UNIVERSIDAD NACIONAL DE BARRANCA

Facultad de Ciencias Jurídicas, Contables Financieras y Administrativas

Escuela Profesional de Derecho y Ciencia Política

TESIS

Determinación regulativa del phishing como modalidad del fraude informático para protección de datos en el Distrito de Barranca, 2022-2023

PARA OPTAR EL TÍTULO PROFESIONAL DE:

Abogado

PRESENTADO POR:

Gonzales Muñoa Sofía Leonor

Delgado Zavaleta Henry Pablo

BARRANCA-PERÚ

2025

CONTRA CARATULA

.....

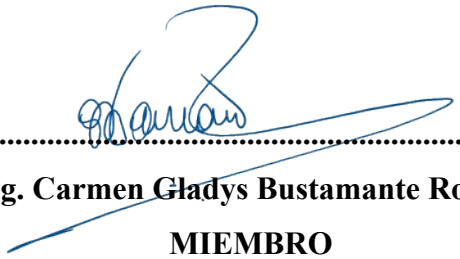
Dra. Yorrlanka Evelin Damián Espinoza

PRESIDENTE

.....

Dr. Oswaldo Pablo Lara Rivera

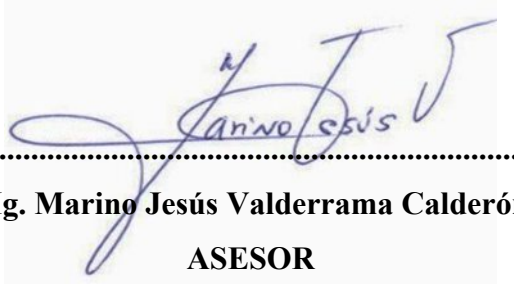
MIEMBRO



.....

Mg. Carmen Gladys Bustamante Rosales

MIEMBRO



.....

Mg. Marino Jesús Valderrama Calderón

ASESOR

REPORTE DE TURNITIN

Tesis_Gonzales Muñoa y Delgado Zavaleta.docx

INFORME DE ORIGINALIDAD

17%	16%	4%	7%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	repositorio.unab.edu.pe Fuente de Internet	3%
2	hdl.handle.net Fuente de Internet	1%
3	www.defensoria.gob.pe Fuente de Internet	1%
4	www.coursehero.com Fuente de Internet	1%
5	www.informatica-juridica.com Fuente de Internet	1%
6	Submitted to Corporación Universitaria Minuto de Dios, UNIMINUTO Trabajo del estudiante	1%
7	Submitted to Instituto Superior de Artes, Ciencias y Comunicación IACC Trabajo del estudiante	<1%
8	Submitted to Corporación Universitaria Minuto de Dios,UNIMINUTO Trabajo del estudiante	<1%
9	view.genial.ly Fuente de Internet	<1%
10	Submitted to Universidad Tecnologica del Peru Trabajo del estudiante	<1%
11	Submitted to Universidad Internacional de la Rioja Trabajo del estudiante	<1%
12	repositorio.unsch.edu.pe Fuente de Internet	<1%
13	repositorio.ucv.edu.pe Fuente de Internet	<1%

ACTA DE SUSTENTACIÓN DE TESIS

UNIVERSIDAD NACIONAL DE BARRANCA

FACULTAD DE CIENCIAS JURÍDICAS, CONTABLES FINANCIERAS Y ADMINISTRATIVAS
ESCUELA PROFESIONAL DE DERECHO Y CIENCIA POLÍTICA

JURADO EVALUADOR PARA LA SUSTENTACIÓN DE TESIS - R.C.O. Nº 553-2025-UNAB

Barranca, 17 de junio de 2025

ACTA DE SUSTENTACIÓN DE TESIS

Los integrantes del Jurado Evaluador:

Presidenta :	Dra. Yorlanka Evelin Damián Espinoza
Miembro :	Dr. Oswaldo Pablo Lara Rivera
Miembro :	Mg. Carmen Gladys Bustamante Rosales
Asesor :	Mg. Marino Jesús Valderrama Calderón

Se reúnen para evaluar la sustentación de tesis titulada: Determinación regulativa del phishing como modalidad del fraude informático para protección de datos en el Distrito de Barranca, 2022-2023.

Presentada por los graduados:

- GONZALES MUÑOA, SOFIA LEONOR
- DELGADO ZAVALETA, HENRY PABLO

Para optar el Título Profesional de ABOGADO

Luego de haber evaluado la sustentación de la tesis, concluye de manera unánime (X) por mayoría simple ( ) calificar a:

Apellidos y Nombres:			Nota:	
- GONZALES MUÑOA, SOFIA LEONOR - DELGADO ZAVALETA, HENRY PABLO			15	
Sobresaliente ( )	Muy bueno ( )	Bueno (X)	Regular ( )	Desaprobado ( )

Los miembros del Jurado Evaluador firman en señal de conformidad.

Dra. Yorlanka Evelin Damián Espinoza
Presidenta

Dr. Oswaldo Pablo Lara Rivera
Miembro

Mg. Carmen Gladys Bustamante Rosales
Miembro

Mg. Marino Jesús Valderrama Calderón
Asesor

DEDICATORIAS

Dedicamos esta tesis a nuestras familias, quienes han sido nuestro pilar emocional y la mayor fuente de motivación a lo largo de este desafiante proceso académico. Su apoyo incondicional, confianza y valores nos han guiado y fortalecido en cada paso hacia la culminación de este trabajo.

Asimismo, dedicamos este esfuerzo a todas las personas que, con dedicación y compromiso, trabajan por combatir los delitos informáticos. Con la esperanza de contribuir a la regulación del phishing y a la protección efectiva de los datos personales en el Distrito de Barranca y más allá. Finalmente, deseamos que esta investigación inspire un cambio positivo y significativo en la sociedad.

Sofía y Henry

AGRADECIMIENTOS

A nuestras familias, nuestro mayor pilar, les agradecemos profundamente por su amor incondicional, paciencia y confianza inquebrantable. Sus enseñanzas y palabras de aliento han sido nuestra fuente de inspiración y motivación en los momentos más desafiantes.

Expresamos nuestro agradecimiento a nuestro asesor, cuya orientación y compromiso fueron clave para el desarrollo de esta investigación. Su apoyo no solo fortaleció este trabajo, sino que también contribuyó de manera significativa a nuestro crecimiento académico y personal.

Los autores

DECLARATORIA DE AUTENTICIDAD

Por el presente documento, **Gonzales Muñoa Sofía Leonor**, identificada con DNI N° 70916441, egresada de la carrera de Derecho y Ciencia Política, informo que elaboré la Tesis denominada: **Determinación regulativa del phishing como modalidad del fraude informático para protección de datos en el Distrito de Barranca, 2022-2023**, para optar el título profesional de Abogado, declaro que toda la información presentada en la presente tesis es auténtica y veraz.

Por lo cual firmo la presente, en señal de veracidad, caso contrario me someteré a las sanciones de ley que dictamine la Universidad Nacional de Barranca.

Barranca, 31 de enero del 2025

……
Gonzales Muñoa Sofía Leonor
DNI: 70916441

DECLARATORIA DE AUTENTICIDAD

Por el presente documento, **Delgado Zavaleta Henry Pablo**, identificado con DNI N° 72200186, egresado de la carrera de Derecho y Ciencia Política, informo que elaboré la Tesis denominada: **Determinación regulativa del phishing como modalidad del fraude informático para protección de datos en el Distrito de Barranca, 2022-2023**, para optar el título profesional de Abogado, declaro que toda la información presentada en la presente tesis es auténtica y veraz.

Por lo cual firmo la presente, en señal de veracidad, caso contrario me someteré a las sanciones de ley que dictamine la Universidad Nacional de Barranca.

Barranca, 31 de enero del 2025

…...……
Delgado Zavaleta Henry Pablo
DNI: 72200186

ÍNDICE

pág.

INDICE DE CUADROS

Pág.

INDICE DE GRAFICOS

Pág.

II. INFORMACIÓN GENERAL

2.1. Título del proyecto

Determinación regulativa del phishing como modalidad del fraude informático para protección de datos en el Distrito de Barranca, 2022-2023

2.2. Autores

Gonzales Muñoa, Sofía Leonor
Delgado Zavaleta, Henry Pablo

2.3. Asesor

Mg. Marino Jesús Valderrama Calderón.

2.4. Tipo de investigación

Por su alcance descriptivo

2.5. Programa y línea de investigación vigente

Programa: Área de ciencias sociales
Línea de investigación: Derecho público

2.6. Duración del proyecto

Fecha de inicio: Agosto de 2024.
Fecha de término: Enero de 2025.

2.7. Localización del proyecto

Distrito de Barranca de Lima Provincias

III. RESUMEN DEL PROYECTO

En presente estudio desarrolló un análisis sobre la determinación regulativa del phishing como modalidad del fraude informático para la protección de datos en el Distrito de Barranca, durante el período 2022-2023. Se consideraron aspectos esenciales para garantizar una protección efectiva de los datos personales y una respuesta adecuada a las amenazas cibernéticas en el ámbito distrital. Asimismo, se destacó la necesidad de implementar medidas de seguridad adicionales en plataformas en línea, fomentar la colaboración en la investigación policial y promover el intercambio de información sobre amenazas cibernéticas. El objetivo general consistió en analizar la determinación de la regulación del phishing como modalidad del fraude informático en la protección de datos personales en el Distrito de Barranca. La hipótesis general planteó que la determinación de la regulación del phishing como modalidad de fraude informático protegió los datos personales en dicho distrito durante el período estudiado. La metodología se basó en una investigación de finalidad básica, con un alcance descriptivo y un enfoque cualitativo, utilizando un diseño no experimental y transversal. La muestra estuvo conformada por documentos provenientes de revistas, libros, encuestas del INEI e informes de la Policía Nacional del Perú. Se empleó la técnica de análisis documental y como instrumento, la guía de análisis de documentos. Los resultados permitieron determinar que una regulación eficaz del phishing contribuyó a la seguridad de los datos personales y a la prevención de amenazas cibernéticas. Finalmente, el impacto del estudio radicó en el reconocimiento del phishing como un delito, lo que facilitó la aplicación de la ley y permitió a las autoridades y organismos competentes adoptar medidas sancionatorias para combatirlo.

