muchos de los casos de delitos informáticos no llegan a la imputación de la pena, pues existen algunas deficiencias en el proceso de la investigación, las cuales generan que nuestro actual sistema de justicia sea inapropiado para el procesamiento de estos delitos.

4.1.3. Objetivo 3: respecto al tercer objetivo específico, es importante tener en cuenta los resultados obtenidos en la Figura 5 y Figura 6, en las cuales se tiene la definición exacta de las agravantes y los tipos de agravantes que se desarrollan en la Ley N.º 30096 – Ley de delitos informáticos, los mismos que dejan ver que la determinación de la pena, no solamente hace referencia a la división tradicional de atenuantes y agravantes, sino que también se deben considerar los tipos que cada una desarrolla de acuerdo a lo estipulado en el Código Penal, por lo que, en este caso se desarrollaron los tipos de agravantes existentes, identificándolas como agravantes genéricas, específicas y cualificadas.

- De acuerdo a la información obtenida en la Figura 5, se tiene que el primer tipo de agravantes, son aquellas que no están destinadas para un solo tipo penal en específico, sino que su actuación puede ser aplicada a todos los delitos existentes, haciendo así que al momento de su determinación de la pena se ubique en una pena concreta de acuerdo a los tercios establecidos por el Código Penal; en el segundo tipo de agravantes, las especificas solo se regulan en la parte especial, por lo que se estas se desarrollan en un párrafo adicional y dentro de

determinados delitos, por lo que, en este caso la pena concreta solo se basa en cuanto a lo estipulado por el legislador en el artículo en específico; finalmente, como tercer tipo de agravante se tienen a las cualificadas, las que su eficacia incide solamente en la estructura de la pena conminada, lo que significa que sus efectos pueden alterar o modificar los límites máximos o mínimos previstos en cada delito, creando así un nuevo marco penal conminada.

- En conclusión, después del análisis realizado al tipo de agravantes que se desarrolla en la dogmática penal y en la identificación de las agravantes que desarrolla a Ley N.º 30096, se puede confirmar que las agravantes presentes en la normativa antes mencionada son las agravantes específicas, todo esto ya que desarrollan distintos tipos de circunstancias que van a implicar el aumento de la peligrosidad de acuerdo a la conducta cometida, por lo que, solo implican especificación de conductas adicionales que agravan las penas de los ciberdelitos.

4.1.4. Objetivo general: después del análisis realizado en cada uno de los objetivos específicos, para poder confirmar el problema de investigación presentado, y de coincidir en su gran mayoría con el análisis realizado por los autores antes mencionados, es importante desarrollar adecuadamente la hipótesis planteada, teniendo en cuenta que es necesario especificar los dos fundamentos jurídicos necesarios para poder llevar acabo la incorporación del *phishing* como agravante en el artículo 11° de la Ley N.º 30096 – Ley de Delitos Informáticos, siendo los siguientes:

- **Primer fundamento**: la mayor gravedad del injusto penal que representa el p*hishing*, es por esto que, es importante conocer que al momento de individualizar cualquier pena que busca sancionar un delito que se desarrolla en una norma en específico, se debe analizar no solo las circunstancias en las que se llevó a cabo el hecho, sino también que se debe tener en cuenta la gravedad del injusto cometido, penal pues se sabe que la gravedad del hecho no es igual a la gravedad del injusto cometido, puesto que la primera se basa en las circunstancias que permiten que el hecho punible se materialice, lo que no hace referencia a la gravedad del delito, mientras que la segunda, es considerada por el legislador al momento de aplicar la pena abstracta correspondiente, sabiendo que esto hace referencia al máximo y mínimo de la pena que se aplica en cada delito, además, de que se deben tener en cuenta las consecuencias accesorias y los criterios que permiten al legislador razonar respecto al aumento o disminución de la pena.
- **Segundo fundamento:** se considera el incremento de la culpabilidad del autor al momento de utilizar el *phishing* como modalidad delictiva, lo cual hace referencia a que cuando se habla de culpabilidad se hace referencia al conocimiento que tiene el autor al momento de cometer un injusto penal, pues lo hace teniendo en cuenta que su conducta es típica y antijurídica, la misma que la realiza desde su capacidad de decidir y orientar su actuar de acuerdo a las limitaciones existentes en las normativas, por lo que, cuando un autor comete un delito integrante de la Ley de Delitos Informáticos hace uso del *phishing* como una

modalidad para lograr su cometido, se le considerará como una agravante para la comisión del delito principal, lo que hace que se incremente así su culpabilidad.

