UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO
FACULTAD DE DERECHO Y CIENCIA POLÍTICA
ESCUELA PROFESIONAL DE DERECHO

TESIS:

La tipificación del phishing, smishing y vishing como defraudación en base a la concepción del bien jurídica seguridad informática.

Autor:

Bach. LARIOS RODRIGUEZ LUIS ANGEL

Asesora:

Mag. COLINA MORENO MARY ISABEL.

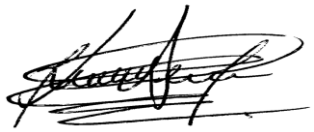
PARA OPTAR EL TÍTULO PROFESIONAL DE ABOGADO

Fecha de sustentación:

31 DE MAYO DEL 2024

LAMBAYEQUE

Tesis denominada "La tipificación del phishing, smishing y vishing como defraudación en base a la concepción del bien jurídico seguridad informática" **presentada para optar el TITULO PROFESIONAL DE ABOGADO, por:**



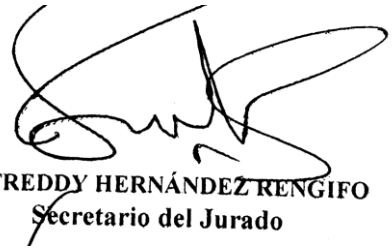
……

Bach. Larios Rodríguez Luis Ángel
Autor

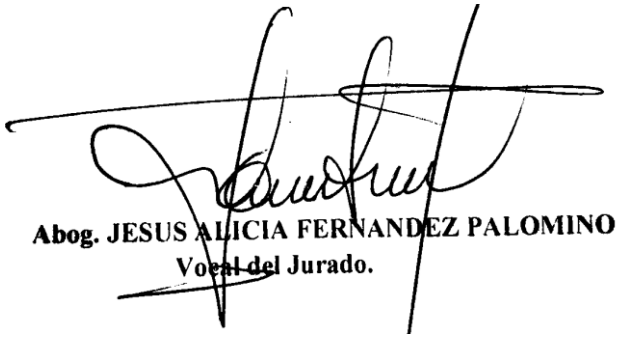
Mag. MARY ISABEL COLINA MORENO
Asesor

APROBADO POR:

Mag. CARLOS MANUEL MARTINEZ OBLITAS
Presidente del Jurado



Dr. FREDDY HERNÁNDEZ RENGIFO
Secretario del Jurado



Abog. JESUS ALICIA FERNANDEZ PALOMINO
Vocal del Jurado.

Dedicatoria

Quiero dedicar este trabajo de tesis a mi padre Miguel y mi madre Marleny, por su paciencia, sus consejos y su gran apoyo incondicional, porque todo lo que hoy soy es gracias a ellos.

Agradecimiento

A mis padres y familiares por apoyarnos e incentivarnos a estudiar una carrera profesional con mucho esfuerzo y sobre todo los valores inculcados cada día.

UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO
FACULTAD DE DERECHO Y CIENCIA POLITICA
UNIDAD DE INVESTIGACION

ACTA DE SUSTENTACIÓN
A C T A DE SUSTENTACIÓN PRESENCIAL N° 41-2024-UI-FDCP

Sustentación para optar el Título de ABOGADO de: **Luis Angel Larios Rodriguez.**
Siendo las 18:00 p.m. del día viernes 31 de mayo del 2024 se reunieron en la Sala de simulación de audiencias 1 de la Universidad Nacional "Pedro Ruiz Gallo", los miembros del jurado evaluador de la tesis titulada: " ***LA TIPIFICACIÓN DEL PHISHING, SMISHING Y VISHING COMO DEFRAUDACIÓN EN BASE A LA CONCEPCIÓN DEL BIEN JURÍDICO SEGURIDAD INFORMÁTICA"***, designados por Resolución N° 256-2022-FDCP-VIRTUALde fecha 7 de septiembre de 2022, con la finalidad Evaluar y Calificar la sustentación de la tesis antes mencionada, por parte de los Señores Catedráticos:

PRESIDENTE : **Mag. CARLOS MANUEL MARTINEZ OBLITAS.**
SECRETARIO : **Dr. FREDDY HERNÁNDEZ RENGIFO.**
VOCAL : **Abog. JESUS ALICIA FERNANDEZ PALOMINO**

La tesis fue asesorada por Mag. MARY ISABEL COLINA MORENO, nombrada por Resolución N°256-2022-FDCP-VIRTUAL de fecha 7 de septiembre de 2022.
El acto de sustentación fue autorizado por Resolución N° 295 -2024-FDCP-VIRTUAL de fecha 22 de mayo del 2024.
La tesis fue presentada y sustentada por el bachiller **Luis Angel Larios Rodriguez** y tuvo una duración de 30 minutos. Después de la sustentación y absueltas las preguntas y observaciones de los miembros del jurado; se procedió a la calificación respectiva, obteniendo el siguiente resultado: APROBADO **con la nota de** 17 (DIECISIETE) **en la escala vigesimal,** mención **de** BUENO .
Por lo que queda APTO para obtener el Título Profesional de **ABOGADO**, de acuerdo con la Ley Universitaria 30220 y la normatividad vigente de la Facultad de Derecho y Ciencia Política, y la Universidad Nacional Pedro Ruiz Gallo.
Siendo las 19:12 p.m., del mismo día, se da por concluido el acto académico tomando la juramentación respectiva y suscribiendo el Acta los miembros del jurado.

LambayequeLambayeque, viernes 31 de mayo del 2024

Mag. CARLOS MANUEL MARTINEZ OBLITAS
Presidente del Jurado

Dr. FREDDY HERNÁNDEZ RENGIFO
Secretario del Jurado

Abog. JESUS ALICIA FERNANDEZ PALOMINO
Vocal del Jurado.

CONSTANCIA DE APROBACIÓN DE ORIGINALIDAD DE TESIS

*Yo, **Mg. MARY ISABEL COLINA MORENO,** Asesora del tesista**: LUIS ANGEL LARIOS RODRIGUEZ**, luego de la revisión exhaustiva de su Tesis titulada* **"LA TIPIFICACIÓN DEL PHISHING, SMISHING Y VISHING COMO DEFRAUDACIÓN EN BASE A LA CONCEPCIÓN DEL BIEN JURÍDICO SEGURIDAD INFORMÁTICA",** *constado que la misma tiene un índice de similitud de **13 %** verificable en el reporte de similitud del programa Turnitin.*

La suscrita analizó dicho reporte y concluyó que cada una de las coincidencias detectadas no constituyen plagio. A mi leal saber y entender, la tesis cumple con todas las normas para el uso de citas y referencias establecidas por la Universidad Nacional Pedro Ruiz Gallo.

Lambayeque, 22 DE MARZO del 2024.

Mg. MARY ISABEL COLINA MORENO
D.N.I 40997649
ASESORA

Bach. Larios Rodríguez Luis Ángel
Autor

La tipificación del phishing, smishing y vishing como defraudación en base a la concepción del bien jurídico seguridad informática

INFORME DE ORIGINALIDAD

13%	13%	2%	3%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	hdl.handle.net Fuente de Internet	5%
2	repositorio.unprg.edu.pe Fuente de Internet	3%
3	repositorio.unfv.edu.pe Fuente de Internet	1%
4	www.peruweek.pe Fuente de Internet	1%
5	docplayer.es Fuente de Internet	1%
6	repositorio.upn.edu.pe Fuente de Internet	1%
7	repositorio.ucv.edu.pe Fuente de Internet	<1%
8	repositorio.unprg.edu.pe:8080 Fuente de Internet	<1%

Mg. MARY ISABEL COLINA MORENO
D.N.I 40997649
ASESORA

Recibo digital

Este recibo confirma quesu trabajo ha sido recibido por Turnitin. A continuación podrá ver la información del recibo con respecto a su entrega.

La primera página de tus entregas se muestra abajo.

Autor de la entrega:	Luis Ángel Larios Rodríguez
Título del ejercicio:	Quick Submit
Título de la entrega:	La tipificación del phishing, smishing y vishing como defrau...
Nombre del archivo:	TESIS_LARIOS_RODRIGUEZ_LUIS_ANGEL.docx
Tamaño del archivo:	2.13M
Total páginas:	80
Total de palabras:	15,491
Total de caracteres:	83,900
Fecha de entrega:	20-mar.-2024 12:22p. m. (UTC-0500)
Identificador de la entre...	2325936967

UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO

FACULTAD DE DERECHO Y CIENCIA POLÍTICA

ESCUELA PROFESIONAL DE DERECHO

Tesis

La tipificación del phishing, smishing y vishing como defraudación en base a la concepción del bien jurídico seguridad informática

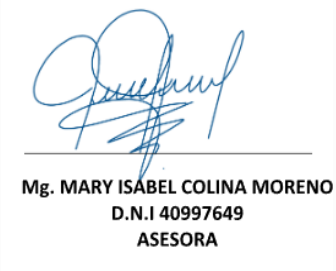
Autor:

Bach. Larios Rodríguez Luis Ángel

Asesor:

Presentado para optar el título profesional de Abogado

Lambayeque, 2024



Mg. MARY ISABEL COLINA MORENO
D.N.I 40997649
ASESORA

Índice general

Índice de tablas

Resumen

Esta tesis se ha enfocado en la tarea proyectada a determinar si resulta adecuada la tipificación del phishing, smishing y vishing como modalidad de defraudación, esta observación ha tenido como finalidad principal verificar la viabilidad jurídica vinculada con la necesidad social para que en base a ello como incorporación se pueda garantizar el bien jurídico seguridad informática. Para el análisis de tales condiciones se ha tenido que recurrir a la evaluación de la propia norma con el fin de entender su sentido, para ello se ha involucrado el método de observación de la realidad jurídica y los métodos de interpretación jurídica tanto exegético así como el sistemático.

El resultado de esta observación es lo que permite señalar como necesaria la incorporación de la acción delictiva de phishing, smishing y vishing como tipos penales que permitan el reconocimiento de estas acciones como delictivas y que pueda establecerse una sanción adecuada para ellos. Esta postura se centra en la base de la seguridad jurídica que debe amparar a todas las interacciones que se producen en la sociedad y que en los tiempos actuales se esta concentrando en el medio de la informática puesto que se ha creado el ciberespacio que de acuerdo a la dirección que esta tomando y la intensidad de su crecimiento podría establecerse como un medio de interacción generalizado.

Palabras clave: Tipificación, Phishing, Smishing, Vishing, Defraudación, Seguridad informática

Abstract

This thesis has focused on the projected task of determining whether the classification of phishing, smishing and vishing as a form of fraud is appropriate. The main purpose of this observation has been to verify the legal viability linked to social need so that, based on it, as incorporation, the legal good of computer security can be guaranteed. For the analysis of such conditions, it has been necessary to resort to the evaluation of the norm itself in order to understand its meaning; for this, the method of observation of legal reality and the methods of legal interpretation, both exegetical as well as the systematic.

The result of this observation is what allows us to point out as necessary the incorporation of the criminal action of phishing, smishing and vishing as criminal types that allow the recognition of these actions as criminal and that an appropriate sanction can be established for them. This position focuses on the basis of legal security that must protect all interactions that occur in society and that in current times is concentrating on the medium of information technology since cyberspace has been created that, according to The direction it is taking and the intensity of its growth could be established as a generalized means of interaction.

Keywords: Typing, Phishing, Smishing, Vishing, Fraud, Computer Security

Introducción

El título de: “La tipificación del phishing, smishing y vishing como defraudación en base a la concepción del bien jurídico seguridad informática” surge en razón de la experiencia del investigador respecto al contacto directo con la tarea del titular de la acción penal respecto a la identificación del tipo delictivo para ser aplicado sobre este tipo de actos desarrollados en el espacio cibernético o informático. Ello ha impulsado a la evaluación de las posibilidades jurídicas que en base a la protección del bien jurídico antes indicado, pudiera generarse la incorporación de esta acción delictiva en las tipologías penales peruanas.

Es necesario indicar que existen pautas de conocimiento previo que han sido revisados con el fin de tener un panorama más claro respecto a la realización de este trabajo como es el caso de que la influencia de la globalización es lo que conduce a la necesidad de hacer uso del medio informático para el ejercicio de actividades transaccionales, vista desde le óptica de lo práctico y operativo resulta muy útil el ciberespacio para lograr efectividad en este tipo de actos. Sobre esta condición especial es lo que se presenta como necesidad de la intervención del Estado para ocuparse de las garantías que deban ser respetadas en esta interacción, que de hecho resulta ser su obligación institucional.

Actualmente existe mayor incidencia en la actividad personal, laboral y social relacionada con las redes sociales como un servicio digital, lo cual adopta una condición imprescindible para el desarrollo de los trabajos y el movimiento financiero incluso, lo cual se traduce en un tema de inseguridad dado que más de la

mitad de empresas que brindan su servicio a través de estos medios informático se preocupan de manera incompleta dado que no se cuenta con herramientas de control ante la posible acción fraudulenta de los que se dedican a la defraudación bajo las modalidades de del phishing, smishing y vishing

Es necesario por ello fortalecer las garantías sociales frente al riesgo que supone la actividad económica que puede ser ejecutada mediante el uso de medios informáticos. Ello se evidencia en función de la presencia de casos en los que este tipo de movimientos se plantean como el medio perfecto para ejecutar defraudaciones por personas inescrupulosas, poniendo en riesgo la seguridad ciudadana a este nivel, lo cual debe ser atendido por el Estado mediante el derecho con tal de lograr un alcance de control y protección adecuados.