Palabras Clave: Phishing; fraude informático; protección de datos

ABSTRACT

In this study, an analysis was developed on the regulatory determination of phishing as a modality of computer fraud for data protection in the District of Barranca, during the period 2022-2023. Essential aspects were considered to guarantee effective protection of personal data and an adequate response to cyber threats at the district level. Likewise, the need to implement additional security measures on online platforms, encourage collaboration in police investigation and promote the exchange of information on cyber threats was highlighted. The general objective was to analyze the determination of the regulation of phishing as a modality of computer fraud in the protection of personal data in the District of Barranca. The general hypothesis stated that the determination of the regulation of phishing as a form of computer fraud protected personal data in said district during the period studied. The methodology was based on a research of basic purpose, with a descriptive scope and a qualitative approach, using a non-experimental and transversal design. The sample was made up of documents from magazines, books, INEI surveys and reports from the National Police of Peru. The documentary analysis technique was used and as an instrument, the document analysis guide. The results determined that effective phishing regulation contributed to the security of personal data and the prevention of cyber threats. Finally, the impact of the study was in the recognition of phishing as a crime, which facilitated the application of the law and allowed the competent authorities and organizations to adopt sanctioning measures to combat it.

Keywords: Phishing; computer fraud; data protection

IV. PLANTEAMIENTO DEL PROYECTO

4.1. Situación del problema

La investigación se circunscribió en la determinación regulativa del phishing como modalidad del fraude informático para protección de datos en el Distrito de Barranca, 2022-2023, ya que el phishing fue identificado como una técnica basada en el envío de correos electrónicos, los cuales reemplazaban o suplantaban la identidad de los usuarios, solicitando en muchos casos información personal. Esta acción resultó ser una actividad criminal que infringía la ley, aprovechándose de que aún no se encontraba regulada en la Ley de Delitos Informáticos (Ley N°30096), lo cual generaba malestar en las personas víctimas de la inseguridad informática. El término phishing, proveniente de la palabra en inglés "fishing" (pesca), hacía alusión al acto de "pescar" usuarios mediante anzuelos (trampas) cada vez más complejos para obtener contraseñas e información financiera de los usuarios (Esparta, 2022).

Por otro lado, el phishing constituyó un problema relacionado con el fraude informático al vulnerar los datos personales de los usuarios, quienes se encontraban desprotegidos frente a la sustracción de sus datos personales, contraseñas y redes sociales. Estos eran afectados a través de la modalidad del phishing, mediante la cual los ciberdelincuentes accedían con engaño a enlaces de páginas web, generando perjuicios económicos, sociales y jurídicos. En otras palabras, con este fraude quedaron desprotegidos los datos personales de los usuarios.

Las investigaciones previas señalaron que el phishing había tomado mayor relevancia con el pasar del tiempo, desarrollándose y perfeccionándose constantemente. Esta modalidad del fraude informático presentó nuevas variantes, y las páginas fraudulentas adquirieron una mayor similitud con las páginas web legales, llegando incluso a solicitar cambios de contraseñas, números de tarjetas de crédito o información de cuentas bancarias, haciéndose pasar por entidades de confianza, lo que llevó a los usuarios a caer en el ardid de los ciberdelincuentes.

Por otro lado, dichas investigaciones afirmaron que esta modalidad era una de las más utilizadas y afectaba significativamente la seguridad informática, generando cuantiosos daños relacionados con los datos confidenciales de los usuarios. Aunque también indicaron que era relativamente fácil de detectar, los estafadores habían mejorado sus tácticas, creando correos electrónicos y sitios web que parecían auténticos. Además, no se limitaron solo al correo electrónico, sino que también utilizaron mensajes de texto, llamadas telefónicas, mensajes instantáneos e incluso redes sociales para llevar a cabo sus ataques.

En cuanto a la brecha, el phishing se refirió al espacio entre el conocimiento de una persona sobre el phishing y su capacidad para identificar y evitar con éxito los intentos de este fraude. Sin embargo, se destacó que, aunque muchas personas habían oído hablar del phishing, no todas comprendían completamente cómo funcionaba o cómo identificarlo. Esta falta de comprensión dejó a muchas personas vulnerables a los ataques de phishing. Incluso las personas con un buen conocimiento sobre el tema podían ser engañadas debido a factores humanos como distracción, urgencia o falta de atención. Los estafadores aprovecharon estas vulnerabilidades para aumentar las posibilidades de éxito de sus ataques. Por tanto, reducir la brecha del phishing requirió un esfuerzo conjunto de los usuarios, las organizaciones y los proveedores de servicios en línea para mantenerse informados, vigilantes y proactivos en la protección contra los ataques de phishing.

Por último, se consideró que la brecha podría ser cubierta mediante esta investigación, para evitar consecuencias mayores del phishing que iban más allá del robo de información financiera, enfrentando problemas como el robo de identidad, pérdida de fondos, acceso no autorizado a cuentas en línea e incluso acoso cibernético. Por tanto, cubrir la brecha del phishing requirió un enfoque integral que combinara educación, tecnología y políticas de seguridad sólidas. Al capacitar a las personas y fortalecer las defensas tecnológicas, las organizaciones lograron reducir significativamente el riesgo de caer en trampas de phishing. Finalmente, se propuso un anteproyecto de ley para regular el phishing como delito de fraude informático, tal como Colombia lo reguló mediante la Ley N° 1273.

4.2. Formulación del proyecto

Problema general

¿Para qué determinar la regulación del phishing como modalidad del fraude informático en la protección de datos en el Distrito de Barranca, 2022-2023?

Problemas específicos

Pe.1. ¿Cómo, determinar la regulación del phishing en la modalidad de fraude informático en el Distrito de Barranca, 2022-2023?

Pe.2. ¿Qué regular en el phishing para la protección de datos personales en el Distrito de Barranca, 2022-2023?

V. JUSTIFICACIÓN

El proyecto se justificó en tres esferas: teórica, práctica y social, como se desarrolló a continuación:

La investigación se justificó de forma teórica, ya que el Perú no había establecido regulaciones específicas centradas únicamente en el phishing. Sin embargo, el país contaba con leyes y regulaciones relacionadas con la protección de datos personales, delitos informáticos y seguridad cibernética que podían abordar aspectos del phishing. La Ley N.º 29733, Ley de Protección de Datos Personales, estableció disposiciones para proteger la privacidad de los datos personales y definió las responsabilidades de las entidades que procesaban esta información. Aunque Perú no había promulgado regulaciones específicas sobre el phishing, las leyes existentes no sancionaban expresamente esta práctica. Por tanto, fue importante que las autoridades peruanas estuvieran al tanto de las amenazas cibernéticas, incluido el phishing, y tomar medidas para proteger a los ciudadanos mediante el anteproyecto de una ley que tipificará la conducta del agente y la sancionará con pena privativa de la libertad.

Desde una perspectiva práctica, promovió una cultura de seguridad. Al educar a las personas sobre los riesgos del phishing y cómo prevenirlo, se fomentó una cultura de seguridad cibernética en la que todos eran conscientes de las amenazas en línea y tomaban medidas proactivas para protegerse a sí mismos y a otros. Vale decir, prevenir el phishing no solo ayudó a proteger los datos y las finanzas, sino que también contribuyó a mantener la reputación, garantizar la continuidad del negocio, cumplir con las regulaciones y promover una cultura de seguridad cibernética entre los ciudadanos, las empresas y la sociedad en general. En tanto que, las sanciones y medidas de cumplimiento de las regulaciones de seguridad cibernética y protección de datos disuadieron la participación en prácticas de phishing y otras actividades delictivas en línea.

Asimismo, se justificó desde el ámbito social, como fuente de ingresos económicos. Aunque no ética ni legalmente justificable, algunos individuos o grupos percibieron el phishing como una oportunidad para obtener ganancias rápidas o información

confidencial de manera relativamente sencilla. En otros términos, como un potencial de ganancias de los estafadores que vieron el phishing como una forma de trabajo y fuente de riqueza, ya sea vendiendo la información robada en el mercado negro, realizando transacciones financieras fraudulentas o extorsionando a las víctimas. Sin embargo, fue importante tener en cuenta que, aunque el phishing pudiera ofrecer beneficios aparentes en términos de ganancias financieras rápidas o acceso a información confidencial, estas acciones fueron ilegales y éticamente condenables. El phishing no solo causó daños a las víctimas individuales, sino que también socavó la confianza en la seguridad en línea y tuvo consecuencias legales graves para los perpetradores. En última instancia, la práctica del phishing resultó destructiva y perjudicial tanto para las víctimas como para la sociedad en su conjunto.

VI. ANTECEDENTES Y ESTADO DEL ARTE

6.1. Antecedentes Internacionales

Vázquez, Hernández, Cesar, & Núñez (2023) investigaron mediante su artículo intitulado el crecimiento del phishing. Su metodología fue de análisis de documentos, con su técnica de la encuesta y su instrumento del cuestionario en línea. Concluyeron que el "Phishing", ataca a la sociedad y que se mantienen con su afectación, su incremento no es exponencial ni alarmante, pero está controlado porque los ciudadanos tienen conocimiento de las estafas virtuales, por último, la desinformación es la causa principal que genera víctimas individuales y masivas.

Castillo (2021) en su tesis de maestría investigó sobre "Phishing: Día de pesca". Su metodología fue desarrollada dentro de los parámetros de la monografía, con su técnica de análisis documental, con su instrumento de la guía de documentos relacionados con el objeto de estudio. En sus conclusiones hace la diferencia entre cibercrimen y delitos informáticos. El primero es aquellas que no atentan contra un bien jurídico concreto, inclusive se trata de conductas no penalizadas, mientras el segundo encuentra respuesta en las normas sustanciales penales, es decir, se han incorporado al código penal como delitos que afectan bienes jurídicamente tutelados, también concluye que el ciberespacio es un ámbito de oportunidad criminal que demanda políticas públicas para tutelar a los ciudadanos, tanto de sus bienes y persona.