- En conclusión, se ha logrado demostrar los objetivos específicos, el objetivo general y también la hipótesis planteada la cual hace referencia a los dos fundamentos jurídicos del problema de investigación desarrollado.

4.2. Limitaciones

En la presente investigación se tuvo como limitantes las siguientes, primero que, la información recopilada se obtuvo a partir de los repositorios de universidades nacionales e internacionales, noticias nacionales e internacionales, páginas web y artículos de opinión, siendo importante resaltar que en el Perú, aún no se cuenta con la información necesaria para desarrollar adecuadamente algunas problemáticas respecto a los delitos informáticos, ya que la mayoría de la información obtenida son de medios internacionales, lo cual hace resaltar la carencia de material de investigación en nuestro país, reflejando así la falta de doctrina y jurisprudencia nacional para el desarrollo de temas de actualidad, lo cual limita el adecuado desarrollo de investigaciones actuales.

Segundo, que la investigación se realizó tomando en cuenta la Ley N.º 30096 – Ley de Delitos Informáticos y su modificatoria Ley N.º 30171 – Modificatoria de la Ley de Delitos Informáticos, el Convenio de Budapest, Observatorio Peruano de Cibercriminalidad, Reportes de la ciberseguridad propuesto por el Ministerio Público en su Informe 04, referente al periodo 2013 – 2020; no obstante, se debe mencionar que la carencia de información actual sobre delitos Informáticos hizo que exista una escasez de fuentes bibliográficas especializadas en el tema, por lo que para la construcción de los antecedentes,

justificación y marco teórico fue necesario recurrir a artículos, consultas en páginas web, revistas, noticias nacionales e internacionales y libros nacionales actualizados, para poder obtener material bibliográfico para la investigación.

4.3. Conclusiones

- **Primero:** La Ley N.º 30096 – Ley de Delitos Informáticos, posee diversos artículos que regulan diversas conductas delictivas cibernéticas que se dan en nuestro país, por lo que, el presente trabajo de investigación logró analizar a cada uno de estos artículos y consiguió identificar cuáles eran los bienes jurídicos afectados por este tipo de conductas, teniendo como base de análisis a los elementos del tipo penal, para así poder confirmar si la regulación vigente, cumple con la correcta tipificación legislativa para poder evitar la existencia de futuras confusiones interpretativas al momento de aplicar una sanción penal en este tipo de delitos informáticos.
- **Segundo:** En la actualidad, los delitos informáticos se han ido incrementando a nivel mundial, todo esto debido a la evolución que han ido sufriendo este tipo de conductas, lo que ha permitido que se creen nuevas modalidades delictivas, las cuales aún no han sido reguladas adecuadamente por los ordenamientos jurídicos de cada país, por lo que, se ha logrado identificar y definir a las modalidades informáticas que afectan frecuentemente a la Ley N.º 30096 – Ley De Delitos Informáticos en el Perú, para que así el sistema de administración de Justicia, que son el Ministerio Público, el Poder Judicial y la Policía

Nacional del Perú, mejoren las deficiencias legislativas que poseen y así puedan erradicar la carencia normativa existente en nuestro país.