Por tal razón se debe impulsar el conocimiento orientado a que finalmente se sugiera al Legislativo en tanto poder del Estado encargado de la creación de leyes, deberá analizar con cuidado este tipo de actos que configuran defraudación en el sistema informático, vale decir aquello que se ha calificado como phishing, smishing y vishing. Tal identificación debería propiciar la creación de reglas específicas en el ámbito penal referido a las defraudaciones con la intención de generar un espacio proteccionista respecto del bien jurídica seguridad informática; dicha acción estatal obedecerá a una política pública de lucha contra el crimen orientada a este ámbito virtual que cada día es más usado por la sociedad.

Desde luego este análisis requiere de una ruta, por lo mismo que se planteó dicha secuencia en el contenido del Primer Capítulo de la tesis el mismo que señala los aspectos metodológicos que se han seguido partiendo por el planteamiento del problema para seguir luego por la formulación de la interrogante que cuestiona el tema y lo hace de la siguiente manera: ¿Qué tan adecuada resulta la tipificación del phishing, smishing y vishing como modalidad de defraudación para garantizar el bien jurídico de seguridad informática?

Bajo la misma percepción de las variables que incorpora tal cuestionamiento que funge de formulación del problema se han creado las metas que siguieron la investigación, así en el campo general que dice: determinar si resulta adecuada la tipificación del phishing, smishing y vishing como modalidad de defraudación para garantizar el bien jurídico denominado seguridad informática. Del mismo modo de manera específica se ha señalado como metas: Interpretar la posibilidad de incorporar la tipificación del phishing, smishing y vishing en base a la teoría de las necesidades; desarrollar las justificaciones jurídicas para comprender el bien jurídico de seguridad informática como objeto de protección en el ámbito penal, analizar el nivel de afectación que produce la incidencia del phishing, smishing y vishing como defraudación sobre la seguridad informática.

Se aprecia luego en la construcción del Capítulo Segundo de la investigación que se ha creado un marco teórico relacionado con la descripción de las acciones conceptualizadas como phishing, smishing y vishing para vincular la posibilidad de tipificarlas en base a al teoría de las necesidades, lo cual significa que la observación

de la realidad permitirá establecer si finalmente se puede considerar como una necesidad social a la incorporación de estas conductas como mecanismos de sanción que promueva el Estado peruano.

También es posible observar en el Tercer Capitulo de esta construcción académica el desarrollo de la teoría relacionada con el bien jurídico conocido como seguridad informática, lo cual ha servido de base para el reconocimiento de su protección en el campo de la normativa punitiva. Esto quiere decir que tanto se ha contemplado la posibilidad de satisfacer una necesidad social relacionada tanto con la seguridad ciudadana así como con la seguridad jurídica que debe ostentar el medio en que se desarrolla la interacción cibernética.

Capítulo I

Los aspectos metodológicos de la investigación

1.1. El planteamiento del problema

La realidad actual que se encuentra influenciada y determinada por las condiciones que establece la globalización que obliga a los seres humanos a la utilización de los medios informáticos, conlleva al reconocimiento de ciertas necesidades de protección que emanan de la cantidad de casos en los que se advierte la intervención del fraude informático, específicamente bajo las modalidades de del phishing, smishing y vishing. Por ello resulta importante tener en cuenta el nivel de acción de parte del Estado para lograr la prevención de este tipo de acciones ilícitas, así se reconocerá la necesidad de incorporar este tipo de modalidades de defraudación para garantizar el nivel de seguridad jurídica que se entiende debe presentarse en las transacciones que se realizan de manera virtual como modalidad de defraudación para garantizar el bien jurídico de seguridad informática.

Para el caso peruano se han visto reportados una cantidad superior a los " (…) 433 millones de este tipo de ataques en la red virtual, El 60% de las empresas peruanas muestra preocupación por no tener suficiente capacidad para enfrentar estos ataques". (Revista Economía, 2022); esta situación deja en claro que esta época en la existe mayor incidencia en la actividad personal, laboral y social relacionada con las redes sociales como un servicio digital, lo cual adopta una condición imprescindible para el desarrollo de los trabajos y el movimiento financiero incluso.

Es precisamente este tipo de circunstancia la que permite establecer un vínculo entre la necesidad de control que se supone debe manejar el Estado para consolidar un elemento de protección, y las condiciones en las que se desarrolla la normativa penal, puesto que se precisa de ciertos factores que funden la creación de tipos penales, sobre todo en el aspecto de la configuración específica del bien jurídico que se ha de proteger.

Es importante considerar como circunstancia que muestra una realidad de necesidad social el hecho de que sobre todo en el periodo de la pandemia se ha mostrado a nivel internacional sobre todo en América Latina, que "(…) el 49% de las empresas peruanas encuestadas percibió un incremento en los ataques cibernéticos a raíz de la pandemia, y el 21% considera que la ingeniería social (phishing) es el ciberataque que más se ha incrementado, mientras que el 20% considera que ha sido el malware".

Ha de señalarse que en la actualidad existe una regulación especial mediante la Ley 30096 que se ocupa de los delitos informáticos, en la cual se puede establecer una similitud con la característica de acción delictiva del Pishing, respecto a lo señalado en el artículo octavo puesto que se vincula con la condición de delitos patrimoniales, los delitos del fraude cometido por medios informáticos, así como el tenor de la acción delictiva en contra de la fe pública. Esta indicación es con la finalidad de promover el análisis normativo a fin de establecer si en función a dicha estructura resultaría satisfactorio el control o si existe realmente la necesidad de crear nuevos tipos delictivos.

Tal propuesta de análisis se proyecta a la revisión de las posibilidades jurídicas enfocadas al reconocimiento de este tipo de acciones ilícitas desde la perspectiva de los delitos de tipo abstracto para considerarlos como tipo base para alcanzar el nivel de prevención y en tanto se pueda reconocer el nivel del resultado ya en esta otra modalidad alcanzar la posibilidad de generar una agravante que eleve la sanción penal.

1.2. La formulación del problema

¿Qué tan adecuada resulta la tipificación del phishing, smishing y vishing como modalidad de defraudación para garantizar el bien jurídico de seguridad informática?

1.3. La justificación de la investigación

Para el desarrollo de este trabajo académico se ha verificado de manera previa una justificación basada en la necesidad de garantías sociales frente al riesgo que supone la actividad económica que puede ser ejecutada mediante el uso de medios informáticos. Ello se evidencia en función de la presencia de casos en los que este tipo de movimientos se plantean como el medio perfecto para ejecutar defraudaciones por personas inescrupulosas, poniendo en riesgo la seguridad ciudadana a este nivel, lo cual debe ser atendido por el Estado mediante el derecho con tal de lograr un alcance de control y protección adecuados.

En dicho afán es que se puede ubicar una justificación de tipo legislativa, ello implica que el Legislativo en tanto poder del Estado encargado de la creación de leyes, deberá analizar con cuidado este tipo de actos que configuran defraudación en el sistema informático, vale decir aquello que se ha calificado como phishing, smishing y vishing. Tal identificación debería propiciar la creación de reglas específicas en el ámbito penal referido a las defraudaciones con la intención de generar un espacio proteccionista respecto del bien jurídica seguridad informática; dicha acción estatal obedecerá a una política pública de lucha contra el crimen orientada a este ámbito virtual que cada día es más usado por la sociedad.

1.4.La importancia de la investigación

La proyección de este tema que en tanto necesidad de protección sugiere la creación de tipos penales específicos destinados al control de la actividad informática que abre la puerta a la defraudación señalada bajo la modalidad de phishing, smishing y vishing; encuentra su punto de importancia en tanto se espera ampliar la protección que ejerce el Estado mediante el control punitivo que se aplica con el Derecho Penal.

Es en virtud de tal creación que se puede reconocer la existencia de beneficiarios tanto a nivel general que viene a ser la sociedad, en tanto que la creación de los tipos penales específicos arriba indicado, permitirá proteger los intereses comunes relacionados con la seguridad informática. También se puede considerar como beneficiarios directos a cada uno de los sujetos que desarrolla

actividades informáticas, en tanto que el riesgo de defraudación será controlado penalmente.

1.5.Los objetivos de la investigación

1.5.1. El objetivo general

- Determinar si resulta adecuada la tipificación del phishing, smishing y vishing como modalidad de defraudación para garantizar el bien jurídico seguridad informática.

1.5.2. Los objetivos específicos

- Interpretar la posibilidad de incorporar la tipificación del phishing, smishing y vishing en base a la teoría de las necesidades.
- Desarrollar las justificaciones jurídicas para comprender el bien jurídico de seguridad informática como objeto de protección en el ámbito penal
- Analizar el nivel de afectación que produce la incidencia del phishing, smishing y vishing como defraudación sobre la seguridad informática.

1.6. La hipótesis de la investigación

Resulta adecuada y necesaria la tipificación del phishing, smishing y vishing como modalidad de defraudación con el fin de garantizar el bien jurídico de seguridad informática en beneficio de los intereses sociales.

1.7.Las variables de la investigación

1.7.1. Sobre la variable independiente

Tipificación del phishing, smishing y vishing.

1.7.2. Sobre la variable dependiente

El bien jurídico de seguridad informática

1.8.Los métodos aplicados en la investigación

Con la finalidad de establecer un criterio de observación del problema de manera correcta, se han planteado los métodos de investigación que en el campo de la interpretación de las reglas jurídicas se puede concebir como herramientas de utilidad para seguir la ruta de inferencias que jurídicamente justifiquen la propuesta.

1.8.1. El método exegético jurídico:

Este método de interpretación jurídica se inspira en la percepción literal de las leyes con el fin de establecer su criterio normativo y reconocer el verdadero sentido que de su construcción s deriva. Tal cual según esta interpretación, se deben tomar las pautas de aplicación objetiva de la regla, lo cual se verifica como un elemento esencial a tener en consideración para la construcción de la propuesta normativa, que se entiende debe ser sometida a la verificación de los factores que justifican la necesidad de crear tipos penales en base a los bienes jurídicos.

1.8.2. El método sistemático jurídico

Se consolida este método también sobre las reglas del ordenamiento jurídico, así pues, las reglas se interpretarán en función a su participación dentro del esquema, la cual debe ser armónica con el resto de las pautas normativas, en primer lugar deberá coincidir con la percepción normativa constitucional, así se evita que la nueva construcción jurídica se convierta en un foco de vulneración de derechos constitucionalmente protegidos.

Capítulo II

El Phishing, Smishing y Vishing y la teoría de las necesidades como fundamento para su tipificación

2.1. Los trabajos previos a la investigación

La búsqueda de investigaciones anteriores ha tenido como resultado la ubicación de la tesis de Ventura Quijano Mishell Alisson (2021) que lleva por título "La tipificación del Phishing, Smishing y Vishing en nuestro sistema penal peruano, para la lucha contra la ciberdelincuencia en Lima, 2020", presentada a la Universidad Privada del Norte para obtener el título profesional de Abogada; de la cual se recoge la siguiente conclusión:

"(…) la naturaleza jurídica que deben adoptar las modalidades del phishing, smishing y vishing como primera instancia se concebirían como delitos de peligro abstracto cuyo bien jurídico a proteger seria la seguridad informática, y segunda instancia cuando estos delitos logren agravarse la naturaleza jurídica cambiaria a delitos de resultado cuya finalidad es proteger al usuario". (Ventura & Roque, 2021, pág. 77)

También se toma como referencia la tesis de Devia Gonzales Edmundo Ariel (2017), que lleva por título "Delito informático: Estafa informática del artículo 248.2 del Código Penal", presentada a la Universidad de Sevilla para obtener el grado de Doctor en Derecho, de la cual se recoge la siguiente conclusión:

“Se ha visto, que él legislaciones como la chilena se ha tenido que forzar la ley penal, para poder adecuarla a los nuevos delitos, especialmente en el caso del fraude, debiendo ser un esfuerzo la judicatura para poder lograr que a base de la norma existente pueda sancionarse un hecho ilícito relacionado con la informática en este caso estafa informática. Podemos decir entonces, que es necesario adecuar la técnica legislativa a los nuevos tiempos”. (Devia, 2017, pág. 366)

De igual manera se ha considerado la investigación de Hidalgo Coronel Carito Natividad y Solano Vidal Gerson Steve (2021) que lleva por título “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”, presentada a la Universidad Nacional del Santa para obtener el título profesional de Abogado; de la cual se ha recogido la siguiente conclusión:

“Es necesaria la creación de un tipo penal específico, que regule adecuadamente el phishing, donde se establezca con precisión la conducta típica, el bien jurídico protegido, así como una pena en concordancia con la magnitud del daño causado a los bienes jurídicos”. (Hidalgo & Solano, 2021, pág. 116)

Se hace necesario tomar en consideración la tesis de Sosa Umbo Omar Arturo (2022) que lleva por título “Phishing como modalidad de delitos informáticos: a propósito de la suplantación y robo a los beneficiarios del bono universal en el Perú”, presentada a la Universidad Nacional de Piura para optar el título profesional de Abogado, de la misma que se recoge lo siguiente:

“El delito de Phishing es un delito informático porque cumple con las características de ser un comportamiento que se aprovecha del uso indebido de

tecnologías de la información y de la comunicación para el acceso ilícito de datos informáticos privado y poder usarlos en perjuicio de los sujetos pasivos del delito. El delito de Phishing no se encuentra expresamente tipificado en la Ley 30096 a pesar de contar con similitudes normativas con el delito de Suplantación de Identidad. Uno de los análisis que se pudo observar es la existencia de disposiciones generales en cuanto a la redacción de delitos, sobre todo, el delito de Suplantación de Identidad dejando de lado la realidad material de otros delitos, que, aunque parecidos como el Phishing, hoy no gozan de tipificación legal y propician su impunidad". (Sosa, 2022, pág. 48)

Finalmente se ha de considerar la investigación desarrollada por Esparta Centeno Maritza Marisol (2022) que lleva por título: "Mecanismos de prevención y protección del bien jurídico tutelado frente a la modalidad delictiva Phishing en el ordenamiento jurídico penal peruano", presentada a la Universidad Inca Garcilaso de la Vega para obtener el título de Abogada, tesis de la cual se ha recogido la siguiente indicación:

"Se determinó que el tratamiento legislativo en el derecho comparado respecto del phishing tal como los países de México y Colombia, cuentan con una legislación adecuada, ya que tipifican el delito de manera específica, de tal manera que permite una persecución eficaz dicha modalidad delictiva; sin embargo, cabe precisar que en el caso de Ecuador no está tipificado lo cual permite que no hay un avance en cuanto a la severidad de la pena". (Esparta, 2022, pág. 80)

2.2. La concepción del phishing, smishing y vishing como acciones delictivas

De acuerdo al planteamiento de la investigación es importante considerar la situación real respecto al desarrollo de actividades ilícitas que conllevan a la percepción del fraude en el ámbito específico de la informática, sobre ello se puede establecer como una necesidad en tanto que "A pesar del interés teórico que genera el fraude informático, así como de la importancia práctica que tiene dicho delito, aún no existe total claridad respecto de qué implica con exactitud cometer una conducta que pueda calificarse de tal". (Mayer & Oliver, 2020, pág. 179)

Es en razón de ello que resulta importante considerar los planteamientos descriptivos que se han realizado sobre las modalidades delictivas seleccionadas, tales como el phishing, smishing y vishing, así pues, se tiene que el bien jurídico protegido con estos tipos penales corresponde a la seguridad informática en beneficio de los intereses sociales.