Hernández & Baluja (2021) investigaron en su artículo sobre el phishing, para ello usaron la metodología de análisis de casos, y de los métodos aplicados desde lo más convencional hasta lo más sofisticado como automatizados para su detección del ataque cibernético. Concluyeron que la educación de los usuarios en la especialidad de la informática y la computación influye positivamente para disminuir los ataques, pero se requiere su constancia porque el phishing evoluciona en gran magnitud y educar a los ciudadanos es costoso, más aún la prevención es altamente costoso que los presupuestos nacionales no alcanzan.

6.2. Antecedentes Nacionales

Ruiz & Solis (2024) investigaron en su artículo denominado fraude con phishig. Su metodología fue de enfoque cualitativo, de nivel básico, inductivo, su muestra fueron el personal policial a los cuales les entrevistaron. Sus conclusiones consisten en que ejecutan el ataque mediante correos personales e institucionales, suplantaciones de páginas web en su mayoría de las que se dedican a créditos y servicios de banca para cometer el ilícito de fraude informático, apoderándose del patrimonio de los clientes y es la causa principal que vulnera los datos del usuario y contraseñas de los timados electrónicamente.

Díaz y Goitia (2024), en su investigación titulada El delito de phishing en las entidades financieras del Perú*,* emplearon una metodología hipotético-deductiva no experimental, enfocado cualitativamente para analizar el phishing en el sector financiero peruano. Su estudio destacó que el phishing generalmente implica la clonación de sitios web para engañar a los usuarios y obtener información sensible, como datos personales y financieros. Las autoras enfatizaron la urgencia de implementar programas de compliance en las instituciones financieras como una herramienta preventiva. Concluyeron que los marcos de compliance pueden mitigar eficazmente los riesgos del phishing al promover la concienciación organizacional y proteger los datos de los usuarios, mejorando así la seguridad jurídica y reduciendo las pérdidas económicas.

Carrero (2024), en su tesis titulada *Incorporación de la modalidad del Phishing en la Ley de Delitos Informáticos*, analiza la creciente incidencia del phishing como modalidad delictiva y su ausencia en la legislación peruana. Para ello, utilizó una metodología analítica y documental, basada en legislación nacional e internacional, así como datos estadísticos sobre delitos informáticos. Entre sus conclusiones, resalta la urgente necesidad de incluir el phishing en el artículo 8 de la Ley N.º 30096, ya que este delito afecta principalmente el patrimonio de las víctimas mediante el uso de medios tecnológicos, como correos electrónicos fraudulentos y la suplantación de páginas web, lo que facilita el robo de datos personales y financieros.

Nazario y Villanueva (2022), en su tesis titulada Fraude informático en la modalidad de phishing y la necesaria actualización de la legislación para una eficiente persecución y sanción penal, desarrollaron una metodología mixta con enfoque cuantitativo y cualitativo. La investigación tuvo como población a operadores del Derecho, como abogados especialistas en Derecho Penal, jueces y fiscales de la ciudad de Chiclayo. Concluyeron que la actualización de la legislación peruana contribuyó a una persecución y sanción penal más eficiente del delito de phishing. Además, señalaron que la falta de normativas específicas generaba impunidad en estos casos, afectando a la sociedad y dejando vacíos legales que facilitaban la acción de los ciberdelincuentes.

Esparta (2022) en su trabajo de investigación sobre el phishing en la sociedad peruana, para optar el título profesional de Abogado. En su metodología uso la entrevista y análisis de casos de enfoque cuantitativo, llegó a la conclusión siguiente: Que el phishing es un tipo de fraude informático, con el propósito de extraer datos del usuario, a través de páginas clonadas que tienden a causar una apariencia real de las verdaderas páginas, con lo cual induce al error de los usuarios cayendo en su trampa, lo cual se realiza a través de la emisión de correos electrónicos, que contienen mensajes maliciosos; señalando a demás en su conclusión número 3, que, en los países de Colombia y México, ya cuentan con una legislación adecuada, que tipifica el delito de phishing de manera específica, lo cual conlleva que la persecución de esta modalidad es más eficaz.

Hidalgo y Solano (2021) en su trabajo de investigación titulado: “El phishing como conducta delictiva no regulada en el ordenamiento jurídico peruano. En su metodología plantearon como objetivo general describir el phishing para su regulación como conducta delictiva, en su enfoque cualitativo y tipo de investigación básica. Concluyeron que el avance tecnológico en el mundo es disruptivo, e indispensable la presencia de los medios tecnológicos en la vida cotidiana en actividades, como laborales, educacionales, comerciales y ocio; también lleva a nuevas formas delictivas a través de los medios informáticos o sean perfeccionadas, generando consigo que el phishing utilizándose con más frecuencia en nuestro país.

6.3. Antecedentes Regionales

De La Cruz (2021) investigó en su tesis de pregrado respecto al phishing bancario en Huaura. Entre sus metodologías utilizó la investigación exploratoria de un enfoque mixto, con su técnica de análisis de documentos relacionados con la actividad bancaria y el cuestionario. En las conclusiones, los bancos ante las estafas no devuelven al cliente el dinero sustraído ilícitamente de sus cuentas bancarias, justificándose porque no contrató el seguro por fraude financiero y no asumen el riesgo financiero por el uso de la banca por internet donde a través del phishing engañan aparentando ser una institución de confianza, con notificaciones de mensajes de correo electrónico o llamada telefónica.

6.4. Antecedentes Locales

Vesga (2024), investigó en su tesis de pregrado sobre, delitos informáticos en Barranca. Para ejecutar su metodología uso la investigación desde la óptica del enfoque cuantitativo, en el nivel descriptivo, el diseño no experimental, y recopilaron la información a través de la encuesta y entrevista. Llegó a las conclusiones, que los medios informáticos como internet, correos electrónicos, llamadas telefónicas, son las vías idóneas para el ingreso sin consentimiento a las plataformas de datos, incluso hacen sabotaje o se apropian de la información que no les pertenece y vulneran el Derecho fundamental a la invulnerabilidad de las comunicaciones.

6.5. Estado del arte

1. Phishing

1.1. Evolución

Según Ramos (2022) narra que el término "phishing" fue acuñado por primera vez a mediados de la década de 1990 por hackers y estafadores que buscaban formas de robar información confidencial en línea. Sin embargo, las tácticas que ahora asociamos con el phishing tienen sus raíces en prácticas más antiguas de ingeniería social y fraude en línea; como a continuación se aprecia líneas abajo:

Orígenes de la ingeniería social: Mucho antes de que se inventara el término "phishing", los estafadores ya estaban utilizando técnicas de ingeniería social para engañar a las personas y obtener acceso a información confidencial. Esto incluía tácticas como hacerse pasar por empleados de empresas legítimas por teléfono para obtener contraseñas o datos financieros. En otros términos, Gutierrez (2019) lo definió como robo de identidad con ingeniería social, jerga que define el uso de artimañas para que los ciudadanos facilitan información importante”

Primeros ejemplos de phishing: A mediados de la década de 1990, los hackers comenzaron a utilizar el correo electrónico como una herramienta para el robo de identidad y la recolección de información confidencial. En lugar de ataques masivos y automáticos, estos primeros casos de phishing a menudo implicaban el envío de correos electrónicos personalizados a individuos o empresas, haciéndose pasar por instituciones legítimas como bancos o proveedores de servicios en línea.

Crecimiento y sofisticación: A medida que Internet se volvía más omnipresente en la vida cotidiana de las personas, el phishing se volvió más común y sofisticado. Los estafadores comenzaron a utilizar tácticas más

elaboradas, como la creación de sitios web falsos que imitaban perfectamente a empresas legítimas, para engañar a las víctimas y hacer que compartieran información confidencial.

Spear phishing y otros avances: En la década de 2000, el phishing evolucionó para incluir variantes más dirigidas y específicas, como el "spear phishing", que se dirige a individuos o empresas específicas utilizando información personalizada y detallada. Además, surgieron otras formas de phishing, como el "vishing" (phishing por voz a través de llamadas telefónicas) y el "smishing" (phishing a través de mensajes de texto).

Phishing moderno: Hoy en día, el phishing sigue siendo una amenaza importante en línea, con estafadores constantemente desarrollando nuevas técnicas y tácticas para engañar a las personas y robar información confidencial. Esto incluye el uso de sitios web falsos, correos electrónicos y mensajes de texto fraudulentos, así como técnicas de ingeniería social cada vez más sofisticadas.

De modo que, el phishing ha evolucionado desde sus modestos comienzos en la década de 1990 hasta convertirse en una de las formas más comunes de fraude en línea en la actualidad. A lo largo de su historia, los estafadores han demostrado una notable capacidad para adaptarse y desarrollar nuevas tácticas para engañar a las personas y robar información confidencial en línea.

1.2. Definiciones

La palabra Phishing tiene su sigla ph y deviene del idioma inglés "fishing" que traducido al español se refiere a la “pesca”, en el caso concreto significa “pesca de contraseñas”. Por otro lado, el phishing es una forma de ciberdelincuencia en la que los estafadores intentan engañar a las personas para que revelen información confidencial, como contraseñas, números de tarjetas de crédito o información personal, haciéndose pasar por una entidad de confianza. Esto se suele hacer a través de correos electrónicos, mensajes de texto, llamadas telefónicas o mensajes instantáneos que parecen legítimos, pero en realidad son fraudulentos. Los mensajes de phishing a menudo contienen enlaces a sitios

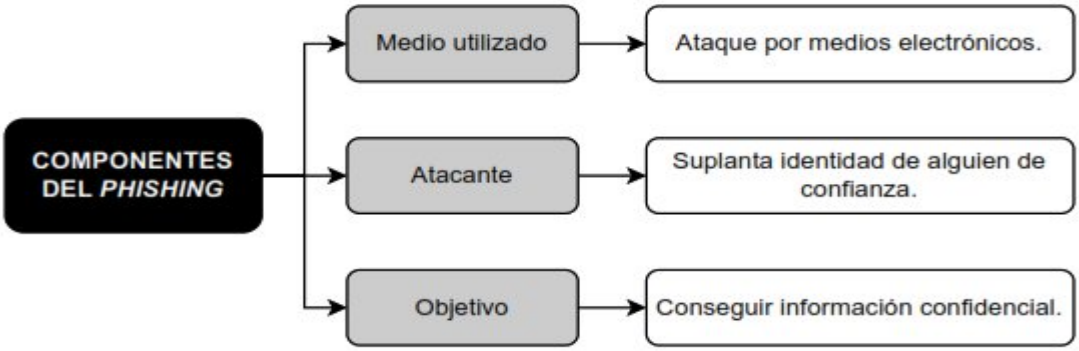
web falsos que imitan a sitios legítimos, donde se les pide a las víctimas que ingresen su información confidencial. El objetivo final del phishing es obtener acceso no autorizado a cuentas, robar identidades o cometer fraudes financieros (Gutiérrez, 2019). Por eso, es importante estar atento a las señales de phishing y tener cuidado al compartir información personal en línea.