- **Tercero:** De acuerdo a las agravantes desarrolladas en la presente investigación se tiene que el *phishing,* es una modalidad informática que cumple con todas las características de un comportamiento que se aprovecha del uso indebido de las tecnologías de la información y de la comunicación, para obtener el acceso ilícito a los datos informáticos privados de sus víctimas para generarles un perjuicio, permitiéndonos ver que este tipo de modalidad debería ser considerada como parte de las agravantes existentes en esta normativa, ya que al haber analizado la conducta delictiva que esta desarrolla, se puede presentar como una agravante especifica, la cual es necesaria su ejecución para la comisión de otros delitos previstos en la presente ley, además, de que su integración en este artículo, le permitiría al Perú posicionarse como el primer país en Latinoamérica que regula el *phishing* dentro de su ley de delitos informáticos.
- **Cuarto:** El *phishing,* al ser una modalidad delictiva actual que no se encuentra debidamente regulada y que se va incrementando a pasos agigantados a nivel mundial, es necesaria que cuente con una tipificación que se encuentre en un ordenamiento jurídico en específico, para así poder evitar su impunidad legislativa y aplicar la sanción correspondiente, teniendo en cuanta también, que el presente trabajo de investigación logró confirmar su hipótesis probando la necesidad regulatoria de esta modalidad dentro del artículo 11° de la Ley N.º

30096 – Ley de Delitos Informáticos, a partir de la cual se da la mayor gravedad del injusto penal y se incrementa la culpabilidad del autor, al momento en el que este utiliza el *phishing* como una modalidad de obtención de información personal de sus víctimas, para la comisión de otros delitos de la misma ley.

4.4. Recomendaciones

- Se recomienda la capacitación adecuada de los operadores de justicia, para que estos puedan identificar con exactitud la existencia del *phishing* en la comisión de los ciberdelitos, para que su tipificación sea aplicada adecuadamente y dicha modalidad ya se encuentre instalada dentro de la Ley N.º 30096.
- Se recomienda la integración de la conducta del *phishing*, en el artículo 11° de la Ley N.º 30096 – Ley de delitos informáticos, para que su sanción se aplique de acuerdo a ley, teniendo en cuenta que su integración busca determinar la mayor gravedad del injusto penal y verificar el incremento de la culpabilidad del autor mediante la utilización del *Phishing*, como modalidad delictiva para así obtener información personal de sus víctimas, para posteriormente utilizar dicha información y poder cometer futuros delitos informáticos.
- Finalmente, se propone la modificación de la Ley N.º 30171 – Ley Que Modifica Los Delitos Informáticos, proponiendo una adición legislativa a la norma antes mencionada en su artículo 11, siendo la propuesta legislativa la siguiente: "***5. El agente que envía o remite enlaces maliciosos a través de internet, de forma unitaria o masiva, para la***

obtención de información personal para la comisión de los delitos previstos en la presente ley".

REFERENCIAS

- Aranzamendi, L. (2013). *Instructivo teórico-práctico del diseño y redacción de la Tesis en Derecho*. Grijley.
- ANDALUCIACERT. (2017). *Informe de divulgación Phishing* (Informe). https://www.andaluciaesdigital.es/documents/410971/1437699/phising+2017/01950ce7-731f-48a6-821a-79388e571bff?version=1.0
- Andréu, J. (2018). *Las técnicas de Análisis de Contenido: Una revisión actualizada*. (Monografía). http://mastor.cl/blog/wpcontent/uploads/2018/02/Andreu.-analisis-de-contenido.-34-pags-pdf.pdf
- Belisario, A. (2014). *Análisis de Métodos de Ataques de Phishing*. [Trabajo final de posgrado, Universidad de Buenos Aires]. http://bibliotecadigital.econ.uba.ar/econ/collection/tpos/document/1502-0840_BelisarioMendezAN
- Carrasco, S (2005). Metodología de la investigación científica. San Marcos.
- Castillo, M. (2005). *Estudio Técnico de los delitos informáticos.* Futura.
- Chandarman, R. y Van Niekerk, B. (2017). *Students' cybersecurity awareness at a private tertiary educational institution. (Conciencia de los estudiantes sobre ciberseguridad en una institución educativa terciaria privada). African Journal of Information and Communication*. http://www.scielo.org.za/scielo.php?script=sci_arttext&pid=S20777213201700010007&lang=en
- Davara, M. (1995). *Análisis de la Ley de Fraude Informático.* Vega, J. (2010) *Los delitos informáticos en el Código Penal.* [Tesis de grado, Universidad Católica de Santa María]. . http://tesis.ucsm.edu.pe/repositorio/bitstream/handle/UCSM/6824/88.0774.MG.pdf?sequence=1&isAllowed=y
- Espinoza, V.R. (2022). *Delitos informáticos y nuevas modalidades delictivas.* (1.ª ed.). Instituto Pacífico.
- Ortega, D.P. y Fernández, C.A. (2009). *Metodología y técnicas de investigación: manual aplicado a las ciencias jurídicas y el derecho*. Universidad Privada Antenor Orrego.