Llegado a este punto de la línea investigativa es importante delimitar lo que se debe entender por delitos informáticos, siendo por lo general "(…) aquellas conductas dirigidas a burlar los sistemas de dispositivos de seguridad, esto es, invasiones a computadoras, correos o sistemas de datas mediante una clave de acceso; conductas típicas que únicamente pueden ser cometidas a través de la tecnología". (Villavicencio, 2014, págs. 286-287)

Por consiguiente, los delitos informáticos son aquellos por los cuales se criminalizan conductas las cuales ingresan indebidamente a sistemas informáticos, lo transgreden y roban información, entendiéndose que el objetivo o finalidad de

esta clase de delitos es introducirse, extraer, y/o menoscabar sistemas o datos informatizados; empero también están los delitos computacionales, que es la realización de delitos tradicionales pero a través de medios electrónicos. Por ej., difamar mediante Facebook.

Entonces, abarcando esas dos diferenciaciones, se entiende que no todos los ciber-crímenes son castigados penalmente, ya que si este delito puede ser cometido a través de otra modalidad que no sea usando la tecnología, ya no puede ser considerado delito informático. Dicho lo anterior, los delitos convencionales como hurto, difamación, etc., que puedan ser realizados utilizando medios electrónicos como herramienta para cometer delitos, más no como objetivo. Por ende resulta muy importante identificar y delimitar cuáles son los delitos informáticos y, los delitos computacionales.

Se debe hacer tal puntualización, porque la Ley N° 30096, que regula los delitos informáticos, no explica en forma general qué debemos entender por tales ilícitos, es decir, no nos pone un concepto o palabras clave, teniéndose que interpretar en base a una fuente de derecho, en este caso la doctrina. Puesto que hay irrisorias sentencias o resoluciones, de las cuales podamos recoger la interpretación hecha por magistrados, quedando también en evidencia la falta de especialistas y peritos en delitos informáticos.

Dicho lo anterior, cabe precisar que sólo algunas conductas o modalidades de fraude informático se encuentran reguladas en la Ley de Delitos Informáticos, Nº 30096, norma que se tipifica las conductas penalmente relevantes, que afectan

desde sistemas y datos informáticos, la indemnidad y libertad sexuales, la intimidad; hasta el secreto de las comunicaciones, el patrimonio y la fe pública, en los cuales el sujeto activo hace uso de la tecnología con la finalidad de cometer diferentes ilícitos penales. (Zeballos, 2020)

Dicho en otros términos, si bien desde el año 2013 por Ley es atribuible a estos delitos la protección del bien jurídico correspondiente a la seguridad informática en beneficio de los intereses sociales; al ser considerados los delitos informáticos como pluriofensivos, también se deben proteger los bienes jurídicos tradicionales afectados a través de este tipo de delitos como son: el patrimonio, la reserva y confidencialidad de los datos, la fe pública, la indemnidad sexual y otros.

Sobre una posible incorporación de las modalidades del phishing, el smishing, y vishing, la autora Ventura (2021) citando al Dr. Ayala, menciona que la necesidad de su tipificación se sitúa en base a la criminalidad evolutiva percibida en la última década; de la mano con las nuevas formas de tecnología informática y la comisión de ellas como el empleo de ordenadores o dispositivos en general, que trasmiten datos o información. (pág. 47)

Lo que el autor citado busca dar a entender, es que la tipificación de las modalidades en mención beneficiaría al ordenamiento jurídico, ya que se individualizarían las conductas punibles, toda vez que, esta se legislaría a partir de una realidad social (muy concurrida en nuestro país), y no desde la realidad mundial; por lo que, discutiendo jurídicamente de lograrse la regulación de estas modalidades, se marcaría un precedente normativo, estaríamos adelantándonos a

proteger un bien jurídico que en diferentes legislaciones lo han acogido como la tutela de la seguridad informática.

Por otro lado, para muchos autores es trascendental que la ciudadanía reconozca las modalidades de fraude informático con la finalidad de que se pueda evitar el incremento de víctimas de delitos informáticos; es decir, resulta evidente la necesidad de que la población primero deba ser orientada sobre las formas de prevención del delito, y así en caso de ser una víctima potencial de estos delitos informáticos es sustancial conocer la Justicia Penal.

"(…) y si en caso ocurriera, se ha creado una División de Investigación de Alta Tecnología-DIVINDAT, que viene funcionando hace más de dos décadas, para que víctimas puedan denunciar el hecho ante tales autoridades policiales o, ante el Ministerio Público". (Zeballos, 2020)

Teniendo en cuenta lo anterior, los legisladores deben optar por mejores formas de enfrentar y difundir dichos delitos y, a la vez subir el listón de los operadores judiciales, con ello será eficaz la prevención de delitos informáticos, se debe también seleccionar a jueces con mayor nivel de formación para hacer frente no sólo a los delitos tradicionales sino también a los de alta tecnología.

Entrando específicamente al tratamiento de las modalidades mencionadas (phishing, smishing y vishing), todas estas conductas sancionables se materializan por lo general con la obtención de datos informáticos, suplantación de la identidad,

vulneración al secreto a las comunicaciones y la interceptación de datos informáticos o fraude informático.

Acerca del phishing, se debe entender a toda conducta destinada a robar y suplantar la identidad del sujeto pasivo (víctima), este delito se materializa obteniendo información privada mediante artificios y engaños, tal información varía desde: números y claves de tarjetas de crédito, información de estados de cuenta u otros datos de carácter personal. Esta modalidad se ha desarrollado a tal punto que ya tiene una subespecie, denominada spear phishing; que a diferencia del anterior, se centra en atacar a grupos vulnerables como adultos mayores.

Mientras que el smishing, se materializa con el envío de mensajes de texto en celulares, los cuales suelen enmascarar el número telefónico de origen, limitándose a mostrar en el texto direcciones web, enlaces, o links, parecidas a direcciones institucionales de empresas u organismos públicos; produciéndose tal vulneración al momento que el usuario haga clic sobre dicho enlace, el cual lo redireccionará a una página de phishing o, en otros casos, desde ese momento el dispositivo ya se encuentra contaminado por un código malicioso.

Por su parte, el vishing se entiende por aquellas conducta delictivas en la cual el sujeto activo envía mensajes de texto haciéndose pasar por una entidad bancaria, pidiendo bajo alguna excusa que se comunique con cierto número falso o, en otros casos, se solicita que responda el SMS revelando información confidencial, tales como: números de tarjeta o claves. (Gómez, 2006)

Sin lugar a dudas, los delitos informáticos merecen un especial tratamiento doctrinario, ya que estas y más modalidades de fraude cibernético, van en aumento; en ese orden de ideas, debemos tener en cuenta que la tipificación de estas modalidades de comisión de fraudes informáticos servirá para atenuar los delitos informáticos, y a su vez, identificar el espacio virtual donde se computan dichos ilícitos; ya que debido a su naturaleza exige que los agentes de justicia se encuentren estrictamente calificados para su tratamiento.

Sobre esto último, Ventura (2021) refiere que: "deberían se realizarse especializaciones para distinguir las diferentes modalidades mediante las cuales se comisionan estos ilícitos penales, de modo tal que se rompa con aquellas directrices habituales para la imputación de un delito tradicional". (pág. 9)

2.3. La justicia en la teoría de las necesidades

Es conveniente establecer este apartado teórico con la finalidad de clarificar la forma en que se construyen las reglas, esto es que se basan en la verificación de las necesidades sociales que debe percibir el legislador a fin de que se generen las políticas públicas destinadas a controlar, en este caso materia de control será la actividad delictiva en el campo de los delitos generado en el ámbito digital de la virtualidad.

Siendo así es importante reconocer que la cuestión teórica de la justicia se enfoca en el ámbito del derecho constitucional puesto que "La libertad y la igualdad, como elementos estructurales de la concepción de justicia procedimental, se

encuentran representadas en la persona moral que las articula simultáneamente, pero dando prioridad a la libertad". (Echeverry & Jaramillo, 2006, pág. 30)

Esta pauta es lo que permite establecer un sentido de justicia en razón de la capacidad que tiene el ser humano que se orienta a la efectividad de la protección, lo cual desde luego esta pautado sobre la percepción de estos sujetos sobre aquello resulta en beneficio o en perjuicio para su bienestar, lo cual lleva al sujeto moral a establecer un vínculo entre ambas posturas para tomar una determinación en base a su facultad de elección deliberada, lo cual conlleva a los acuerdos que se plasman en la sociedad.

Este aspecto es lo que deja en claro que sobre la cuestión de libertad pesa una consecuencia de riesgo, lo cual genera sin duda la necesidad de establecer pautas de parte del Estado para consolidar el efecto de protección en base al control de la actividad. Para el caso de las manipulaciones que sufre la actividad patrimonial en el ámbito de la comunicación digital, se encuentra una condición de peligro que debe ser atendida en función a las características peculiares que emanan de su propia naturaleza digital.

Esta condición de la teoría de las necesidades se verifica en el planteamiento que "(…) como John Rawls enfatiza en la necesidad de construir una pauta de distribución equitativa de las ventajas y desventajas provenientes de la cooperación". (Echeverry & Jaramillo, 2006, pág. 49)

Entonces, de acuerdo a lo señalado, se reconoce la postura de Rawls como base argumentativa que ancla la necesidad da la teoría de la justicia, puesto que se verifica como aquella necesaria acción que proyecte la construcción e pautas que distribuyan con equidad las ventajas que se han planteado en el sistema de justicia. Tal es el caso de la distribución de control de la justicia en el ámbito penal que se oriente a la protección de los individuos ante aquella latente amenaza de ciberataques que se consolidan como estafas perjudicándolos patrimonialmente.

Es apropiado dejar en claro que existen posturas un tanto más puntuales sobre el vínculo entre la necesidad social o personal y la creación de los derechos como reglas, puesto que señala "(…) pueden entenderse razones no concluyentes para la acción pero que pueden orientarla cuando no haya otros factores que demuestren lo contrario; ya que establecida la existencia de una necesidad constituye por sí misma una buena razón para satisfacerla aunque no para establecer directamente la existencia de un derecho". (Ribotta, 2008, pág. 52)

Capítulo III

El bien jurídico seguridad informática y su protección en el ámbito penal

Para la correcta comprensión del sentido de este capítulo, se ha diseñado una estructura que versa en dos fases, la primera orientada a la determinación de los bienes jurídicos en lo que respecta a su intervención en el esquema de protección que organiza el Estado para que mediante el derecho penal se ejerza control sobre el nivel de criminalidad que existe en la sociedad. Esta condición es importante considerar en primer término, puesto que conllevará a la comprensión de la concepción de los bienes jurídicos y entender que requerimientos intervienen para que sean contemplados en la construcción típica de los delitos.

Esta perspectiva invita a la construcción de la segunda fase de este capítulo que abarca a la seguridad informática para que sea incorporada en el ámbito de protección del derecho penal, esto es las justificaciones en el desarrollo de su actividad que orienten a un sendero de protección. Interesa más bien la conducción de elementos justificantes respecto al riesgo de lesión o perjuicio que pudiera producir tal afectación de la seguridad informática, sería ello lo que oriente el sentido de necesidad de tipificación de las acciones delictivas en torno a este supuesto.

3.1. La protección de los bienes jurídicos en el derecho penal

Lo que se debe comprender como bien jurídico depende de su función en el ámbito de la teoría del derecho penal, puesto que ello ha servido para adaptar ciertos

criterios que conlleven a clasificar algunas acciones humanas como delictivas, esto es sirve de soporte a la intervención punitiva que realiza el Estado. Este tipo de contemplaciones sirve entonces para la construcción de los tipos penales que permiten reconocer el nivel de responsabilidad de los sujetos mediante las reglas de imputación, lamentablemente esta construcción típica en los últimos tiempos ha recibido serias críticas respecto a su efectividad.

Una de las principales razones respecto al cumplimiento cabal de las funciones de los tipos penales es que no contemplan aun en su totalidad ciertos derechos que son relevantes en el ámbito social y requieren de la protección que otorga el derecho penal. Esto es que las descripciones que se hacen en estos tipos aún no logra recoger derechos emergentes en función a los cambios sociales; tal es el caso de la cuestión informática que traslada la necesidad de protección a la intervención estatal.