El phishing es una técnica de ciberataque en la que los delincuentes intentan engañar a las personas para que revelen información confidencial, como contraseñas, números de tarjetas de crédito o información personal, haciéndose pasar por una entidad de confianza. Esto se realiza generalmente a través de correos electrónicos, mensajes de texto o llamadas telefónicas que parecen legítimos, pero son fraudulentos. Los estafadores suelen utilizar tácticas de ingeniería social para manipular a las víctimas y llevarlas a divulgar su información personal o financiera (Ramos, 2022). Por ello, el objetivo final del phishing es obtener acceso no autorizado a cuentas, robar identidades o cometer fraudes financieros.

2. Fraude informático

Al respecto, Ortega (2024) sostiene que el fraude informático, también conocido como ciberfraude, se refiere a cualquier actividad fraudulenta que se lleva a cabo utilizando tecnologías de la información y la comunicación (TIC). Esto puede incluir una amplia gama de actividades delictivas que se realizan en línea, como el robo de identidad, el phishing, la estafa en línea, el fraude con tarjetas de crédito, el fraude bancario, entre otros. Como a continuación se lista ejemplos comunes de fraude informático:

Phishing: Como hemos discutido anteriormente, el phishing implica el envío de correos electrónicos fraudulentos que parecen provenir de una fuente legítima, como un banco o una empresa, con el objetivo de engañar a las personas para que revelen información confidencial, como contraseñas o números de tarjetas de crédito.



Fuente: Colex (2023)

Ransomware: Este tipo de fraude implica el uso de software malicioso que infecta los sistemas informáticos de las víctimas y cifra sus archivos, exigiendo un rescate a cambio de la restauración de los datos.

Fraude en tarjetas de crédito: Los delincuentes pueden utilizar información de tarjetas de crédito robada para realizar compras fraudulentas en línea o realizar transacciones financieras no autorizadas.

Fraude en subastas y comercio electrónico: Los estafadores pueden utilizar sitios web de subastas en línea o plataformas de comercio electrónico para vender productos inexistentes o falsificados, o para aceptar pagos y no enviar los artículos.

Estafas de soporte técnico: Los estafadores se hacen pasar por representantes de empresas de tecnología legítimas y contactan a los usuarios, afirmado que hay un problema con su computadora o dispositivo, y solicitan acceso remoto o pagos para solucionar el problema, cuando en realidad no hay ningún problema real.

Fraude de inversión en criptomonedas: Con el crecimiento del mercado de las criptomonedas, también ha habido un aumento en los esquemas fraudulentos relacionados con la inversión en criptomonedas, donde los estafadores prometen grandes retornos de inversión, pero en realidad roban los fondos de los inversores.

3. Protección de datos

En esta parte, Gavancho (2015) define a la protección de bases de datos como un conjunto de prácticas y medidas diseñadas para garantizar la seguridad y la integridad de la información almacenada en una base de datos. Esto incluye la implementación de controles de acceso, cifrado de datos, auditorías de seguridad, respaldo de datos y otras medidas de seguridad para proteger la información contra accesos no autorizados, pérdida, robo o corrupción.

Asimismo, Zegarra (2015) lo define como las prácticas, políticas y medidas de seguridad diseñadas para proteger la información almacenada en una base de datos contra accesos no autorizados, pérdida, corrupción o robo. La seguridad de la base de datos es fundamental para garantizar la integridad, confidencialidad y disponibilidad de los datos almacenados en ella. A su vez, refiere algunos aspectos importantes sobre la protección de bases de datos:

Control de acceso: Limitar quién puede acceder a la base de datos y qué acciones pueden realizar los usuarios autorizados. Esto se logra mediante la implementación de mecanismos de autenticación, autorización y auditoría de usuarios.

Cifrado de datos: Proteger los datos sensibles mediante el uso de algoritmos de cifrado para convertir la información en un formato ilegible para cualquier persona que no tenga la clave de descifrado correspondiente.

Auditoría y registro de eventos: Registrar todas las actividades que ocurren en la base de datos, como accesos, consultas y modificaciones de datos. La auditoría de eventos ayuda a detectar y responder rápidamente a posibles amenazas o anomalías de seguridad.

Respaldo y recuperación: Realizar copias de seguridad regulares de la base de datos para garantizar la disponibilidad y la integridad de los datos en caso de pérdida de datos debido a errores humanos, fallas de hardware o software, o ataques cibernéticos.

Actualizaciones y parches de seguridad: Mantener el software de la base de datos actualizado con las últimas actualizaciones y parches de seguridad para proteger contra vulnerabilidades conocidas y mantener la seguridad de la información.

Políticas de retención de datos: Establecer políticas claras sobre la retención y eliminación de datos para garantizar el cumplimiento de las regulaciones de privacidad y protección de datos.

4. Daños y perjuicios

Para Rosas (2014) el daño y su secuela causado por el phishing es significativo y tiene repercusiones tanto para las víctimas como para los perpetradores. Aquí hay algunos aspectos del daño y perjuicio asociado con el phishing:

Violación de la privacidad y protección de datos: El phishing puede resultar en la violación de la privacidad y la protección de datos personales de las víctimas. Cuando los estafadores obtienen acceso a información confidencial, como contraseñas, números de tarjetas de crédito y datos personales, están violando la privacidad de las personas y pueden estar violando leyes de protección de datos.

Fraude y robo de identidad: El phishing puede resultar en fraudes financieros y robo de identidad, lo que puede causar pérdidas económicas significativas para las víctimas. Estos delitos pueden ser perseguidos legalmente y pueden dar lugar a cargos penales contra los perpetradores.

Daños financieros: Las víctimas de phishing pueden sufrir pérdidas financieras directas como resultado de transacciones no autorizadas realizadas por los estafadores con la información robada. Esto puede incluir la pérdida de fondos de cuentas bancarias, el robo de dinero de tarjetas de crédito y otros tipos de fraude financiero.

Daño reputacional: Las empresas y organizaciones afectadas por ataques de phishing pueden sufrir daños en su reputación y credibilidad. La divulgación de una violación de seguridad o un incidente de phishing puede afectar negativamente la

confianza de los clientes, socios comerciales y otros stakeholders, lo que puede tener repercusiones a largo plazo en la reputación y el éxito del negocio.

Responsabilidad legal: Las organizaciones pueden enfrentar responsabilidad legal por no proteger adecuadamente la información personal y financiera de sus clientes. Esto puede resultar en demandas civiles, multas regulatorias y otras sanciones legales por incumplimiento de las leyes de protección de datos y privacidad.

5. Recomendaciones contra el phishig

Los autores de la tesis, recomiendan, para identificar si un mensaje o correo electrónico es un intento de phishing, seguir las siguientes estrategias:

1. Verifica el remitente

- **Dirección de correo:** Asegúrate de que el correo proviene de un dominio legítimo (por ejemplo, @empresa.com y no @empresa.xyz o @servicios-cliente.com). Los atacantes suelen usar direcciones similares a las legítimas para engañarte.
- **Incongruencias en el nombre:** Si el nombre del remitente no coincide con la dirección de correo, es un indicador de phishing.

2. Evalúa el contenido

- **Errores ortográficos o gramaticales**: Los correos fraudulentos suelen contener errores en la redacción, lo que puede ser un indicio de fraude.
- **Urgencia excesiva:** Frases como "¡Tu cuenta será suspendida en 24 horas!" o "¡Responde inmediatamente!" buscan presionarte para que actúes sin pensar.
- **Solicitudes de información sensible**: Ninguna entidad legítima te pedirá tus contraseñas, número de tarjeta, códigos de acceso o datos personales a través de un correo.

3. Inspecciona los enlaces

- **URL sospechosas:** Pasa el cursor sobre los enlaces (sin hacer clic) para verificar si dirigen al sitio legítimo. Por ejemplo, un enlace puede parecer real pero redirigirte a una página falsa (e.g., www.empresalegitima.com.seguridad-falsa.net).
- **Falsos botones:** Botones que al pasar el cursor revelan enlaces no relacionados con el supuesto remitente.

4. Archivos adjuntos

- **Extensiones peligrosas:** No abras archivos con extensiones como .exe, .zip o .bat. Pueden contener malware diseñado para robar tus datos.

- **Adjuntos inesperados:** Si recibes un archivo que no solicitaste, desconfía, incluso si parece provenir de alguien conocido.

5. Examina el saludo

- **Genérico:** Correos dirigidos con términos como "Estimado usuario" o "Cliente valioso" en lugar de tu nombre completo pueden ser fraudulentos.

6. Comprueba el diseño

- **Inconsistencias:** Mensajes con logotipos pixelados, colores diferentes o diseños que no coinciden con los de la empresa real son sospechosos.

7. Otros indicadores

- **Falta de contacto oficial:** Si no incluye información de contacto verificable, como un número de atención al cliente o una dirección física, es un posible intento de phishing.
- **Direcciones internacionales sospechosas:** Si la comunicación parece provenir de un país donde la empresa no opera, puede ser un fraude.