- Fuentes, K. V. (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.* [Tesis de grado, Universidad Señor de Sipán]. https://repositorio.uss.edu.pe/handle/20.500.12802/8345
- Hernández, R., Fernández, C. y Baptista, M. (2016). *Metodología de la investigación*. (6ª. ed.). Mc GrawHill Education.
- González, J. A. (2013). *Delincuencia informática: daños informáticos del artículo 264 del Código Penal y propuesta de reforma*. [Tesis doctoral, Universidad Complutense de Madrid].https://eprints.ucm.es/id/eprint/23826/
- Gonzales Juárez, D. y Peña Enríquez, J. (2012). *Estudio del impacto de la ingeniería social – phishing* [Tesis de pregrado, Universidad Nacional Autónoma de México]. https://repositorio.unam.mx/contenidos/estudio-de-impacto-de-la-ingenieria-social-phishing3506472?c=BJbD08&d=false&q=*:*&i=3&v=1&t=search_0&as=0
- Herrera, E. (2016). *El Phishing como delito informático y su falta de tipificación en el Código Orgánico Integral Penal.* [Tesis de titulación, Universidad Central del Ecuador]. http://www.dspace.uce.edu.ec/handle/25000/8132.
- Hernández, R. M. (2014). *La investigación cualitativa a través de entrevistas: su análisis mediante la teoría fundamentada*. Cuestiones pedagógicas: Revista de ciencias de la educación, (23), 187-210. https://dialnet.unirioja.es/servlet/articulo?codigo=4909706
- Hidalgo, C y Solano, G. (2021). *El phishing como conducta delictiva no regulada en el ordenamiento jurídico peruano, propuesta de incorporación del artículo 7 – A en la Ley de Delitos Informáticos 30096.* [Tesis de titulación, Universidad Nacional del Santa]. https://repositorio.uns.edu.pe/handle/20.500.14278/3849
- Infante, B. (2019). *Análisis del delito de hurto de identidad virtual: frente a la seguridad de los sistemas informáticos.* [Tesis de Título, Universidad Nacional de Piura].*https://repositorio.unp.edu.pe/bitstream/handle/20.500.12676/2524/DECP-INF-GUE-2019.pdf?sequence=1&isAllowed=y*.
- Jiménez, J. (2017). *Manual de derecho penal informático.* (1ª. ed). Jurista Editores EIRL.