En base a esta comprensión se puede decir que no se logra este nivel de efectividad por un tema de ausencia de preocupación de parte de la gestión que se presume ha de fomentar la construcción de políticas públicas que recojan las necesidades sociales de manera correcta. Esta labor resulta de relevancia en tanto que la construcción de los tipos penales requerirá de criterios mínimos para su elaboración, esto es respecto a la percepción de las características para fundar un sistema penal adecuado como son: "(…) conceptualización, capacidad de fundar el sistema, capacidad para fundar el ilícito, titularidad de los bienes, disponibilidad de los bienes, entre otros (…)". (Kierszenbaum, 2009, pág. 210)

Es correcto entender que las percepciones que se tienen respecto al bien jurídico como un tema complejo, esto en tanto que se le asume como parte esencial de la estructura jurídica penal no solo por la descripción específica de las acciones que se califican como ilícitas, sino también porque constituyen una delimitación o restricción para que la intervención punitiva del Estado sea moderada a fin de evitar arbitrariedades que se comporten como vulneración de derechos. Tal protección debe estar en equilibrio con la necesidad social que implica la concepción de un bien jurídico, ello en tanto que se busca la garantía de "(…) solamente aquellos bienes que le puedan resultar útiles a los individuos para desarrollarse en sociedad (…)". (García Arroyo , 2022, pág. 40)

En sí debe tenerse como válida la idea de un retorno a la verificación de la esencial necesidad de protección de ciertos derechos para que sean incorporados como bienes jurídicos, tanto a nivel de riesgo de su existencia o ejecución, así como en función de la magnitud de lesividad que puede experimentar con relación a los ataques de otras personas o condiciones. Es por ello preciso que se complete el análisis de intervención del derecho penal con el fin de evitar excesos en el ámbito de protección que le compete al Estado, lo cual también traería como resultado la correcta identificación de bienes jurídicos que urge ser incorporados en el ámbito de la punición; tal es el caso del derecho que se desprende de la seguridad informática como un ideal para garantizar su efectividad y ejercicio en el mundo social.

3.2. La seguridad informática y su protección penal

En la sociedad moderna, servicios de todo tipo y en general muchas actividades realizadas cotidianamente dependen de sistemas y redes informáticas. Como ejemplo tenemos los servicios financieros, suministro eléctrico (redes de distribución), servicios médicos (historial clínico informatizado), redes de abastecimiento (agua, gas, etc.), o incluso los mismos órganos administrativos forman parte de todo el conjunto de servicios, que bien sean públicos o privados para un mejor funcionamiento se han visto en la necesidad de hacer uso de sistemas y/o redes informáticas.

Teniendo en cuenta lo anterior, a la seguridad informática se puede definir como cualquier medida que impida la ejecución de operaciones no autorizadas sobre un sistema o red informática, cuyos efectos puedan conllevar daños sobre la información, equipo o software; comprometiendo la confidencialidad, autenticidad o integridad de los usuarios (Gómez, 2006, pág. 27); entre otras afectaciones que se irán conociendo a lo largo de la investigación.

Sin embargo, actualmente la informática en su concepción amplia, pese a ser considerado el mecanismo más inmerso en las actividades del ser humano, (pero al no tener los filtros necesarios) y ser ampliamente vulnerable; viene siendo manipulado de forma incorrecta, motivo por el cual tiende a afectar ciertos derechos fundamentales, y con ello también se ven afectados determinados bienes jurídicos como la seguridad informática en beneficio de los intereses sociales.

Razón por lo cual ha tenido que intervenir el ámbito penal para delimitar su sanción y hacer cumplir la misma, en ese sentido, se debe tener en cuenta la definición de los autores Herrera y Núñez (1999), quienes diferencian peculiarmente el objeto del delito; con el bien jurídico protegido, precisando como el soporte lógico de un sistema de procesamiento de información incorporando además una distinción por los "delitos computacionales o informatizados y los delitos informáticos. (págs. 241-242)

Distinción que introdujera Jijena (1993); en ese contexto, los delitos computacionales están definidos como aquellas conductas delictivas tradicionales mediante en el cual se han utilizado los medios informáticos como herramienta de comisión; por otro lado entiende a los delitos informáticos como aquellos actos ilícitos que daña el soporte lógico de un sistema informático, en otras palabras un atentado al software, programas, datos o información. (pág. 350)

La principal característica de los delitos informáticos reside en la exclusiva protección que se le quiere dar a una nueva realidad que ha conquistado el mundo. Tal protección se puede expresar en términos de un específico bien jurídico que la norma tutela, el objeto material del delito lo constituyen los datos, informaciones y programas informáticos ajenos. (Moscoso, 2014, pág. 14)

Sobre esto último, se ha debatido por mucho tiempo acerca del bien jurídico protegido en los delitos informáticos, esto es porque dicho tipo penal es considerado como pluriofensivo; en otras palabras, pueden dañar paralelamente otros bienes jurídicos, los mismos que son protegidos por los tipos penales tradicionales, como:

el patrimonio, la reserva y confidencialidad de los datos, la fe pública, la indemnidad sexual y otros.

El interés digno de protección penal en los delitos informáticos está relacionado con la confidencialidad del soporte lógico de un sistema automatizado de información. La aceptación de tal bien jurídico implica un reconocimiento y respeto implícito del principio de la última ratio, fundamental para decidir la intervención del derecho penal en la sanción de conductas, limitando el campo de acción en la tipificación de conductas como delito informático y con ella la defraudación en base al bien jurídico seguridad informática en beneficio de los intereses sociales. (Ventura & Roque, 2021)

Para los usuarios, proteger su información suele ser más significativo que resguardar el software o sus dispositivos, por lo que, para conservar la seguridad de los datos, se deben cumplir tres elementos esenciales: primero la integridad, se concibe que la información únicamente puede ser modificada por entidades autorizadas; disponibilidad, donde se puede acceder a la información cuando se necesita, y confidencialidad, por la cual solo las instancias autorizadas o competentes pueden ver los datos. (Vélez, 2022, párr. 4)

Para Espinoza (2017), los representantes y legisladores deben poner énfasis en "(…) prevenir, reducir, tipificar y sancionar debidamente los delitos informáticos para el control de la sociedad frente al mundo digital y darles seguridad jurídica a las leyes sobre delitos informáticos, con el fin de reducir los índices de cibercriminalidad". (pág. 166)

Antes de culminar este acápite, cabe precisa que por delito informático se entiende a determinadas conductas que dañan bienes jurídicos relacionados con la tecnología, como una conducta típica, antijurídica y culpable cuyo objeto es la protección de tecnología de información.

Capítulo IV

Análisis y resultados

4.1. Sobre el análisis:

Es en esta sección de la tesis en la que se desarrollará la evaluación de la realidad en la que se estaría produciendo la situación problemática identificada por la tesis, evaluación que se hará en función a lo que se ha determinado como meta principal de la investigación esto es el objetivo general: Determinar si resulta adecuada la tipificación del phishing, smishing y vishing como modalidad de defraudación para garantizar el bien jurídico seguridad informática.

Sobre lo indicado corresponde aplicar dicha evaluación respecto a la población y la muestra planteada, material de análisis que se ha conseguido mediante el acceso a la información ante el Ministerio Público, lo cual se tiene como resultado bajo la indicación siguiente:

Población

En función a la propuesta de nuestro trabajo nos proyectamos a definir como población al Distrito Judicial de Lima Centro, en el cual se enfocará el trabajo de campo direccionado a obtener información proporcionada por el Ministerio Público, con el fin de evaluar el nivel de incidencia de casos que no se encuentran tipificados y en función a ello establecer la necesidad de nuevas tipificaciones

punitivas que alcancen a establecer una verdadera protección del bien jurídico seguridad informática.

Además de esta indicación se debe señalar que de la data proporcionada se ha obtenido una parte que constituye la Muestra de la investigación y se consigna en función al total de los datos que señalan los actos ilícitos cometidos que no se encuentran tipificados en el ordenamiento de la Ley de Delitos Informáticos.

Para la obtención de información respecto a la forma en que se está tratando la posible tipificación de la “Estafa Informática”, se ha solicitado información en los despachos fiscales provinciales penales del distrito judicial de Lima centro, tomando como muestra la data estadística que permite verificar la existencia de ilícitos no tipificados en la Ley de delitos informáticos. Además se ha recurrido a la búsqueda de datos mediáticos en los que se plasman las condiciones conceptuales que describen a la tipificación propuesta por esta investigación con la intención de proteger la seguridad informática de manera más eficiente, resultados que se muestran en el análisis de la opinión pública.

4.2. Análisis estadístico sobre delitos no tipificados

Como se ha indicado anteriormente con la data proporcionada por el Ministerio Público se ha procedido a evaluar el nivel de incidencia de casos en los que no es posible generar una tipificación adecuada dado que la conducta no se encuentra descrita de manera específica en el esquema de la Ley de delitos informáticos, ello toda vez que no se cuenta incluso con la operatividad tecnológica ni por parte de la Policía Nacional especializada ni por el Ministerio Público que permita reconocer el origen de los actos y menos la identificación de los agentes, por lo cual se produce el archivamiento de la denuncia sin mayor efecto jurídico.

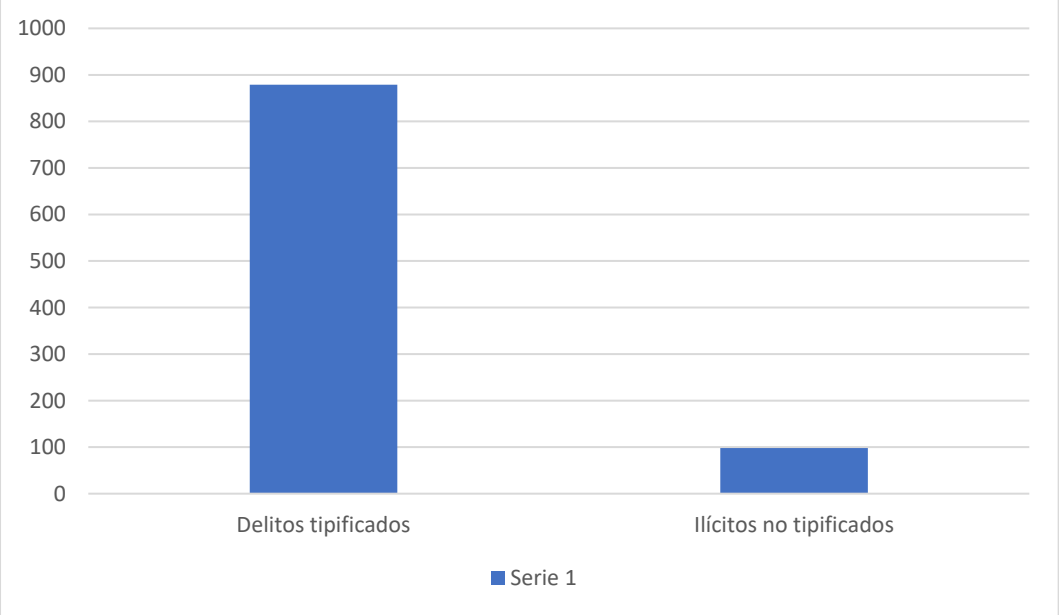
Según lo que se plantea el resultado de la verificación estadística que proporciona el Ministerio Público indica cantidades variadas en cuanto a los tipos establecidos en el ámbito de la Ley de Delitos Informáticos, siendo los más cercanos a la descripción conceptual sobre lo que propone esta investigación como lo sería la tipificación del phishing, smishing y vishing, por lo mismo que se toma estas cifras en tanto que se vinculan con la posibilidad de coincidir como la modalidad de defraudación para garantizar el bien jurídico seguridad informática, lo cual se detalla a continuación:

Tabla 1: comparación de la data estadística sobre la cantidad de delitos informáticos tipificados e imputados frente a la cantidad de ilícitos no tipificados y archivados en el Distrito Judicial de Lima Centro durante los años 2022 y 2023

Delitos tipificados	Ilícitos no tipificados
879	98

Las cifras mostradas como resultado de la evaluación estadística, detallan una condición de insuficiencia de la Ley de Delitos Informáticos para cubrir los aspectos que se muestran como índices delictivos solamente en el distrito judicial de Lima Centro, lo cual si se trasladaría como análisis a nivel nacional sin duda tendría una mayor cantidad de casos en los que no se podría establecer un parámetro adecuado de control. Sin duda alguna lo que deja ver este resultado es que se tiene un primer nivel de acción de la protección estatal sobre el bien jurídico seguridad informática en tanto que la tutela jurídica aun no se ha consolidado de manera adecuada o mas bien resulta insuficiente para asumir la innovación de la delincuencia informática.

Ilustración 1: Gráfica comparativa de la data estadística sobre la cantidad de delitos informáticos tipificados e imputados frente a la cantidad de ilícitos no tipificados y archivados en el Distrito Judicial de Lima Centro durante los años 2022 y 2023



Fuente: Elaboración propia en base a la información proporcionada por el Ministerio Público según anexo 1.