6. Phishing mediante inteligencia artificial (IA)

La evolución del phishing ha encontrado en la Inteligencia Artificial (IA) una herramienta poderosa para sofisticar ataques, ampliando su alcance y efectividad. Este fenómeno, conocido como phishing asistido por IA, representa una amenaza significativa debido a su capacidad para replicar patrones humanos y evadir métodos tradicionales de detección. A continuación, se detallan los aspectos más relevantes de esta problemática:

1. ¿Qué es el phishing con IA?

El phishing con IA utiliza tecnologías como aprendizaje automático (Machine Learning) y procesamiento de lenguaje natural (NLP) para crear ataques más persuasivos, personalizados y difíciles de detectar. Los ciberdelincuentes emplean IA para analizar grandes cantidades de datos, identificar vulnerabilidades y generar mensajes que imitan la comunicación legítima de personas o instituciones.

2. Métodos de phishing con IA

2.1. Generación automática de contenido personalizado

- **Análisis de datos:** Los atacantes recopilan información pública y privada, como redes sociales, historiales de navegación y datos filtrados, para crear mensajes altamente personalizados.
- **NLP avanzado:** Herramientas como ChatGPT u otras IA generativas permiten redactar correos y mensajes con gramática impecable, eliminando los errores típicos que solían delatar los intentos de phishing.

2.2. Deepfakes y suplantación de identidad visual

- **Deepfakes de video o audio:** Los atacantes utilizan IA para generar videos o audios realistas que imitan la voz y apariencia de personas conocidas, como directivos de empresas, con el fin de solicitar transferencias de dinero o acceso a información sensible.
- **Clonación de sitios web:** La IA puede replicar páginas web legítimas con gran precisión, haciendo casi imposible diferenciar entre un sitio real y uno falso.

2.3. Automatización de ataques masivos

- **Chatbots maliciosos:** Los ciberdelincuentes programan IA conversacionales para interactuar con víctimas en tiempo real, simulando atención al cliente o soporte técnico.
- **Simulación de correos empresariales (BEC):** Los sistemas de IA pueden generar correos empresariales que imitan perfectamente el tono, formato y contexto de comunicaciones internas.

3. Impacto del phishing con IA

El uso de IA en el phishing amplifica la escala y efectividad de los ataques, lo que genera consecuencias graves en diversos ámbitos:

- **Aumento en la tasa de éxito:** Los mensajes personalizados generan mayor confianza en las víctimas, incrementando las posibilidades de que estas hagan clic en enlaces maliciosos o compartan información sensible.
- **Desafíos para la detección**: Las soluciones tradicionales, como filtros de spam o sistemas basados en firmas, son insuficientes frente a ataques que evolucionan dinámicamente.
- **Costos económicos y reputacionales:** Las organizaciones enfrentan pérdidas financieras, daños a la reputación y posibles sanciones regulatorias si no protegen adecuadamente los datos de sus usuarios.

4. Estrategias de mitigación

4.1. Educación y concienciación

La capacitación de usuarios es fundamental para reconocer señales de phishing, incluso en mensajes altamente sofisticados. Los programas de simulación de phishing pueden entrenar a los empleados para identificar intentos maliciosos.

4.2. Uso de herramientas impulsadas por IA

La misma tecnología utilizada para los ataques puede emplearse en su detección:

- **Análisis de comportamiento:** Sistemas de IA que detectan anomalías en patrones de comunicación y accesos.

- **Herramientas de autenticación avanzada:** Implementar autenticación multifactorial (MFA) y certificados digitales para validar identidades.

4.3. Colaboración entre organizaciones

La cooperación entre empresas, gobiernos y plataformas tecnológicas es esencial para compartir información sobre nuevas tácticas de phishing y desarrollar soluciones conjuntas.

De modo que, el phishing con IA es un desafío emergente que requiere respuestas proactivas e innovadoras. Si bien la tecnología ha potenciado las capacidades de los ciberdelincuentes, también ofrece herramientas avanzadas para contrarrestar estas amenazas. Las organizaciones deben adoptar un enfoque integral que combine tecnología, educación y colaboración para protegerse frente a esta nueva generación de ataques.

Este fenómeno subraya la necesidad de una legislación actualizada y políticas públicas efectivas que regulen el uso indebido de la IA y refuercen la ciberseguridad en todos los niveles.

7. Qué hacer si sospechas de phishing

Los autores de la tesis, sugieren:

- No respondas al mensaje.
- No hagas clic en enlaces ni descargues archivos adjuntos.
- **Verifica directamente con la empresa:** Accede al sitio oficial o llama al número de atención al cliente para confirmar la autenticidad del mensaje.
- **Reporta el correo:** Usa herramientas de tu proveedor de correo (como Gmail o Outlook) para marcarlo como phishing o envíalo al área de seguridad de la empresa correspondiente.

8. Autenticación biométrica: Una barrera contra el phishing

Por otra parte, Gutierrez (2019) indica en este sub capitulo, que la autenticación biométrica se está posicionando como una solución robusta para mejorar la seguridad digital y prevenir ataques como el phishing. Esta tecnología utiliza características físicas y comportamentales únicas de las personas, como huellas dactilares, reconocimiento facial, iris del ojo o patrones de voz, para verificar identidades. A medida que la biometría se adopta como estándar en sistemas de autenticación, se

vuelve más complicado para los ciberdelincuentes suplantar identidades, ya que estas características son inherentemente únicas e intransferibles.

1. ¿Cómo funciona la autenticación biométrica?

La autenticación biométrica opera a través de los siguientes pasos:

- **Captura**: El sistema registra una característica biométrica, como una huella dactilar o un escaneo facial.
- **Procesamiento**: Los datos capturados se convierten en un patrón digital que se almacena de manera segura en una base de datos o en el dispositivo.
- **Verificación**: Cuando el usuario intenta autenticarse, se compara la característica biométrica proporcionada con el patrón almacenado. Si coinciden, se concede el acceso.

2. ¿Por qué es efectiva contra el phishing?

La biometría dificulta los intentos de suplantación de identidad en los siguientes aspectos:

2.1. Inmutabilidad y unicidad

- Las características biométricas son únicas para cada individuo. A diferencia de contraseñas o PINs, no pueden ser fácilmente robadas, adivinadas o compartidas.
- Ejemplo: Aunque un ciberdelincuente engañe a la víctima para que proporcione credenciales de acceso (usuario y contraseña), no podrá replicar su huella dactilar o escaneo de iris.

2.2. Imposibilidad de replicación a escala

- Incluso con tecnologías avanzadas como deepfakes, replicar características biométricas con la precisión suficiente para engañar a sistemas modernos es extremadamente complicado y costoso.
- Ejemplo: Mientras que un deepfake puede imitar una voz para un ataque telefónico, los sistemas biométricos que analizan patrones vocales únicos (tono, cadencia y frecuencia) pueden detectar la falsificación.

2.3. Combinación con autenticación multifactorial (MFA)

- La biometría puede integrarse como un segundo o tercer factor de autenticación, añadiendo una capa adicional de seguridad.
- Ejemplo: Un atacante que logre acceder a un dispositivo protegido con contraseña aún necesitará la huella dactilar del propietario para completar el acceso.

3. Áreas de aplicación y ventajas

3.1. Financiera

- Bancos y plataformas de pago digital están adoptando la biometría para autorizar transacciones.
- **Beneficio:** Si un atacante intenta realizar un pago con credenciales robadas, necesitará la verificación biométrica, que es difícil de falsificar.

3.2. Empresarial

- Las empresas utilizan autenticación biométrica para controlar el acceso a sistemas críticos y proteger datos sensibles.
- **Beneficio:** Los ataques de phishing dirigidos a empleados no son suficientes para obtener acceso sin la característica biométrica.

3.3. Dispositivos personales

- Smartphones, laptops y dispositivos IoT ahora incluyen reconocimiento facial, de huella dactilar y voz como métodos de desbloqueo.
- **Beneficio:** Aunque un atacante tenga acceso físico al dispositivo, no podrá acceder a los datos sin la biometría del propietario.

4. Retos y desafíos

Aunque la autenticación biométrica es una herramienta poderosa contra el phishing, enfrenta algunos desafíos:

4.1. Privacidad y almacenamiento

- Los datos biométricos deben almacenarse de forma segura, ya que, si son robados, no pueden ser "reiniciados" como una contraseña.

- **Solución:** Utilizar almacenamiento en dispositivos locales en lugar de bases de datos centralizadas para minimizar el riesgo de filtraciones.

4.2. Falsos positivos o negativos

- Factores externos, como cambios físicos (heridas, envejecimiento) o problemas técnicos, pueden dificultar la autenticación.
- **Solución:** Implementar sistemas de respaldo, como autenticación multifactorial o recuperación de acceso mediante métodos tradicionales.

4.3. Tecnologías emergentes

- **Los** atacantes podrían eventualmente desarrollar métodos para falsificar biometría (por ejemplo, impresión 3D avanzada para replicar huellas).
- **Solución:** Avanzar en sistemas biométricos multifactoriales que analicen múltiples características simultáneamente (por ejemplo, huella dactilar y reconocimiento de voz).

5. Futuro de la biometría en la lucha contra el phishing

- **Biometría conductual:** Los sistemas del futuro analizarán patrones de escritura, uso del mouse o interacciones con dispositivos, creando una capa adicional de autenticación difícil de replicar.
- **Integración en blockchain:** La biometría podría vincularse a identidades digitales protegidas por blockchain, asegurando que solo el usuario legítimo pueda acceder a datos o sistemas.
- **IA defensiva:** Las tecnologías de inteligencia artificial evolucionarán para detectar intentos sofisticados de replicar características biométricas.

En suma, algo personal, como una impresión de su voz, su huella dactilar, un escaneo de retina o reconocimiento facial, u otras características únicas de su cuerpo, conocidas colectivamente como **biometría**.