- Kaspersky Latam. (2018). *Panorama de amenazas. Phishing.* https://latam.kaspersky.com/about/press-releases/2018_panorama-deamenazas-phishing
- Leguizamón, M. S. M. (2015). *El Phishing.* [Trabajo final de grado, Universitat Jaume I.].https://repositori.uji.es/xmlui/handle/10234/127507
- Lerma, H. D. (2011). *Presentación de informes. El documento final de investigación*. (3ª. ed.). Ecoe Ediciones.
- Microsoft. (setiembre de 2020). *Microsoft Digital Defense Report.* https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWxPuf.
- Ministerio Público (2019). *Boletín Estadístico del Ministerio Público.* (Informe). https://agenciafiscal.pe/Storage/modsnw/pdf/12055-k1Nl6Ag7Le1Bg4B.pdf.
- Ministerio Público (2020). *Anuario estadístico del Ministerio Público.* (Informe). https://cdn.www.gob.pe/uploads/document/file/1895323/ANUARIO%202020%20FINAL%203.pdf.pdf.
- Ministerio Público. (2021). *Ciberdelincuencia en el Perú: pautas para una investigación fiscal especializada.* (Informe). *https://cdn.www.gob.pe/uploads/document/file/1669400/CIBERDELINCUENCIA%20EN%20EL%20PERU%CC%81%20-%20PAUTAS%20PARA%20SU%20INVESTIGACIO%CC%81N%20FISCAL%20ESPECIALIZADA%20-%2015%20FEBRERO%202021.pdf*.
- Monje, C. (2011). *Metodología de la Investigación Cuantitativa y Cualitativa: Guía Didáctica*. Universidad Surcolombiana.
- Ramos, C. (2007). *Cómo hacer una Tesis de Derecho y no envejecer en el intento*. (4ª. ed.). Gaceta Jurídica.
- Rojas, M. (2002). *Manual de investigación y redacción científica*. Book Xx press.
- Rojas, S. (2013). *Revealing non-alphabetical guises of spam-trigger vocables* [Reconocimiento de variantes enmascaradas de vocablos desencadenadores de correo indeseado]. DYNA, *3*(80), 50-51. http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S00127353201300060006&lang=en
- Rubio, M. (2009). *El sistema jurídico. Introducción al derecho.* (10ª. ed.). Fondo Editorial PUCP.

- Pardo, A. (2018). *Tratamiento jurídico penal de los delitos informáticos contra el patrimonio, Distrito Judicial de Lima, 2018.* [Tesis de posgrado]. Universidad César Vallejo. https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/20372/Pardo_VA.pdf?sequence=1&isAllowed=y
- Salvi Grilleti, N. C. (2019). *El Phishinh en la Argentina.* [Tesis de grado, Universidad Siglo 21].https://repositorio.uesiglo21.edu.ar/handle/ues21/16066
- Sain, G. (2015). Evolución Histórica de los Delitos Informáticos. *Revista Pensamiento Penal*, 2- 4. https://www.pensamientopenal.com.ar/doctrina/40877-evolucion-historica-delitos-informaticos
- Semprini, G. M. (Julio de 2018). *Entrevista de profundidad para la investigación.* Argentina.
- Tantaleán, R. (2015). El alcance de las investigaciones jurídicas. *Derecho y Cambio Social. (41), 1 – 22.* https://dialnet.unirioja.es/servlet/articulo?codigo=5456857
- Valle, J.C. (2013). *El delito informático de phishing.* [Tesis de pregrado, Universidad Regional Autónoma de Los Andes.]. https://dspace.uniandes.edu.ec/handle/123456789/2819
- Vega J. y Arévalo, M. (2022). *Ciberdelitos. Análisis en el sistema penal*. Editorial Iustitia.
- Urquiaga, M. (2018). *Guía de investigación científica 2018.* Universidad privada del Norte.
- Witker, J. (1995). *La investigación jurídica*. McGraw-Hill.

ANEXOS

ANEXO 01:

Propuesta de ley **"Año de la unidad, la paz y el desarrollo"**

Proyecto de Ley N.º _____

PROYECTO DE LEY QUE INCORPORA EL INCISO 5 EN EL ARTÍCULO 11° DE LA LEY DE DELITOS INFORMÁTICOS – LEY N° 30096, PARA IMPLEMENTAR EL DELITO DE PHISHING MEDIANTE SU DEFINICIÓN EN EL ARTÍCULO 11° COMO NUEVA AGRAVANTE DEL MISMO CUERPO NORMATIVO.