OBSERVACIÓN: La existencia de ilícitos reconocidos en la realidad por parte el Ministerio Público que no encajan en la configuración típica que establece la ley de delitos informáticos, es lo que permite razonar sobre la existencia de una posibilidad o más bien la necesidad de ajustar la mencionada Ley hacia estos aspectos, que como se aprecia en el gráfico, representa casi el 10% del total de las imputaciones realizadas en función a la normativa existente. Ello impulsa al razonamiento de que la condición que muestran las figuras del phishing, smishing y vishing, que permitirían la contemplación jurídica de aspectos no incorporados en la regla y que desde luego cumplen con la característica de defraudación, la misma que se ha concebido respecto del concepto de del bien jurídico, seguridad informática

4.3. Análisis de la opinión mediática sobre los delitos phishing, smishing y vishing

Tal como se ha indicado en la estructura de análisis de esta investigación se ha recurrido a la información mediática con el fin de verificar la existencia de casos relacionados con el concepto del phishing, smishing y vishing, que se producen en la realidad social y que permitirían identificar la necesidad de ser regulados y promover la implementación de medios informáticos suficientes para que la intervención del Estado sea eficaz mediante el ius puniendi y de este modo reforzar el campo de acción sobre los delitos informáticos en función al bien jurídico seguridad informática.

Tabla 2: Tabla descriptiva de la información mediática sobre los delitos phishing, smishing y vishing

Fuente de información	Descripción
Diario La República- Perú https://larepublica.pe/tecnologia/2022/10/30/peru-es-el-pais-con-mas-ataques-de-phishing-en-latinoamerica-como-evitar-caer-en-esta-ciberestafa-evat	"Perú es el país con más ataques de phishing en Latinoamérica: ¿cómo evitar caer en esta ciberestafa?" Esta descripción esta referida a la existencia de una modalidad delictiva que se manifiesta a través del uso de los mensajes de texto comunes, mediante los cuales se solicita información sobre las tarjetas de crédito, acción que se vale tanto de la ignorancia de la población sobre la protección informática y el cuidado que se debe tener con este tipo de

	información personal, razón por la que se terminan produciendo este tipo de ataques. La realidad que muestra la nota periodística es que existe un alto nivel de este tipo de acciones que se conoce teóricamente como Phishing y que desde el año 2021 ha ido incrementando su acción al punto de considerar un resultado cuadruplicado de las cantidades de denuncias por este tipo de casos. Muestra además la existencia de modalidades que se ocupan del uso de los correos electrónicos con la intención de establecer un mayor alcance de los sujetos incautos sobre su información personal, para lo cual se precisa de una alta y sofisticada tecnología informática. La data recopilada a nivel de Latino América pone al Perú en el más alto nivel de acciones que han detectado y denunciado este tipo de actos, alcanzado a representar el 33% de este espacio geográfico superando a los demás

	países, lo cual indica una situación de riesgo alto, más aún si la Ley especializada no establecer una tipificación o sanción para garantizar la protección de la seguridad informática.
Diario Oficial El Peruano https://www.elperuano.pe/noticia/221669-el-sector-financiero-es-el-mas-usado-en-los-ataques-de-phishing	"El sector financiero es el más usado en los ataques de phishing" Según lo que se puede apreciar de la información mediatizada, es que existe un alto índice de acciones que se producen en la realidad social sobre el phishing, al punto de haberse establecido un registro de treinta y un millones casos en los que se ha producido este tipo de acción ilícita, que pone al Perú en el tercer lugar de los países latinoamericanos. Indica además que según las cifras estadísticas se tiene un nivel de incremento a nivel de Latinoamérica que se grafica con el 617% hasta el año 2023 lo cual se considera un real problema social, puesto que sin duda tiene vinculación con el aspecto jurídico que deberían desarrollar los estados con el fin de evitar este tipo de actos, siendo una de las

	herramientas más importantes para este fin el hecho de establecer sanciones específicas que permitan la persecución de este tipo de actos, lo cual precisa de ser incorporada a la ley correspondiente. Toda esta situación del incremento entre los últimos años lo relacionan con el incremento del uso de las tecnologías informáticas a razón de los últimos acontecimientos mundiales relacionados con la pandemia de COVID-19. Esta circunstancia obligó a la población a un acercamiento a la tecnología de este tipo sin tener el previo conocimiento de la peligrosidad y los cuidados necesarios en el campo informático. Situación que se ve incrementada sobre todo en el campo de las actividades financieras y empresariales que requieren de esta intervención tecnológica para alcanzar un mejor desarrollo económico pero que tiene efectos negativos como la exposición de la información ante un espacio invadido por este

	tipo de delincuentes y que se posicionan en un espacio de poder frente a la vulnerabilidad de los usuarios de estos sistemas informáticos.
Diario El Comercio- Perú Alertan de las campañas de 'smishing', que emplean SMS fraudulentos para infectar los celulares y robar a las víctimas | TECNOLOGIA | EL COMERCIO PERÚ	"Alertan de las campañas de 'smishing', que emplean SMS fraudulentos para infectar los celulares y robar a las víctimas" Como se puede apreciar esta información mediática sobre el campo de los delitos informáticos detalla condiciones de la modalidad de Smishing, que se vincula con la intervención tecnológica de los teléfonos móviles para promover la estafa cibernética. Se muestra la capacidad de la delincuencia para acceder a esta tecnología informática social, en la que se valen del acceso a los medios informáticos a través de los mensajes celulares y obligan o manipulan la voluntad de las víctimas con el fin de que se genere la descarga de aplicaciones maliciosas que provocan el robo de la información contenida en las tarjetas de crédito u otros elementos que vinculen con entidades financieras para

	establecer el robo no solo de datos sino también con ellos acceder al dinero de las víctimas. Este tipo de acción delictiva bajo la modalidad indicada, se vale incluso del acceso a los equipos móviles con el fin de trasladar a través de este equipo infectado otros mensajes a más celulares con los medios informáticos para acceder a la información sensible y lograr así mayor cantidad de víctimas. Como se puede apreciar es un actuar que se vale de la tecnología social para desarrollar acciones delictivas como un mal uso de esta información, lo que depende también del interés de los Estados para alcanzar un efectivo control.
Diario El Comercio- Perú	"Osiptel registró 305 casos de fraude financiero en el año" La situación nacional que se muestra es de consideración en tanto que el nivel de gravedad lo detecta la información proporcionada por la Policía Nacional, dado que solo en Lima la existencia de caso delictivo llega a superar la cantidad de cuatro

	mil, vinculados de manera directa con el consumo de la ciudadanía. De una manera más específica se muestra la cantidad de mas de trescientos casos detectados por OSIPTEL que como ente regulador se ocupa de las telecomunicaciones, todos respecto a la acción delictiva relacionada con los fraudes en el campo de lo financiero, desde luego en este espacio de actividad se utilizan los medios tecnológicos, aspecto que se convierte en una puerta de ingreso a los mal intencionados sujetos cibercriminales. Se pueden apreciar datos interesantes que muestran la condición de necesidad social respecto a mayor control de la actividad delincuencial en este campo de la tecnología informática, lo cual indica que un poco más de la mitad de casos se estarían registrando respecto a la reposición de los chips de celulares, espacio que es aprovechado para acceder a la información más sensible de los usuarios.

Capítulo V

Contrastación de la hipótesis

5.1. Discusión de los resultados

5.1.1. Discusión sobre el objetivo específico: "Interpretar la posibilidad de incorporar la tipificación del phishing, smishing y vishing en base a la teoría de las necesidades"

Discusión de los trabajos previos

Se tiene como primer antecedente a criticar, la tesis desarrollada por Ventura (2021) ¿Qué efectos debe contemplar el bien jurídico a ser protegido por el tipo penal propuesto sobre la modalidad de pishing?, según lo señalado por el antecedente existen dos vertientes para asumir el bien jurídico que se presume como protección del tipo penal propuesto sobre la modalidad de Pishing, la primera vinculada con la condición abstracta para su protección, entre tanto que señala otra alternativa relacionada con la protección del usuario que acude al servicio de la informática.

Esta connotación conlleva a la crítica sobre el postulado de los efectos de la protección, que resulta ser en función a la garantía que se ofrece para mantener protegido el sistema de justicia vinculado con el ordenamiento jurídico, respecto de la intervención de terceros; entre tanto que es posible asumir la existencia de un bien jurídico con referencia al entorno del propio sujeto titular del derecho que se pretende proteger.

En tal sentido la connotación de un bien jurídico para este tipo de acto delictivo se traduce en la necesidad de asegurar el tráfico informático para los

usuarios del ciberespacio; a tal punto que se obtiene garantía tanto sobre el sujeto de derecho que accede a este ámbito, así como a la condición abstracta que constituye.

Además se tiene la postura desarrollada por los investigadores Hidalgo y solano (2021) quienes plantean la necesidad de generar un tipo penal específico que se configure en el ordenamiento jurídico penal en un artículo 7-A en la ley de delitos informáticos N° 30096, lo cual se advierte como una intención positiva pero carente de fundamentos puntuales que muestren la justificación de este nuevo tipo penal, sobre todo atendiendo a la peculiaridad específica que sugiere, puesto que lo configuraría como un tipo autónomo. Ante lo señalado cabe preguntarse ¿cuál es el fundamento jurídico válido para incorporar al Phishing como un tipo penal autónomo?

De acuerdo a lo estudiado puede señalarse de esta modalidad de afectación en el ámbito informático, que se trata de una acción que traslada el interés delictivo a través de lo que se conoce como el cebo informático para atraer a las posibles víctimas, siendo que estas últimas al acceder a dicho entorno virtual terminen siendo afectadas en sus derechos, sobre todo en el aspecto patrimonial, de confidencialidad e incluso de identidad. Esta última indicación es lo que posiblemente justificaría la intervención del Estado para crear un tipo penal específico destinado a proteger este tipo de intereses; sin embargo, la intención de estos autores puede ser criticada respecto a la ausencia de razones justificantes para dicho establecimiento tipológico de la conducta descrita.

Se ha de tener en cuenta la tesis de Sosa (2022) en la que solo se realiza una descripción de la modalidad de Phishing asumiéndola como una suplantación de identidad, que desde luego no se encuentra regulada en la ley de delitos

informáticos, señalando que bien podría incorporarse bajo el argumento de similitud con el delito de suplantación de identidad, desde luego en la modalidad relacionada con el manejo y abuso de la data informática. Sobre ello se puede señalar que resultaría apropiado conocer el alcance del tipo sugerido, esto es que aspectos descriptivos deben observarse para que se configure la suplantación.

También se ha considerado la investigación de Esparta(2022) sobre las distintas modalidades delictivas del pishing y los mecanismos de prevención y la protección del bien juridico tutelado, el uso de la información personal en el ciberespacio a nivel mundial , resulta increíble la posibilidad de acceder a tanta información de datos personales a través de la red , estos ilícitos desbordan sobre la soberanía de los estados, convirtiéndose en un tema de criterio transnacional que requiere de mucha atención y cooperación de todos los gobiernos sin distinción alguna, con el fin de generar un debate sobre su regularización jurídica en lo referente al ciberdelito , cibercrimen o delitos informáticos en general.

¿el phishing como conducta delictiva aún no está regulada en el ordenamiento jurídico peruano? Tal cual se ha señalado en el antecedente de Esparta, se precisa de que los tipos penales tengan un acondicionamiento exacto a la realidad que intenta describir, para ello se precisa del conocimiento adecuado de los conceptos jurídicos vinculados al phishing. Esta condición será lo que permita una regulación adecuada, es decir evitar con ello que se califique la acción haciendo el acondicionamiento de la conducta a otro tipo penal que lo recoge.

De acuerdo a las condiciones en las que se han desarrollado los trabajos previos, permite establecer un nivel de conocimiento que traslada la información como objeto de la acción ilícita hacia un nivel de importancia suficiente que

garantice la protección de los derechos involucrados, acción en la que toma parte el Estado a través de la incorporación de reglas suficientes para satisfacer el requerimiento de seguridad. En tal sentido conviene consultar si es que ¿la concepción de las figuras conocidas como Phishing, Smishing y vishing es lo suficientemente adecuada para permitir la configuración de un tipo penal que las describa de manera conjunta o individual?

Considerando el hecho de que la conceptualización de estas modalidades de intervención delictiva resulta muy cercana en cuanto a la manera de obtener los datos que serán materia del tráfico, así como respecto a los agentes que cometen dichos actos; se convierte en una condición de similitud que conllevaría a la construcción de un tipo penal que acumule las tres acciones en una sola figura delictiva.

Esta connotación en grupo de las acciones a describirse en el tipo penal propuesto, tienen su base en el supuesto de que se trata de acciones comunes relacionadas con la obtención de información mediante engaño, lo cual permite asumirla como un fraude, razón por la que se admitiría como parte específica de los delitos informáticos. Para tal efecto se habría de considerar como elemento normativo a la acción que persigue obtener la información que los usuarios de diferentes sistemas vinculados con base de datos sean informáticos o de carácter personal; luego de ello tendría que considerarse un aspecto de elementos descriptivos para señalar de manera puntual las condiciones o ámbitos en los que se produce esta modalidad.

Teniendo en cuenta que la incorporación de los tipos penales al sistema de justicia que va de la mano con el ordenamiento jurídico, se precisa de que existan justificaciones como las ya antes explicadas pero que confluyan en un aspecto importante como lo es la necesidad. Justamente este aspecto es lo que se relaciona con la teoría de las necesidades, la misma que en su momento permitió la construcción del propio ordenamiento constitucional. Por lo que resulta correcto cuestionar ¿Qué vínculo existe entre la teoría de las necesidades y la propuesta de reconocimiento del Smishing, Phishing y el Vishing en la estructura típica que contempla la ley de delitos informáticos?

La verdadera razón de incorporar un tipo penal al ordenamiento jurídico, se traslada hacia la concepción de un a necesidad de interés social; esto quiere decir que, la existencia de riesgos dentro de las relaciones sociales provoca un sentido de necesidad respecto al cuidado que debe tener el Estado para consolidar la seguridad ciudadana. Esta necesidad debe estar orientada en razón de las particularidades de cada situación, las mismas que deberán ser individuales para que no se produzca con su incorporación un problema de conflicto de leyes.