9. <u>Peritajes oficiales</u>

Al respecto la Defensoría del Pueblo (2023) narra que en el 2018, el Ministerio Público estableció la Oficina de Peritajes como parte del Instituto de Medicina Legal

y Ciencias Forenses, con la finalidad de gestionar el trabajo de los peritos especializados en emitir opiniones técnico-científicas en diversas áreas, excluyendo la medicina legal. Posteriormente, en julio de 2019, esta oficina pasó a ser un órgano de apoyo bajo la Gerencia General, según lo establecido por la Resolución de la Fiscalía de la Nación N° 1974-2019-MP-FN.

La Oficina de Peritajes ha enfocado su labor en campos forenses como la reconstrucción de escenas del crimen, antropología física, fonética, balística, grafotecnia, contabilidad, ingeniería civil, medio ambiente y análisis digital. Entre 2019 y julio de 2020, el área de análisis digital forense atendió 534 solicitudes, que incluyeron actividades como la autenticación de archivos digitales (audio, imagen y video), recuperación de archivos electrónicos, análisis de sistemas informáticos, desbloqueo de teléfonos celulares y recuperación de mensajes de aplicaciones como WhatsApp.

Sin embargo, los peritos enfrentaron diversas dificultades, como el desconocimiento técnico por parte de los fiscales para formular solicitudes claras sobre el análisis de evidencia digital, presentando requerimientos ambiguos como “entrega de toda información de interés”. Asimismo, enfrentaron una alta demanda de solicitudes periciales, lo que representa un reto adicional para el cumplimiento eficiente de sus funciones.

10. Legislación vigente

El capítulo sobre legislación vigente analiza las disposiciones normativas nacionales e internacionales que abordan la ciberdelincuencia, en especial el phishing, como un delito informático de creciente relevancia.

1. Marco Internacional

En este sub capitulo la Defensoría del Pueblo (2023) afirma que el Perú formalizó su adhesión al Convenio de Budapest sobre Ciberdelincuencia en el 2019, aprobado por el Congreso mediante la Resolución Legislativa N° 30913 y ratificado por el Poder Ejecutivo con el Decreto Supremo N° 010-2019. Este

convenio, que entró en vigor el 1 de diciembre de ese año, establece estándares para prevenir, investigar y sancionar los delitos informáticos y promueve la cooperación internacional.

El Convenio de Budapest incluye dos protocolos adicionales:

- **Primer protocolo (2003):** Criminaliza conductas racistas y xenófobas realizadas mediante sistemas informáticos.

- **Segundo protocolo (2022):** Mejora la cooperación internacional para obtener evidencia digital, facilitando la colaboración con empresas proveedoras de servicios y datos en jurisdicciones extranjeras.

De aquí que, aunque el Perú no se ha adherido a estos protocolos, sigue participando en iniciativas internacionales, como la negociación de una convención integral sobre ciberdelincuencia en el seno de la ONU, la cual se espera sea aprobada.

2. Marco Normativo Nacional

El Perú ha ido desarrollando un marco jurídico progresivo para enfrentar los delitos informáticos, basado en las directrices del *Convenio de Budapest*. La normativa nacional incluye las siguientes disposiciones clave:

2.1. Código Penal

- En 1991, el Código Penal tipificó el hurto telemático como una modalidad agravada de hurto en los delitos contra el patrimonio.
- En el año 2000, se promulgó la Ley N° 27309, que incorporó al Código Penal el capítulo de delitos informáticos, incluyendo:

    - **Artículo 207-A:** Delito informático (acceso indebido a sistemas y bases de datos).
    - **Artículo 207-B:** Daño o alteración de bases de datos y sistemas informáticos.
    - **Artículo 207-C:** Formas agravadas de estos delitos.

2.2. Ley de Delitos Informáticos (Ley N° 30096, publica 22/10/2013)

Publicada en 2013, esta ley derogó el capítulo de delitos informáticos del Código Penal y estableció un marco integral para sancionar ciberdelitos, entendidos como conductas criminológicas de carácter pluriofensiva, "estos es conductas que contravienen diversos bienes jurídicos que en su realización se hace uso de las computadoras u otros equipos de tecnología informática y de comunicación" - TICs[1] (Rosas, 2023, p.108).

A continuación, se agrupa en cinco categorías según los bienes jurídicos protegidos según la ley especial:

1. **Datos y sistemas informáticos:**
   - Acceso ilícito (artículo 2).
   - Atentado a la integridad de datos y sistemas informáticos (artículos 3 y 4)
   - Abuso de mecanismos y dispositivos informáticos (artículo 10).

2. **Indemnidad y libertad sexual:**
   - Grooming (artículo 5).
   - Pornografía infantil (artículo 183-A del Código Penal).
3. **Intimidad y secreto de las comunicaciones:**
   - Interceptación de datos informáticos (artículo 7).
   - Tráfico ilegal de datos personales (artículo 154-A del Código Penal).

4. **Patrimonio:**
   - Fraude informático (artículo 8).
   - Préstamo informático extorsivo (8-A incorporado por ley 32183 en su artículo 2, difundido oficialmente el 11-12-2024)

5. **Fe pública:**
   - Suplantación de identidad (artículo 9).

[1] TICs en plural solo cuando se habla de tipos o clases de estas tecnologías.

En 2014, la Ley fue modificada por la Ley N° 30171, que adaptó estas descripciones a las disposiciones del Convenio de Budapest.

2.3. Otras normativas relevantes

- **Ley N° 29733 (2011):** Ley de Protección de Datos Personales, que regula la privacidad de los datos y establece obligaciones para las entidades que procesan esta información.

- **Decreto Legislativo N° 1182 (2015):** Modifica el artículo 162-A del Código Penal, regulando la interceptación de comunicaciones.

Por consiguiente, el marco normativo vigente en el Perú constituye un avance significativo en la lucha contra los delitos informáticos, incluyendo el phishing. Sin embargo, resulta esencial continuar fortaleciendo las leyes nacionales y fomentar la cooperación internacional para garantizar una protección efectiva frente a las amenazas cibernéticas, en un contexto de creciente dependencia tecnológica y globalización.

11. Derecho comparado

11.1. Colombia

Por otro lado, Rosas (2014) explica que, en el país de Colombia, el phishing es una amenaza significativa en el ámbito de la ciberseguridad, al igual que en muchos otros países. Los colombianos son susceptibles a este tipo de ataques, que pueden ocurrir a través de correos electrónicos, mensajes de texto, llamadas telefónicas u otras formas de comunicación digital.

Legislación y Aplicación de la Ley: Colombia cuenta con leyes y regulaciones relacionadas con la ciberseguridad y el fraude en línea. Las

autoridades colombianas trabajan para hacer cumplir estas leyes y llevar ante la justicia a los perpetradores de ataques de phishing y otros delitos cibernéticos.

Por tanto, el phishing representa una amenaza importante para la seguridad cibernética en Colombia, al igual que en otros lugares del mundo. La educación, la concientización, la cooperación internacional y la aplicación efectiva de la ley son elementos clave en la lucha contra este tipo de delito en el país.

11.2. México

También Zegarra (2015) expone que el phishing en dicho país, es una amenaza significativa en el ámbito de la ciberseguridad. Como en otros países, los ciudadanos mexicanos son susceptibles a este tipo de ataques, que pueden ocurrir a través de diversas plataformas digitales como correos electrónicos, mensajes de texto, llamadas telefónicas y redes sociales. Aquí hay algunos aspectos relevantes sobre el phishing en México:

Legislación y Aplicación de la Ley: México cuenta con leyes y regulaciones relacionadas con la ciberseguridad y el fraude en línea. Las autoridades mexicanas trabajan para hacer cumplir estas leyes y llevar ante la justicia a los perpetradores de ataques de phishing y otros delitos cibernéticos.

Entonces, el phishing representa una amenaza importante para la seguridad cibernética en México, y la educación, la concientización, la cooperación internacional y la aplicación efectiva de la ley son elementos clave en la lucha contra este tipo de delito en el país.

11.3. España

Colex (2023 alega que la adaptación del Código Penal español que se realizó mediante la Ley Orgánica 14/2022 a las directivas europeas, implicó un esfuerzo por armonizar las leyes nacionales con las exigencias legales de la

Unión Europea. Dentro de esta reforma, se incorporó disposiciones específicas para delitos tecnológicos como el phishing que implica la suplantación de identidad para obtener información personal, financiera o confidencial de manera fraudulenta. Este tipo de delito es cada vez más común debido al uso masivo de internet y las plataformas digitales.

Con la reforma introducida por la Ley Orgánica 14/2022, el artículo 249.1.a) del Código Penal español incorpora específicamente el phishing como una conducta punible. Este artículo establece las bases para sancionar con 6 meses a 3 años con pena de prisión a quienes, a través de engaños o suplantación, obtengan datos o bienes de terceros, encajando el phishing en la categoría de estafas tecnológicas.

La actualización legislativa muestra cómo el sistema jurídico se adapta para abordar nuevos tipos de delitos, como los tecnológicos, que no estaban claramente definidos en legislaciones previas **como en el caso de Perú**. Incluso con transposición de directivas europeas, este punto refleja la importancia de la armonización normativa en los estados miembros de la Unión Europea, que no solo responde a necesidades locales, sino también a obligaciones internacionales.

Por último, la protección de la seguridad digital se logró con la inclusión del phishing como un delito tipificado, a su vez demuestra el interés por reforzar la seguridad de los ciudadanos en el ámbito digital, un tema crucial en una sociedad cada vez más tecnológica.

11.4. El phishing en la jurisprudencia española

Según Colex (2023) el phishing ha sido objeto de análisis en diversas sentencias de la jurisprudencia española, reflejando la evolución de los tribunales frente a este delito tecnológico. Estas resoluciones abordan su modus operandi, como se aprecia a contunuacion:

- **La Sentencia de la Audiencia Provincial de Madrid n.º 412/2020**

Analiza un caso de **estafa informática**, conocido al estafador como **phishing**, que consiste en obtener datos confidenciales de manera fraudulenta, como contraseñas o información bancaria. Los delincuentes, llamados "phishers", emplean métodos como correos electrónicos masivos que simulan ser de entidades confiables, páginas web falsas que imitan empresas legítimas o llamadas telefónicas engañosas. También pueden usar correos que introducen "troyanos" en los dispositivos para captar datos bancarios durante transacciones en línea. El objetivo principal es engañar a usuarios de bancos o servicios de pago digital, aprovechando su confianza en aparentes comunicaciones oficiales.