La bachiller de la Escuela Académica Profesional Derecho y Ciencias Políticas de la Universidad Privada del Norte – Sede Cajamarca, YOSSELYM MARILU BETSABETH RAVINES CARRERA, en ejercicio del derecho a la iniciativa legislativa prevista en el artículo 107° de la Constitución Política del Perú y concordante con los artículos 75 ° y 76 ° del Reglamento del Congreso de la República, propone el siguiente Proyecto de Ley:

I. EXPOSICIÓN DE MOTIVOS

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

En la actualidad, una de las modalidades delictivas más empleadas por los ciberdelincuentes es el phishing en sus diversas modalidades, razón por la cual ha ido generando un incremento evidente en cuanto a la comisión de esta conducta delictiva,

teniendo como principal evidencia la gran cantidad de denuncias que se registran en nuestro país ante los diferentes órganos de justicia, por este tipo de delitos.

Si bien es cierto la Ley N° 30096 – Ley de Delitos Informáticos, ya regula variedad de conductas delictivas con el fin de combatir la cibercriminalidad, se debe tener en cuenta que los mismos no son suficientes para actuar en cuanto al dinamismo que presentan estas nuevas conductas tecnológicas, las mismas que varían constantemente en cuanto a su aplicación por parte de los ciberdelincuentes, para que puedan llevar a cabo sus actos ilícitos, lo cual sigue permitiendo que exista impunidad en este tipo de conductas, pues al no encontrarse tipificada en un cuerpo normativo en específicos no pueden ser sancionadas como delitos, ya que en nuestro país el principio general del derecho penal, es el principio de legalidad, el mismo que impide que se pueda sancionar una conducta que no esté previamente regulada como delito.

Razón por la cual, la actuación de los operadores de justicia del derecho penal, se encuentran limitados al momento de enfrentar este tipo de casos, pues se vuelven más difíciles de subsumir en otros tipos penales existentes porque no coinciden con la figura regulada. Por tal motivo, es importante que se cree un tipo penal que defina al *phishing*, y este mismo englobe sus nuevas modalidades que viene desarrollando, pues se debe tener en cuenta que para que los ciberdelincuentes puedan cometer los delitos que son parte de la Ley N° 30096, es necesario que estos hagan uso del *phishing* para poder obtener la información de sus víctimas, por lo que, es necesaria su tipificación para que esta conducta pueda ser sancionada adecuadamente.

II. VIGENCIA DE LA NORMA

Respecto a la de vigencia de la norma propuesta, se tiene que esta no afectará la normatividad Constitucional; por el contrario, la Constitución Política del Perú, establece en su artículo 2° numeral 24 literal "d" que:

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

III. ANÁLISIS COSTO – BENEFICIO

Respecto al Costo, la presente iniciativa legislativa no genera ningún tipo de gasto adicional para el Estado peruano, pues se sigue el mismo procedimiento al momento de legislar: generando así solo copias y el pago a los legisladores y asesores del Congreso que legislan.

Respecto al Beneficio, esta propuesta es de suma importancia pues permitirá que los administradores de justicia del país puedan investigar y sancionar adecuadamente un hecho ilícito que está generando en la actualidad una grave pérdida patrimonial y personal, para aquellas personas que son víctimas del *phishing*, por consiguiente, este beneficio alcanzará también a la población en general, pues se podrá sancionar directamente a uno de los delitos más comunes que se está dando en la sociedad durante los últimos años.

Por lo que, esta propuesta legislativa brindará mayor seguridad a la población peruana frente al accionar de ciberdelincuentes que accedan a la información sensible de sus víctimas para posteriormente ser usada en perjuicio de las víctimas, teniendo en cuenta además que, de regularse este tipo penal en nuestro ordenamiento jurídico, seriamos el

primer país latinoamericano en regular la figura del *phishing* dentro de la Ley N° 30096 – Ley de Delitos Informáticos.