Teniendo en cuenta este primer aspecto, para el caso de los delitos informáticos se tiene ya esta condición particular, pero se hace mucho más específica en tanto que se reconoce en la realidad informática cuestiones bastante particulares que plantean los delitos antes mencionados. Entonces, la regulación de los mismos obedece a una situación de carencia, que consolida un nivel de lesión alto respecto a estas intervenciones sobre la identidad de los sujetos que se sirven de la tecnología para poder realizar acciones de subsistencia.

Siendo así, la teoría de las necesidades se comporta como un elemento de apoyo bastante útil en tanto que se proyecta a la solución de los problemas que

surgen en la sociedad según el avance de las tecnologías, para este caso particular, debiendo procurar un sentido de dinamismo en el derecho y la construcción del ordenamiento jurídico, vale decir que se debe procurar que el derecho siempre seste a la vanguardia de los avances, que en este caso el progreso de la tecnología ha permitido además de ello la apertura de acciones ilícitas, manejadas en función a la ausencia de regulación.

TOMA DE POSTURA:

Respecto a la posibilidad de incorporar la tipificación del phishing, smishing y vishing en base a la teoría de las necesidades se puede señalar que la tecnología informática se va convirtiendo en una herramienta para cometer delitos, la cual conlleva competencias y desafíos al momento de llevar a cabo una investigación. Así, mientras más avanza la tecnología en el ciberespacio, genera más dificultad y muy pocas posibilidades de configurar un delito cibernético, por lo que considero que para la comisión de este tipo de delitos no solamente basta una computadora si no el uso del internet es indispensable. No existe ciberdelito que se pueda cometer sin acceso a internet, P ero no todos los delitos cometidos mediante el uso del internet son ciberdelitos.

Por otro lado, es de mucha importancia actualizar o reclasificar los delitos informáticos o ciberdelito, ya que la tecnología en el ciberespacio avanza y se agrava cada vez más con cada categoría del delito informático, debido que existen alguno de ellos que están dentro del código penal y no dentro de la referida ley especial. Mientras ella no ocurra seguiremos denominando delitos informáticos o ciberdelitos a los 8 tipos penales ya considerados en la ley Nº 30096.

5.1.2. Discusión del objetivo específico: “Desarrollar las justificaciones jurídicas para comprender el bien jurídico de seguridad informática como objeto de protección en el ámbito penal”

Esta discusión se enfoca a la ubicación de fundamentos jurídicos válidos que permitan establecer una ruta correcta hacia la ampliación de los bienes jurídicos existentes como objeto de protección en el ordenamiento jurídico; es así que se debe partir por la comprensión correcta de estos elementos, es así que se cuestiona ¿qué caracteriza a los bienes jurídicos protegidos en el derecho penal?

De acuerdo a dicho cuestionamiento se percibe como apropiada la postura que enfoca al bien jurídico como la traslación de los derechos de mayor relevancia en el conjunto de aquellos que reconoce la constitución y que se perciben como de mayor posibilidad de vulneración; para tal comprensión debe dejarse en claro que no todos los derechos son susceptibles de protección mediante la participación del derecho penal, como tal se percibe el efecto del límite a la intervención penal, esto es que el ius puniendi solamente se puede aplicar en tanto no existan otras formas de solucionar el problema de manera previa, esto es que se debe activar la potestad punitiva en tanto que no se haya resuelto el inconveniente en otros ámbitos jurídicos.

La última ratio se concibe como el principio que plantea lo señalado anteriormente, por lo mismo que resulta válido hacer esta observación de manera inicial, es así que las acciones que operan sobre el ejercicio punitivo dependerán de una verdadera necesidad, esto se ha señalado con anterioridad en la descripción de los actos lesivos de derechos en el ámbito informático. Es sobre este campo en las

que se desarrollan las acciones delictivas donde no se aprecia un manejo adecuado de la intervención del Estado, básicamente en el establecimiento de las pautas descriptivas de la delincuencia que hace uso de la tecnología para cometer actos ilícitos, lo cual convierte en a los derechos que participan en este ámbito sean vulnerados con frecuencia sin que exista la posibilidad de acceder a una atención adecuada respecto de ello.

Se entiende que la construcción de nuevos tipos penales requiere previamente verificar la necesidad de proteger cierto derecho que ante el riesgo latente, pero siempre hace falta el establecimiento de ciertos factores, lo cual conlleva al cuestionamiento ¿qué requisitos se precisan de manera previa para la comprensión de un derecho como tipo penal? Sobre ello se puede indicar que el primer factor que debe considerarse es el de la conceptualización, esto es que se reconozca el derecho en la realidad, vale decir tanto desde el punto de vista teórico así como desde la verificación práctica de su ejecución en la vida cotidiana.

Luego del primer punto que se refiere a conceptualizar de manera correcta el derecho que se pretende proteger, se deberá observar la capacidad del propio sistema para que adopte este nuevo derecho como necesidad de protección, es decir que exista un espacio adecuado como grupo de derechos ya protegidos como posibilidad de acoger este tipo de elemento o derecho a proteger. Además de ello otro factor será el reconocimiento de la capacidad del propio sistema para que funde la acción como acto ilícito, los elementos del tipo que deben ser descritos de manera puntual y certera a fin de lograr el sentido correcto la acción.

Seguidamente se percibe otro factor que implica la verificación de los titulares del bien que se pretende incorporar como materia de protección, esto se vincula con la propia conceptualización del derecho, es así que se tratará de una delimitación de sujetos que puedan ser susceptibles de protección en función a la actividad que desarrollen, caracterización que logra una determinación adecuada del bien jurídico, que desde luego se convierte en otra necesidad de observar el sentido de correspondencia de la protección, es decir que en la realidad se encuentren tales derechos como disponibles, solo así se podrá establecer de manera adecuada la intervención del derecho penal para asumir estos derechos como bienes jurídicos.

Para el caso que se traslada a esta investigación, la percepción conceptual de los actos ilícitos es lo que ha impulsado a la doctrina para establecer una definición lo más cercana posible sobre el phishing, smishing y vishing, sobre ello se ha señalado en la discusión anterior una definición puntual que conlleva al segundo nivel de evaluación para considerarlos como bienes jurídicos susceptibles de protección, ello en tanto que el sistema penal tiene la posibilidad de asumirlos en el esquema de los delitos informáticos, creando desde luego un espacio específico para los que se comenten en el ciberespacio como tal.

De acuerdo a lo señalado por García (2022) es importante contemplar una característica importante como lo es la teoría de las necesidades como base fundante de los derechos y su protección es así que se pregunta ¿cómo se justifica la necesidad social de un bien jurídico? Ante ello se indica que la existencia de derechos en el ordenamiento jurídico tiene como punto de partida la verificación de

la necesidad social, lo cual conlleva a otorgar derechos específicos para cada individuo que van desde los fundamentales relacionados directamente con su integridad y luego los constitucionales netamente vinculados con aspectos del desarrollo de los sujetos en sociedad, derechos que tienen la necesidad de ser protegidos. En este aspecto es donde interviene una suerte de discriminación necesaria de los derechos que si justifica la participación del derecho penal en este caso, para que se ocupe de crear pautas normativas que favorezcan esta seguridad, es precisamente en el caso de los delitos cibernéticos vinculados con el carácter de necesidad de otorgar a los sujetos herramientas de protección en este ámbito que a través del paso del tiempo y del avance tecnológico se ha convertido en un espacio de desarrollo para cada uno de los que intervienen y se vinculan en él.

De acuerdo a lo señalado se puede indicar como posibilidad de contemplar a la seguridad informática dentro del ámbito de protección penal, lo cual se verifica en función a los factores antes indicados para tal fin, sobre todo teniendo en cuenta las razones vinculantes de esta necesidad, dado que la actividad informática y el manejo del ciberespacio se ha convertido en una situación normalizada en la actualidad, se trata de una actividad común de una gran cantidad de personas, lo cual incluso se vincula con la globalización como eje de desarrollo de las naciones y los propios individuos.

Las garantías que se presentan como necesidad de protección deben estar orientadas hacia le ejecución de acciones sin autorización de los titulares de los derechos en el ámbito informático, lo que se pretende es evitar los daños a producirse respecto tanto sobre la información, el equipamiento para el desarrollo

de estas actividades y así como el propio software, que vincule actos lesivos de confidencialidad, el carácter auténtico e íntegro de los sujetos que participan en este tipo de actividades cibernéticas según lo señalado por Gómez (2006).

En función a lo señalado se puede establecer que en efecto se presenta como posibilidad el contemplar al bien jurídico protegido idóneo como la seguridad informática para establecer adecuadamente tipos penales que permitan abarcar la mayor cantidad de acciones ilícitas en el campo de la informática, sobre ello debe cuestionarse ¿sería apropiado considerar el carácter pluriofensivo de los tipos penales? Esta verificación como una de las características de los tipos penales se convierte en una útil herramienta en tanto se presentan en la realidad diversidad de acciones vinculadas entre si, sobre todo en el ámbito de la informática, que compromete como tales datos, equipos, herramientas informáticas, espacios virtuales determinados que consolidan la afectación de diferentes áreas donde se producen las lesiones.

Se pretende una protección idónea del bien jurídico que abarca diversos tipos penales o acciones a describir por un tipo determinado, propiciando un campo de garantía sobre el carácter de confidencialidad en los elementos de acción informática, sobre todo teniendo en cuenta los diversos soportes que permiten la existencia de sistemas de información o datos automatizados. Se proyecta como tal la seguridad o garantía ante la posible defraudación respecto a la seguridad informática que se contempla como elemento de interés social que debe ser protegido de manera adecuada, que en este caso requiere de la participación del ius puniendi según lo señalado por Ventura y Roque (2021).

TOMA DE POSTURA:

Según lo discutido sobre las justificaciones jurídicas para comprender el bien jurídico de seguridad informática como objeto de protección en el ámbito penal, se ha podido establecer que se trata de un concepto en desarrollo, lo cual se debe a la realidad de este espacio donde la actividad humana se encuentra en constante evolución, dadas las circunstancias de avance tecnológico y la presencia de actividades cada vez más innovadoras, por lo mismo que se verifica la necesidad de orientar la atención de la potestad punitiva del Estado a fin de controlar adecuadamente este tipo de riesgos. Sobre todo se pretende establecer un marco normativo que consolide la garantía que se debe plantear ante la posibilidad de vulneraciones en conjunto y que conceptualmente aún no se logran definir con exactitud, lo cual se debe al constante crecimiento de la diversidad de actividades en este espacio virtual, importante ello sin duda por la necesidad de los ciudadanos como sujetos de derecho para alcanzar un desarrollo idóneo con este tipo de actividades y en mérito a la garantía de sus derechos.

5.1.3. Discusión del objetivo específico: "Analizar el nivel de afectación que produce la incidencia del phishing, smishing y vishing como defraudación sobre la seguridad informática"

El sentido de esta investigación se ha centrado en determinar si resulta adecuada la tipificación del phishing, smishing y vishing como modalidad de defraudación para garantizar el bien jurídico seguridad informática, una de las metas que sirven como base para aquella determinación, es lo que hace necesaria la

verificación de la característica lesiva de estas acciones ilícitas en el campo de la informática.

En tal sentido conviene cuestionar ¿qué característica del phishing, smishing y vishing es lo que podría constituirse como un resultado lesivo sobre la seguridad informática en el campo de la defraudación?, en definitiva la condición de seguridad de manera general se erige como un elemento sobre el cual el Estado debe protección a todos los ciudadanos, esto en perspectiva de la estrategia que constituye la política pública destinada para estos fines. El resultado de ello es la construcción del cuerpo normativo que se ocupe de tal fin sobre la garantía de seguridad en sus diferentes vertientes, interesa para esta investigación el carácter de seguridad que involucra la acción de los ciudadanos en las diferentes plataformas virtuales que la tecnología informática ha permitido crear como parte del crecimiento de las comunicaciones.

En la realidad se espera que lo antes explicado pueda servir de control a la actividad de todos los ciudadanos que interactúan en las plataformas antes mencionadas, lamentablemente aun no se tiene un espacio normativo lo suficientemente ágil o dinámico que permita reconocer de manera adecuada la acción lesiva que se produce como resultado de ciertas actividades como lo son el phishing, smishing y vishing. Este tipo acciones y sus resultados dependen de una característica general que se proyecta sobre la incursión de los agentes delictivos en el ámbito de seguridad que se supone debería estar garantizada por la estructura normativa.

Como tal, esta condición o característica específica de este tipo de acciones delictivas, producen sin duda afectación no solo al campo de la seguridad como ya se ha indicado, sino que además, existe correlación en dichos efectos con el ámbito de la economía de los sujetos afectados, puesto que el fonde la intención es apropiarse de los bienes que forman parte del tráfico informático o dependen de él. Este resultado lesivo también afecta de manera directa a las condiciones de seguridad sobre la data específica de cada sujeto, es decir lo que caracteriza a su personalidad a través de la información que se conserva en este tipo de ámbito, la misma que al ser accedida promueve un amplio campo de posibilidades para que el agente delictivo configure sus pretensiones de apropiación incluso de bienes.

Vista la característica de estas acciones delictivas que afectan la seguridad jurídica, es importante cuestionar ¿Qué tanto influye la incidencia sobre la necesidad de crear una tipificación especial para las acciones delictivas nominadas como phishing, smishing y vishing?, lo que se ha esperado del resultado que se desarrolló sobre la realidad punitiva que se desarrolla en el Perú respeto a este tipo de acciones delictivas, es precisamente la verificación del nivel de incidencia de estas acciones delictivas, por lo mismo que se recurrió a la opción de análisis estadístico a fin de reconocer si en efecto se trata de un problema recurrente.