- **La Sentencia de la Audiencia Provincial de Las Palmas n.º 44/2019**
  Aborda el **phishing**, una modalidad de estafa en la que se accede de forma fraudulenta a cuentas bancarias ajenas, haciéndose pasar por sus titulares para realizar transferencias. Los perpetradores suelen operar desde otros países, lo que complica la cooperación policial internacional. Para evitar alertas, emplean intermediarios locales que, a cambio de una comisión, utilizan sus cuentas bancarias para recibir el dinero y transferirlo posteriormente al extranjero. Estos colaboradores suelen ser captados a través de falsas ofertas laborales en internet, asumiendo, en muchos casos, la responsabilidad penal del delito.

- **La Sentencia de la Audiencia Provincial de Valencia n.º 254/2022**

  Describe el phishing como un delito en el que se engaña a la víctima haciéndose pasar por un tercero confiable. Para lograrlo, los responsables utilizan elementos visuales, como emblemas o marcas comerciales similares, con el objetivo de obtener datos personales y de seguridad, generando un perjuicio económico a la víctima.

- **La Sentencia de la Audiencia Provincial de Zaragoza n.º 804/2022**

  Detalla el **phishing** como un ataque diseñado para obtener datos de acceso bancario de manera fraudulenta, con el objetivo de realizar

transferencias no autorizadas. Los delincuentes adquieren herramientas en internet que incluyen programas, listas de correos electrónicos y equipos comprometidos. Envían correos masivos que redirigen a páginas web falsas, alojadas en servidores cuya seguridad ha sido vulnerada, normalmente en otros países. Los datos recopilados se usan para transferir fondos a colaboradores locales, quienes retiran el dinero, se quedan con una comisión y luego lo envían al extranjero a través de empresas especializadas.

- **STS n.º 834/2012, de 25 de octubre**

  El phishing es descrito como un fraude basado en el envío masivo de correos electrónicos que redirigen a páginas web falsas, casi idénticas a las originales de entidades bancarias. Los usuarios son presionados mediante mensajes amenazantes para proporcionar sus claves personales, como medida para evitar supuestas pérdidas económicas. Una vez obtenidas, los datos son utilizados para acceder ilegalmente a las cuentas de las víctimas y sustraer fondos. Este modus operandi, que simula una "pesca" de datos, permite el desapoderamiento económico de las personas afectadas.

- **STS n.º 506/2015, de 27 de julio**

  Se destaca que el phishing es una estrategia delictiva única que busca acceder fraudulentamente a las claves bancarias de usuarios confiados de banca online. Los fondos obtenidos son transferidos a terceros países o colocados a nombre de personas difíciles de identificar. Este método fraudulento permite el acceso no autorizado a las cuentas de las víctimas para extraer dinero y transferirlo a lugares seguros, dificultando la intervención de las autoridades policiales en los países afectados.

- **STS n.º 291/2021, de 7 de abril**

  El phishing bancario consiste en enviar enlaces fraudulentos al correo electrónico o teléfono móvil de las víctimas, simulando ser páginas

oficiales de entidades bancarias. Al ingresar sus claves en estos sitios falsos, los datos son robados y utilizados para realizar transferencias no autorizadas. Además, los acusados empleaban otras modalidades de engaño, como ventas falsas o fraudes en arrendamientos temporales, recibiendo los pagos en cuentas creadas con documentación falsa, para luego apropiarse del dinero sin prestar los servicios ofrecidos.

VII. HIPÓTESIS Y CATEGORÍAS DE ESTUDIO

7.1. Hipótesis

Hipótesis general

La determinación de la regulación del phishing como modalidad de fraude informático protege los datos personales en el Distrito de Barranca, 2022-2023

Hipótesis específicas

He.1. La regulación en el Código Penal del phishing en la modalidad de fraude informático, si se protege los datos personales en el Distrito de Barranca, 2022-2023

He.2. Determinando el bien jurídico económico, social y jurídico en la regulación del phishing, se protege los datos personales en el Distrito de Barranca, 2022-2023

7.2. Categorías de estudio

Categoría X:

- Determinación phishing, y
- Regulación phishing.

Categoría Y:

- Fraude informático, y
- Protección de datos

7.3. Tabla de categorización

CATEGORÍAS	DEFINICIÓN		SUB CATEGORÍAS		INSTRUMENTO	MUESTRA
	Conceptual	Operacional				
Categoría X: Determinación phishing, e Regulación phishing	La determinación de phishing se refiere a la capacidad de reconocer y detectar intentos de phishing. Y, la segunda categoría, las leyes suelen estar diseñadas para proteger a los consumidores, garantizar la seguridad de la información y combatir el crimen cibernético (Zegarra, 2015).	Ambas categorías serán estudiadas por intermedio de la guía de análisis de documentos que contengan información de la determinación del phishing, a efectos de efectuar la discusión de los resultados, luego dar las conclusiones y recomendaciones, conforme a la metodología diseñada.	Capacidad	Reconoce	Guía de análisis documental	Documentales especializadas en phishing
				Intentos fraude		
			Leyes	Protejan		
				Garantiza seguridad		
Categoría Y: Fraude informático, e Protección de datos	El fraude informático, conocido como ciberfraude, es cualquier actividad fraudulenta. Y, la protección de datos es un conjunto de medidas y prácticas diseñadas para garantizar la seguridad, privacidad e integridad de la información personal y confidencial (Rosa, 2014 y Gavancho, 2015).		Delito	Acción ilegal		
				Ciberdelito		
			Medidas prácticas	Integridad información		
				Confidencial		

Fuente: Elaboración de los autores

VIII. OBJETIVOS

Objetivo General

Analizar la determinación de la regulación del phishing como modalidad del fraude informático en la protección de datos en el Distrito de Barranca, 2022-2023

Objetivos Específicos

Oe.1. Describir la regulación del phishing en la modalidad de fraude informático en el Distrito de Barranca, 2022-2023

Oe.2. Clasificar la determinación en la regulación del phishing para la protección de datos personales en el Distrito de Barranca, 2022-2023

IX. METODOLOGÍA

9.1.Tipo y Diseño de investigación

9.1.1. Tipo de investigación

9.1.1.1. Según su finalidad

La investigación fue básica, por cuanto y en tanto, en puridad sirvió de base teóricamente, aportando gran aporte sustantiva para que otros investigadores de la misma línea temática, a efectos que se planteen tesis de alcance mayores, incluso con diseños longitudinales para abordar con mayor amplitud el objeto de la investigación" (Hernández y Mendoza, 2018, p. xxxi).

9.1.1.2. Según su alcance

Cortes y Álvarez (2017) sostienen que un proyecto de investigación se distingue por su alcance, por consiguiente, fue *descriptivo* por razones de su especificidad en sus propiedades internas y externas caracterizándolas de acuerdo a su naturaleza y proporción, incluso precisan los perfiles de los agentes que participan en la investigación ya sea como objetos y sujetos.

9.1.2. Diseño de investigación

9.1.2.1. No experimental y transversal

Se aplicó el diseño *no experimental,* por ser la unidad de análisis hechos y documentales, que no es posible verificarlos en un laboratorio, ni en un tubo de ensayo, microscopio, por lo contrario, su estudio se inicia con el análisis exhaustivo de las categorías X y Y.

Además, el diseño no experimental se subdivide del cual se escogió el tipo *transversal*, de modo que la obtención de los datos y documentales se efectuó en el tiempo determinado en el cronograma de trabajo, sin necesidad de seguir a la unidad de estudio, de información ni a la de muestreo. Por lo tanto, de esa forma se encaminó el trabajo para obtener los resultados y hacer la discusión de los resultados según las técnicas metodológicas.

9.1.3. Enfoque de la investigación

9.1.3.1. Cualitativo

Según, Hernández y Mendoza (2018) el enfoque cualitativo: "estudia hechos y acontecimientos que se vinculan con el mundo subjetivo con el fin de describirlo, comprenderlo en su contexto de la praxis real y efectuar la interpretación de los fenómenos, aplicando el método deductivo, vale decir, inicia de lo particular hacia lo general y más no comprueba teorías".

9.2. Población – Muestra

9.2.1. Población

Se trabajó con el acervo documentario especializado sobre el phishing.

9.2.2. Muestra

En cuanto a la muestra, fue las documentales de revistas, libros, encuesta del Instituto Nacional de Estadística e Informática[2], informes de la Policía Nacional del Perú[3].

[2] En adelante INEI
[3] En adelante PNP

9.3. Técnicas e instrumentos de investigación

9.3.1. Técnica

Se utilizó como técnica de análisis documental que consistió en obtener información directa de las fuentes directas y secundarias debidamente seleccionadas como muestra, mediante un procedimiento libre para su revisión analítica (Hernández y Mendoza, 2018).

9.3.2. Instrumento

El instrumento idóneo fue la guía de análisis documental por cuanto agrupó encuestas del INEI, libros, artículos, legislaciones o documentos que permitieron alcanzar el objetivo investigatorio, con la función exclusiva de analizarlos conforme a las reglas de la investigación científica y sin desligarse del problema materia de estudio (Cortes y Álvarez, 2017).

9.3.3. Procedimiento y análisis

La investigación partió de la recopilación, organización y análisis de datos que el investigador examinó para identificar patrones y hallazgos relevantes que se relacionen con la pregunta de tesis.

Estos hallazgos ayudaron a desarrollar soluciones factibles y prácticas a los problemas actuales. Por tanto, para lograr este objetivo fue necesario analizar:

a) Entrada: se organizó adecuadamente la información obtenida del análisis documental y se sistematizó.

b) Proceso: Se buscó los datos más relevantes de los irrelevantes, concordándolo con la realidad sociocultural e idiosincrasia según la localización del proyecto.

c) Salida: se obtuvo la información relevante utilizando los filtros anteriores, a efectos de extraer y explicar desde su origen y seleccionar los efectos del objeto de estudio, el mismo que se tabuló mediante el Excel, para plasmarlo en cuadros y gráficas en los capítulos de resultados y discusión.