IV. FÓRMULA LEGAL

LA PRESIDENTA DE LA REPÚBLICA

POR CUANTO:

EL CONGRESO DE LA REPÚBLICA;

Ha dado la Ley siguiente:

LEY QUE INCORPORA EL INCISO 5 EN EL ARTÍCULO 11° DE LA LEY DE DELITOS INFORMÁTICOS – LEY N° 30096:

Artículo 1°. - Incorpórese el inciso 5 en el artículo 11°: Agravantes, en el Capítulo VII – Disposiciones Comunes, de la Ley de Delitos Informáticos, Ley N° 30096.

Artículo 11°. – Agravantes

“El juez aumenta la pena privativa de libertad hasta en un tercio por encima del máximo legal fijado para cualquiera de los delitos previstos en la presente Ley cuando:

1. El agente comete el delito en calidad de integrante de una organización criminal.
2. El agente comete el delito mediante el abuso de una posición especial de acceso a la data o información reservada o al conocimiento de esta información en razón del ejercicio de un cargo o función.
3. El agente comete el delito con el fin de obtener un beneficio económico, salvo en los delitos que prevén dicha circunstancia.

4. El delito compromete fines asistenciales, la defensa, la seguridad y la soberanía nacionales.
5. "***El agente que envía o remite enlaces maliciosos a través de internet, de forma unitaria o masiva, para la obtención de información personal para la comisión de los delitos previstos en la presente ley".***

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

Comuníquese a la señora Presidenta de la República para su promulgación.

En Lima, a los tres días del mes de abril de dos mil veintitrés.

JOSÉ DANIEL WILLIAMS ZAPATA

Presidente del Congreso de la República

MARTHA LUPE MOYANO DELGADO

Primera Vicepresidenta del Congreso de la República

A LA SEÑORA PRESIDENTA DE LA REPÚBLICA, POR TANTO:

Mando se publique y cumpla.

Dado en la Casa de Gobierno, en Lima, a los ocho días del mes de febrero del año dos mil veintitrés.

DINA ERCILIA BOLUARTE ZEGARRA

Presidenta de la República

LUIS ALBERTO OTÁROLA PEÑARANDA

Presidente del Consejo de Ministros.

ANEXO 02**:**

Matriz de consistencia

POBLEMA	OBJETIVOS	HIPÓTESIS	CATEGORIAS JURIDICAS	METODOLOGÍA
¿Cuáles son los fundamentos jurídicos para incorporar el *Phishing* como agravante en el artículo 11° de la Ley N.º 30096 – Ley de Delitos Informáticos en el Perú?	**General:** - Determinar los fundamentos jurídicos para la Incorporación del *Phishing* como agravante en el artículo 11° de la Ley N.º 30096 – Ley de Delitos Informáticos en el Perú. **Específicos:** - Identificar y analizar los bienes jurídicos afectados en la Ley N.º 30096 – Ley de Delitos Informáticos en el Perú. - Identificar y analizar las modalidades	Los fundamentos jurídicos para incorporar el *Phishing* como una de las agravantes en el artículo 11° de la Ley N.º 30096 – Ley de Delitos Informáticos son: - La mayor gravedad del injusto penal que representa el *Phishing*. - El incremento de la culpabilidad del autor con la utilización del *Phishing*.	- El *Phishing*. - Artículo 11° de la Ley 30096 – Ley de Delitos Informáticos.	**Tipo:** - Básica - Descriptiva **Diseño:** - No experimental **Enfoque:** - Cualitativo **Alcance:** - Correlacional **Población:** - Principales normas nacionales en materia penal. **Muestra:** - Ley N.º 30096 – Ley de Delitos Informáticos **Técnica:** - Análisis de contenido

	informáticas más frecuentes en la Ley N.º 30096 – Ley de Delitos Informáticos en el Perú. - Identificar las agravantes reguladas en la Ley N.º 30096 – Ley de Delitos Informáticos, en base a las agravantes desarrolladas en la dogmática penal peruana.			**Instrumento:** - Fichaje **Métodos científicos:** - Inductivo - Comparativo **Métodos jurídicos:** - Histórico - Hermenéutico - Dogmático