El resultado que se obtuvo de la verificación de casos a nivel institucional del Ministerio Público, desde la perspectiva estadística mostró una cantidad de casos en los que la tipificación existente en el ámbito penal no alcanza para determinar este tipo de acciones estudiadas como phishing, smishing y vishing, no pueden ser calificadas como acción delictiva. La consecuencia de estas acciones,

según lo que indica el resultado estadístico, se dirige hacia la impunidad, lo cual representa un efecto totalmente negativo respecto a la seguridad que, como ya se dijo, corresponde al Estado para brindarla en función a la contemplación normativa de las posibles afectaciones que se produzcan sobre los bienes jurídicos.

Esta evaluación estadística consolida un tipo de acción, mostrada en función a las características lesivas que producen el phishing, smishing y vishing, como es el caso del acceso a los datos sensibles que posee cada ciudadano, acción que no ha sido autorizada por su propia persona, intervención que como tal constituye la vulneración a su derecho a la identidad e intimidad que forman parte de la dignidad como derecho principista. Cabe indicar que existe además de este tipo de lesividad la interceptación de los sistemas informáticos que pese a que se han creado bajo rigurosas medidas de seguridad, no resultan lo suficientemente efectivas para alcanzar la protección debida que se precisa de la regulación punitiva.

Otro de los aspectos que justifica la intervención del Estado es precisamente la condición de lesividad sobre el patrimonio de las personas afectadas, en sí la particularidad de esta acción ilícita, se orienta hacia la intención de apropiarse de los efectos patrimoniales que se manejan a este nivel de interacción informática. Resulta por ello demostrada la necesidad de establecer pautas jurídicas condicionadas por las características descritas sobre la acción delictiva, para que en base a dicha necesidad se justifique la creación de reglas específicas que contemplen elementos descriptivos respecto al phishing, smishing y vishing como acciones lesivas de la seguridad informática.

TOMA DE POSTURA

Conforme a lo desarrollado sobre el nivel de afectación de los ciberdelitos, donde no se identifican en el sistema legal los delitos de fraude, phishing, vishing y smishing; Sin embargo, los casos especificados han ido aumentando hasta variando sus modalidades cada vez hay más capacidades, es por ello, que existe una urgencia de poder investigar los sujetos, examinando los objetos, condiciones y medios utilizados para realizarlo y así aclarar su clasificación en el ordenamiento jurídico. Ante la afirmación de la falta de leyes adecuadas y jurisdicción aplicable para abordar los delitos que causan perjuicio tanto a la sociedad en general como al ciudadano común, no podemos pasar por alto el hecho de que estas actividades no discriminan ni perfil, estrato social o afiliación a una entidad específica, ya sea privada o gubernamental. Por lo tanto, todos estamos susceptibles a sufrir un nivel de afectación cada vez aún más grande en los intereses patrimoniales o más daño aun en el robo de datos informáticos (suplantación de identidad), es importante señalar que existen suficientes medios tecnológicos disponibles para indagar este tipo de delitos y, además, que es posible imponer sanciones a sus autores, detallando las modalidades que ellos mismos implementan o crean, para no dejar rastro en el espacio cibernético.

5.2. Validación de las variables

5.2.1. Validación de la variable independiente: Tipificación del phishing, smishing y vishing

Respecto a la posibilidad de incorporar la tipificación del phishing, smishing y vishing en base a la teoría de las necesidades se puede señalar que la tecnología informática se va convirtiendo en una herramienta para cometer delitos, la cual conlleva competencias y desafíos al momento de llevar a cabo una investigación. Así, mientras más avanza la tecnología en el ciberespacio, genera más dificultad y muy pocas posibilidades de configurar un delito cibernético, por lo que considero que para la comisión de este tipo de delitos no solamente basta una computadora si no el uso del internet es indispensable. No existe ciberdelito que se pueda cometer sin acceso a internet, P ero no todos los delitos cometidos mediante el uso del internet son ciberdelitos.

Por otro lado, es de mucha importancia actualizar o reclasificar los delitos informáticos o ciberdelito, ya que la tecnología en el ciberespacio avanza y se agrava cada vez más con cada categoría del delito informático, debido que existen alguno de ellos que están dentro del código penal y no dentro de la referida ley especial. Mientras ella no ocurra seguiremos denominando delitos informáticos o ciberdelitos a los 8 tipos penales ya considerados en la ley Nº 30096.

Conforme a lo desarrollado sobre el nivel de afectación de los ciberdelitos, donde no se identifican en el sistema legal los delitos de fraude, phishing, vishing y

smishing; Sin embargo, los casos especificados han ido aumentando hasta variando sus modalidades cada vez hay más capacidades, es por ello, que existe una urgencia de poder investigar los sujetos, examinando los objetos, condiciones y medios utilizados para realizarlo y así aclarar su clasificación en el ordenamiento jurídico. Ante la afirmación de la falta de leyes adecuadas y jurisdicción aplicable para abordar los delitos que causan perjuicio tanto a la sociedad en general como al ciudadano común, no podemos pasar por alto el hecho de que estas actividades no discriminan ni perfil, estrato social o afiliación a una entidad específica, ya sea privada o gubernamental.

Por lo tanto, todos estamos susceptibles a sufrir un nivel de afectación cada vez aún más grande en los intereses patrimoniales o más daño aun en el robo de datos informáticos (suplantación de identidad), es importante señalar que existen suficientes medios tecnológicos disponibles para indagar este tipo de delitos y, además, que es posible imponer sanciones a sus autores, detallando las modalidades que ellos mismos implementan o crean, para no dejar rastro en el espacio cibernético.

Es en base a estas determinaciones que la variable independiente se valida al indicar lo siguiente:

La ausencia de tipificación del phishing, smishing y vishing en la ley de delitos informáticos deja impunes estas acciones delictivas al no poder enmarcar en un ilícito y menos individualizar al agente delictivo.

5.2.2. Validación de la variable dependiente: El bien jurídico de seguridad informática

Según lo discutido sobre las justificaciones jurídicas para comprender el bien jurídico de seguridad informática como objeto de protección en el ámbito penal, se ha podido establecer que se trata de un concepto en desarrollo, lo cual se debe a la realidad de este espacio donde la actividad humana se encuentra en constante evolución, dadas las circunstancias de avance tecnológico y la presencia de actividades cada vez más innovadoras, por lo mismo que se verifica la necesidad de orientar la atención de la potestad punitiva del Estado a fin de controlar adecuadamente este tipo de riesgos. Sobre todo se pretende establecer un marco normativo que consolide la garantía que se debe plantear ante la posibilidad de vulneraciones en conjunto y que conceptualmente aún no se logran definir con exactitud, lo cual se debe al constante crecimiento de la diversidad de actividades en este espacio virtual, importante ello sin duda por la necesidad de los ciudadanos como sujetos de derecho para alcanzar un desarrollo idóneo con este tipo de actividades y en mérito a la garantía de sus derechos.

Es en base a estas determinaciones que la variable dependiente se valida al indicar lo siguiente:

El bien jurídico de seguridad informática requiere de un desarrollo normativo y descriptivo que involucre seguridad jurídica para la interacción en el ciberespacio.

5.3. Contrastación de la hipótesis

5.3.1. Determinación final

La ausencia de tipificación del phishing, smishing y vishing en la ley de delitos informáticos deja impunes estas acciones delictivas al no poder enmarcar en un ilícito y menos individualizar al agente delictivo, por ello es necesaria su incorporación a fin de dotar al bien jurídico de seguridad informática de un desarrollo normativo y descriptivo que involucre seguridad jurídica para la interacción en el ciberespacio.

Conclusiones

Conclusión general

Se concluye que la ausencia de tipificación del phishing, smishing y vishing en la ley de delitos informáticos deja impunes estas acciones delictivas al no poder enmarcar en un ilícito y menos individualizar al agente delictivo, por ello es necesaria su incorporación a fin de dotar al bien jurídico de seguridad informática de un desarrollo normativo y descriptivo que involucre seguridad jurídica para la interacción en el ciberespacio.

Conclusiones específicas

Primera:

Se concluye respecto a la posibilidad de incorporar la tipificación del phishing, smishing y vishing en base a la teoría de las necesidades, que se requiere de la revisión del avance tecnológico en el ciberespacio, para considerar este tipo de delitos. Por lo que es importante actualizar o reclasificar los delitos informáticos o ciberdelito, ya que la tecnología en el ciberespacio avanza y se agrava cada vez más, debido que existen alguno de ellos que están dentro del código penal y no dentro de la referida ley especial. Mientras ello no ocurra seguiremos denominando delitos informáticos o ciberdelitos a los 8 tipos penales ya considerados en la ley Nº 30096.

Segunda:

Se concluye según lo discutido sobre las justificaciones jurídicas para comprender el bien jurídico de seguridad informática como objeto de protección en el ámbito penal, que se trata de un concepto en desarrollo, lo cual se debe a la

realidad de este espacio donde la actividad humana se encuentra en constante evolución, dadas las circunstancias de avance tecnológico y la presencia de actividades cada vez más innovadoras, por lo mismo que se verifica la necesidad de orientar la atención de la potestad punitiva del Estado, para resguardar el interés de los ciudadanos como sujetos de derecho para alcanzar un desarrollo idóneo con este tipo de actividades y en mérito a la garantía de sus derechos.

Tercera:

Se concluye en base a observar el nivel de afectación de los ciberdelitos, donde no se identifican en el sistema legal los delitos de fraude, phishing, vishing y smishing, que la incidencia ha ido aumentando y hasta variando sus modalidades cada vez hay más capacidades, ello se debe a la falta de leyes adecuadas y jurisdicción aplicable teniendo en cuenta que estas actividades no discriminan ni perfil, estrato social o afiliación a una entidad específica, ya sea privada o gubernamental afectando los intereses patrimoniales a través del robo de datos informáticos (suplantación de identidad), es importante señalar que existen suficientes medios tecnológicos disponibles para indagar este tipo de delitos y, además, que es posible imponer sanciones a sus autores, detallando las modalidades que ellos mismos implementan o crean, para no dejar rastro en el espacio cibernético.

Recomendaciones

Primera:

Se recomienda mayor atención al tema de las acciones delictivas que se generan en el ciberespacio dada la naturaleza de este tipo de interacción que con el tiempo se ha instaurado y es posible que se convierta en un espacio de una acción totalitaria en el futuro; esto dependerá como función directa de la intervención del Estado a través de la configuración adecuada de las políticas públicas para el control del crimen, tiene que abrirse el espectro de percepción para generar prioridad en el análisis de la realidad delictiva.

Segunda:

Se debe sugerir que el resultado de los cambios en la política pública se trasladen a la normativa para incorporar la tipología que contemplan las acciones conceptualizadas como phishing, smishing y vishing en la ley de delitos informáticos para evitar la impunidad y fortalecer la garantía del bien jurídico de seguridad informática, involucrando con ello el carácter de seguridad jurídica para la interacción en el ciberespacio.

Bibliografía

Devia, E. (2017). *Delito informático: Estafa informática del artículo 248.2 del Código Penal.* Sevilla: Universidad de Sevilla. Obtenido de https://idus.us.es/bitstream/handle/11441/75625/Tesis%20Edmundo%20Devia%20Completa%20Final%2031%20Mayo%202017.pdf?sequence=1&isAllowed=y

Echeverry, Y., & Jaramillo, J. (2006). El concepto de justicia en John Rawls. *Revista Científica Guillermo de Ockham, IV*(2), 27-52. Obtenido de https://dialnet.unirioja.es/descarga/articulo/2877302.pdf

Esparta, M. (2022). *Mecanismos de prevención y protección del bien jurídico tutelado frente a la modalidad delictiva Phishing en el ordenamiento jurídico penal peruano.* Lima: Universidad Inca Garcilaso de la Vega. Obtenido de http://repositorio.uigv.edu.pe/bitstream/handle/20.500.11818/6595/TESIS_ESPARTA%20CENTENO.pdf?sequence=1

Espinoza, M. (2017). *Derecho Penal Informático: Deslegitimación del poder punitivo en la sociedad de control.* Puno: Universidad Nacional del Altiplano.

García Arroyo , C. (2022). Sobre el concepto de bien juridico. *Revista electrónica de Ciencia Penal y Criminologia*(24), 1-45. Obtenido de http://criminet.ugr.es/recpc/24/recpc24-12.pdf

Gómez, Á. (2006). *Enciclopedia de la Seguridad Informática* (2da ed.). España: Grupo Editorial RA-MA.

Herrera, R., & Núñez, A. (1999). *Derecho Informático.* Santiago: Jurídicas La Ley.

Hidalgo, C., & 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.* Chimbote: Universidad Nacional del Santa. Obtenido de http://repositorio.uns.edu.pe/bitstream/handle/UNS/3849/52376.pdf?sequence=1&isAllowed=y

Jijena, R. (1993). Debate parlamentario en el ámbito del Derecho Informático. Análisis de la Ley 19.223, de junio de 1993, que tipifica delitos en materia de sistemas de información. *Revista de Derecho*, 347-401.

Kierszenbaum, M. (2009). El bien jurídico en el derecho penal. Algunas nociones básicas desde la óptica de la discusión actual. *Lecciones y ensayos*(86), 187-211. Obtenido de http://www.derecho.uba.ar/publicaciones/lye/revistas/86/07-ensayo-kierszenbaum.pdf

Mayer, L., & Oliver, G. (2020). El delito de fraude informático: Concepto y delimitación. *Revista Chilena de Derecho y Tecnología, IX*(1), 151-184. doi:DOI 10.5354/0719-2584.2020.53447

Moscoso, R. (2014). La Ley 19.223 en general y el delito de hacking en particular. *Revista Chilena de Derecho y Tecnología, 3*, 11-78.

Revista Economía. (28 de Enero de 2022). *Ciberataques en el Perú incrementaron en un 15% durante el 2021*. Obtenido de Economía: https://www.revistaeconomia.com/ciberataques-en-el-peru-incrementaron-en-un-15-durante-el-2021/

Ribotta, S. (2008). Necesidades y Derechos: un debate no zanjado sobre fundamentación de derechos. *Jurid. Manizales (Colombia), V*(1), 29-56. Obtenido de https://dialnet.unirioja.es/descarga/articulo/2943462.pdf

Sosa, O. (2022). *Phishing como modalidad de delitos informáticos: a propósito de la suplantación y robo a los beneficiarios del bono universal en el Perú.* Piura: Universidad Nacional de Piura. Obtenido de https://repositorio.unp.edu.pe/bitstream/handle/20.500.12676/3559/DECP-SOS-UMB-2022.pdf?sequence=1&isAllowed=y

Ventura, M., & Roque, G. (2021). *La tipificación del Phishing, Smishing y Vishing en nuestro sistema penal peruano, para la lucha contra la ciberdelincuencia en Lima, 2020.* Lima: Universidad Privada del Norte. Obtenido de https://repositorio.upn.edu.pe/bitstream/handle/11537/28942/Ventura%20Quijano%2c%20Mishell%20Alisson.pdf?sequence=11&isAllowed=y

Villavicencio, F. (2014). Delitos Informáticos. *IUS ET VERITAS*(49).

Zeballos, Ó. (2020). Delitos informáticos: ¿Cuáles son los principales fraudes informáticos que se pueden cometer a través del E-Commerce? *ius360*.

Anexos

1. Data estadística proporcionada por el Ministerio

MINISTERIO PÚBLICO
REPUBLICA DEL PERU

CARGA FISCAL INGRESADA DE LAS FISCALIAS PROVINCIALES Y SUPERIORES
POR DELITOS INFORMÁTICOS
DISTRITO FISCAL DE LIMA CENTRO

OFICINA DE CONTROL DE LA
PRODUCTIVIDAD FISCAL

PERIODOS: ENE-DIC 2022 Y ENE-AGO 2023

ANEXO 01

DISTRITO FISCAL	INSTANCIA	DELITO GENÉRICO	DELITO SUB GENÉRICO	DELITO ESPECÍFICO	ENE-DIC 2022	ENE-AGO 2023	TOTAL
LIMA CENTRO	PROVINCIAL	LEY N° 30096, LEY DE DELITOS INFORMATICOS	DELITOS CONTRA DATOS Y SISTEMAS INFORMATICOS	ACCESO ILICITO (ACCEDER A UN SISTEMA INFORMATICO, EXCEDIENDO LO AUTORIZADO)	140	294	434
				ACCESO ILICITO (ACCEDER SIN AUTORIZACION A SISTEMA INFORMATICO, CON VULNERACION DE MEDIDAS DE SEG...	111	138	249
				ACCESO ILÍCITO (EL QUE DELIBERADAMENTE E ILEGITIMAMENTE ACCEDE A TODO O PARTE DE UN SISTEMA INFORM..	120	90	210
				ATENTADO CONTRA LA INTEGRIDAD DE DATOS INFORMÁTICOS (EL QUE DELIBERADA E ILEGITIMAMENTE DAÑA, INT...	91	113	204
				ATENTADO CONTRA LA INTEGRIDAD DE DATOS INFORMATICOS (INTRODUCIR, BORRAR, DETERIORAR, ALTERAR, SUP...	2	1	3
				ATENTADO CONTRA LA INTEGRIDAD DE SISTEMAS INFORMATICOS (INUTILIZAR UN SISTEMA INFORMATICO, IMPIDI...	34	31	65
				NO TIPIFICADO	16	24	40
			Total DELITOS CONTRA DATOS Y SISTEMAS INFORMATICOS		514	691	1,205
			DELITOS INFORMATICOS CONTRA EL PATRIMONIO	FRAUDE INFORMATICO	6,813	9,707	16,520
				FRAUDE INFORMATICO (AFECTACION DEL PATRIMONIO DEL ESTADO DESTINADO A FINES ASISTENCIALES O PROGRA...	77	69	146
				FRAUDE INFORMÁTICO (EL QUE DELIBERADA E ILEGITIMAENTE PROCURA PARA SI O PARA OTRO UN PROVECHO ILIC..	458	560	1,018
				NO TIPIFICADO	21	42	63
			Total DELITOS INFORMATICOS CONTRA EL PATRIMONIO		7,369	10,378	17,747
			DELITOS INFORMATICOS CONTRA LA FE PUBLICA	NO TIPIFICADO	4	7	11
				SUPLANTACION DE IDENTIDAD	1,933	2,004	3,937
			Total DELITOS INFORMATICOS CONTRA LA FE PUBLICA		1,937	2,011	3,948
			DELITOS INFORMATICOS CONTRA LA INDEMNIDAD Y LIBERTAD SEXUALES	EL QUE A TRAVES DE INTERNET U OTRO MEDIO ANALOGO CONTACTA CON UN MENOR DE 14 AÑOS PARA SOLICITAR...	5	11	16

DISTRITO FISCAL	INSTANCIA	DELITO GENÉRICO	DELITO SUB GENÉRICO	DELITO ESPECÍFICO	ENE-DIC 2022	ENE-AGO 2023	TOTAL
LIMA CENTRO	PROVINCIAL	LEY N° 30096, LEY DE DELITOS INFORMATICOS	DELITOS INFORMATICOS CONTRA LA INDEMNIDAD Y LIBERTAD SEXUALES	PROPOS A NIÑOS, NIÑAS Y ADOL. CON FIN SEXUAL (ENTRE 14 Y 18 AÑOS) POR MEDIOS TECNOLOGICOS	33	40	73
				PROPOS A NIÑOS, NIÑAS Y ADOL. CON FIN SEXUAL (MENOR DE 14 AÑOS) POR MEDIOS TECNOLOGICOS	46	51	97
			Total DELITOS INFORMATICOS CONTRA LA INDEMNIDAD Y LIBERTAD SEXUALES		84	102	186
			DELITOS INFORMATICOS CONTRA LA INTIMIDAD Y EL SECRETO DE LAS COMUNICACIONES	INTERCEPTACION DE DATOS INFORMATICOS	171	62	233
				INTERCEPTACION DE DATOS INFORMATICOS (DELITO COMPROMETE DEFENSA, SEGURIDAD O SOBERANIA NACIONAL)	1	1	2
				INTERCEPTACION DE DATOS INFORMATICOS (INFORMACION CLASIFICADA COMO SECRETA, RESERVADA O CONFIDENC...	5	2	7
				NO TIPIFICADO	1		1
				TRAFICO ILEGAL DE DATOS PARA COMERCIALIZAR, TRAFICAR, VENDER, PROMOVER, FAVORECER O FACILITAR INF...	11	12	23
			Total DELITOS INFORMATICOS CONTRA LA INTIMIDAD Y EL SECRETO DE LAS COMUNICACIONES		189	77	266
			DISPOSICIONES COMUNES	ABUSO DE MECANISMOS Y DISPOSITIVOS INFORMATICOS	47	105	152
				ABUSO DE MECANISMOS Y DISPOSITIVOS INFORMÁTICOS (EL QUE DELIBERADA E ILEGITIMAMENTE FABRICA, DISEÑ...	4	9	13
				FORMA AGRAVADA (ABUSO DE POSICION ESPECIAL DE ACCESO A LA DATA O INFORMACION RESERVADA O AL CONOC...	2		2
				FORMA AGRAVADA (AGENTE COMETE EL DELITO CON EL FIN DE OBTENER BENEFICIO ECONOMICO)	5	9	14
				FORMA AGRAVADA (DELITO COMPROMETE FINES ASISTENCIALES, LA DEFENSA, LA SEGURIDAD Y LA SOBERANIA NA...		1	1
				FORMA AGRAVADA (INTEGRANTE DE ORGANIZACION CRIMINAL)	3	1	4
				NO TIPIFICADO		5	5
			Total DISPOSICIONES COMUNES		61	130	191
			NO TIPIFICADO	NO TIPIFICADO	822	1,028	1,850
			Total NO TIPIFICADO		822	1,028	1,850
		Total LEY N° 30096, LEY DE DELITOS INFORMATICOS			10,976	14,417	25,393
	Total PROVINCIAL				10,976	14,417	25,393
	SUPERIOR	LEY N° 30096, LEY DE DELITOS INFORMATICOS	DELITOS CONTRA DATOS Y SISTEMAS INFORMATICOS	ACCESO ILICITO (ACCEDER A UN SISTEMA INFORMATICO, EXCEDIENDO LO AUTORIZADO)	10	21	31

DISTRITO FISCAL	INSTANCIA	DELITO GENÉRICO	DELITO SUB GENÉRICO	DELITO ESPECÍFICO	ENE-DIC 2022	ENE-AGO 2023	TOTAL
LIMA CENTRO	SUPERIOR	LEY N° 30096, LEY DE DELITOS INFORMATICOS	DELITOS CONTRA DATOS Y SISTEMAS INFORMATICOS	ACCESO ILICITO (ACCEDER SIN AUTORIZACION A SISTEMA INFORMATICO, CON VULNERACION DE MEDIDAS DE SEG...	4	4	8
				ACCESO ILÍCITO (EL QUE DELIBERADAMENTE E ILEGITIMAMENTE ACCEDE A TODO O PARTE DE UN SISTEMA INFORM..	9	8	17
				ATENTADO CONTRA LA INTEGRIDAD DE DATOS INFORMÁTICOS (EL QUE DELIBERADA E ILEGITIMAMENTE DAÑA, INT...	5	9	14
				ATENTADO CONTRA LA INTEGRIDAD DE DATOS INFORMATICOS (INTRODUCIR, BORRAR, DETERIORAR, ALTERAR, SUP...	2	1	3
				ATENTADO CONTRA LA INTEGRIDAD DE SISTEMAS INFORMATICOS (INUTILIZAR UN SISTEMA INFORMATICO, IMPIDI...	4	2	6
				NO TIPIFICADO	2	4	6
			Total DELITOS CONTRA DATOS Y SISTEMAS INFORMATICOS		36	49	85
			DELITOS INFORMATICOS CONTRA EL PATRIMONIO	FRAUDE INFORMATICO	189	182	371
				FRAUDE INFORMATICO (AFECTACION DEL PATRIMONIO DEL ESTADO DESTINADO A FINES ASISTENCIALES O PROGRA...	5	12	17
				FRAUDE INFORMÁTICO (EL QUE DELIBERADA E ILEGITIMAENTE PROCURA PARA SI O PARA OTRO UN PROVECHO ILIC...	23	20	43
				NO TIPIFICADO		1	1
			Total DELITOS INFORMATICOS CONTRA EL PATRIMONIO		217	215	432
			DELITOS INFORMATICOS CONTRA LA FE PUBLICA	SUPLANTACION DE IDENTIDAD	110	113	223
			Total DELITOS INFORMATICOS CONTRA LA FE PUBLICA		110	113	223
			DELITOS INFORMATICOS CONTRA LA INDEMNIDAD Y LIBERTAD SEXUALES	EL QUE A TRAVES DE INTERNET U OTRO MEDIO ANALOGO CONTACTA CON UN MENOR DE 14 AÑOS PARA SOLICITAR...		1	1
				PROPOS A NIÑOS, NIÑAS Y ADOL. CON FIN SEXUAL (ENTRE 14 Y 18 AÑOS) POR MEDIOS TECNOLOGICOS		2	2
				PROPOS A NIÑOS, NIÑAS Y ADOL. CON FIN SEXUAL (MENOR DE 14 AÑOS) POR MEDIOS TECNOLOGICOS		1	1
			Total DELITOS INFORMATICOS CONTRA LA INDEMNIDAD Y LIBERTAD SEXUALES			4	4
			DELITOS INFORMATICOS CONTRA LA INTIMIDAD Y EL SECRETO DE LAS COMUNICACIONES	INTERCEPTACION DE DATOS INFORMATICOS	11	4	15

DISTRITO FISCAL	INSTANCIA	DELITO GENÉRICO	DELITO SUB GENÉRICO	DELITO ESPECÍFICO	ENE-DIC 2022	ENE-AGO 2023	TOTAL
LIMA CENTRO	SUPERIOR	LEY N° 30096, LEY DE DELITOS INFORMATICOS	DELITOS INFORMATICOS CONTRA LA INTIMIDAD Y EL SECRETO DE LAS COMUNICACIONES	TRAFICO ILEGAL DE DATOS PARA COMERCIALIZAR, TRAFICAR, VENDER, PROMOVER, FAVORECER O FACILITAR INF...	1		1
			Total DELITOS INFORMATICOS CONTRA LA INTIMIDAD Y EL SECRETO DE LAS COMUNICACIONES		12	4	16
			DISPOSICIONES COMUNES	ABUSO DE MECANISMOS Y DISPOSITIVOS INFORMATICOS	11	10	21
			Total DISPOSICIONES COMUNES		11	10	21
			NO TIPIFICADO	NO TIPIFICADO	79	19	98
			Total NO TIPIFICADO		79	19	98
		Total LEY N° 30096, LEY DE DELITOS INFORMATICOS			465	414	879
	Total SUPERIOR				465	414	879
Total LIMA CENTRO					11,441	14,831	26,272

NOTA:

- No se consideran los casos anulados.

Fuente de Información: La Bandeja Fiscal

Elaborado por la Oficina de Control de la Productividad Fiscal (OCPF)