El análisis para la precisión del instrumento:

Se utilizó el instrumento de la guía de análisis documental, estos documentos no son cuantificables, sin embargo, se usó para obtener información de calidad y específica para el caso en concreto. Por ende, según los metodólogos no se valida por especialistas, por su propia naturaleza, ya que recopila literatura aceptada pacíficamente por la academia y con el animus de profundizar los conocimientos sobre el tema delimitado por los investigadores.

X. CONSIDERACIONES ÉTICAS

En el informe final de investigación, y de acuerdo con la Universidad Nacional de Barranca (2016), se consideraron las disposiciones de conducta establecidas en el artículo 10 del "Código de Ética para la Investigación", aprobado mediante el acto resolutivo de la Comisión Organizadora N° 573-2016-UNAB, de esta normativa, se extrajeron y aplicaron los siguientes principios:

- Honestidad: Respetando los derechos de autor, parafraseando y citando cuando corresponda.

- Exactitud: La información que se obtengan después de procesar nuestra unidad de análisis debe ser veraz y sin sesgo.

- Eficiencia: Usando la información relevante, para la defensa de la tesis.

- Objetividad: En una investigación se refiere a la imparcialidad y neutralidad en el proceso de recopilación, análisis e interpretación de datos, incluso en la sustentación de la tesis también se aplicó dicho principio.

- Consentimiento informado: Por ser esencial para proteger los derechos y el bienestar de los participantes en la investigación, ya que asegura que las decisiones de participación se tomen de manera informada y voluntaria, en línea con principios éticos y regulaciones internacionales.

- Confidencialidad: En la investigación científica es esencial para proteger la privacidad y los derechos de los participantes. Los investigadores tienen la responsabilidad ética y legal de asegurar que se respete y se mantenga la confidencialidad de la información recopilada durante el proceso de investigación.

XI. RESULTADOS Y DISCUSIÓN

11.1. Resultados

11.1.1. Denuncia policial

Cuadro N° 01

CUADRO N° 1.2
PERÚ: DENUNCIAS POR COMISIÓN DE DELITOS CONTRA EL PATRIMONIO, SEGÚN DELITO ESPECÍFICO, 2019 - 2023

Delito específico	2019	2020	2021	2022	2023	Variación 2023 / 2022	
						Abs.	%
Total	**296 760**	**189 656**	**247 672**	**316 728**	**375 673**	58 945	18,6
Hurto	163 319	102 677	131 973	164 617	195 916	31 299	19,0
Robo	97 886	49 622	62 973	84 281	102 360	18 079	21,5
Estafa y otras defraudaciones	11 160	12 871	19 444	24 823	31 152	6 329	25,5
Receptación	2 960	3 742	5 602	12 502	12 698	196	1,6
Usurpación	6 470	8 680	11 722	11 179	11 155	-24	-0,2
Daños	4 913	3 981	6 081	7 518	8 670	1 152	15,3
Apropiación ilícita	3 506	2 843	3 446	3 439	4 088	649	18,9
Robo en grado tentativa	2 782	1 612	1 989	2 395	2 558	163	6,8
Delitos informáticos	930	1 287	1 551	1 850	2 125	275	14,9
Extorsión	515	467	720	1 835	2 396	561	30,6
Abigeato	1 677	1 156	1 263	1 347	1 502	155	11,5
Disposición común	626	703	893	934	1 042	108	11,6
Fraude en la administración de personas jurídicas	16	15	15	8	11	3	37,5

Fuente: Instituto Nacional de Estadística e Informática - Registro Nacional de Denuncias de Delitos y Faltas. Policía Nacional del Perú-Sistema de Denuncias Policiales (SIDPOL).

Interpretación:

El análisis de las denuncias por **delitos informáticos** en Perú durante los años 2022 y 2023 refleja un **incremento significativo del 14.9%**, pasando de **1,850 denuncias en 2022** a **2,125 en 2023**, según los registros del Instituto Nacional de Estadística e Informática-INEI (2023) y la Policía Nacional del Perú (PNP). Este crecimiento evidencia el impacto creciente de la **criminalidad digital**, impulsada por la expansión del uso de tecnologías, el comercio electrónico y la digitalización de servicios. La variación positiva sugiere tanto un **incremento en la actividad delictiva cibernética** como una posible **mayor disposición de las víctimas a denunciar**, reflejando una mayor visibilización del fenómeno. En este contexto, resulta imperativo fortalecer la **legislación en materia de ciberdelincuencia**, optimizar los **mecanismos de denuncia y persecución penal**, y promover la **capacitación en ciberseguridad** tanto en el sector público como en el privado, a fin de mitigar los riesgos asociados a estos delitos y reducir su impacto en la sociedad.

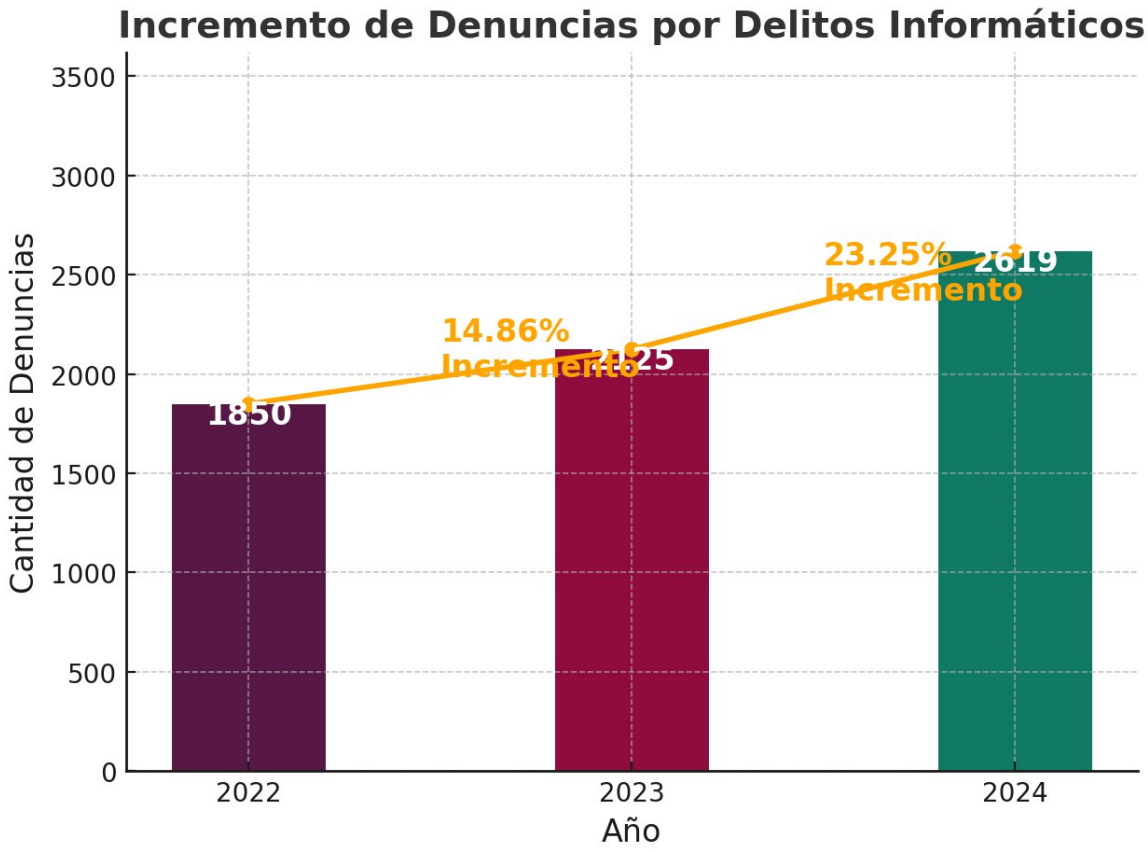


Grafico N° 1

Fuente. Cuadro 1

Elaboración propia

Interpretación:

El crecimiento de las denuncias por delitos informáticos en Perú entre 2022 y 2024 evidencia una tendencia ascendente preocupante, con un incremento del **14.86%** entre 2022 y 2023, y una proyección de crecimiento del **23.25%** para 2024. Este fenómeno puede atribuirse tanto a una mayor incidencia de delitos cibernéticos como a un incremento en la conciencia y reporte de estos eventos. La aceleración en la tasa de crecimiento sugiere la necesidad de fortalecer los mecanismos de **ciberseguridad, regulación y respuesta judicial**, a fin de mitigar el impacto de estas actividades ilícitas en la sociedad y la economía digital. Además, es imperativo que las instituciones gubernamentales, las empresas y los ciudadanos adopten estrategias más robustas de **prevención y protección de datos**, dado que la transformación digital ha ampliado significativamente las superficies de ataque. En este contexto, las **políticas públicas y la cooperación interinstitucional** jugarán un papel crucial para enfrentar este desafío emergente con medidas efectivas de prevención, monitoreo y sanción.

11.1.2. Denuncias ingresadas a la Fiscalía

Cuadro N° 02

CUADRO N° 2.1
PERÚ: DELITOS GENÉRICOS INGRESADOS EN LAS FISCALÍAS PROVINCIALES PENALES Y MIXTAS, 2019 - 2023

Tipo de delito	2019		2020		2021		2022		2023	
	Total	%	Total	%	Total	%	Total	%	Total	%
Total	**1 081 851**	**100,0**	**693 475**	**100,0**	**1 025 359**	**100,0**	**1 126 824**	**100,0**	**1 233 421**	**100,0**
Contra el patrimonio	321 591	29,7	184 754	26,6	262 866	25,6	309 398	27,5	397 236	32,2
Contra la vida, el cuerpo y la salud	426 596	39,4	291 806	42,1	402 959	39,3	355 452	31,5	386 589	31,3
Contra la seguridad pública	79 171	7,3	62 862	9,1	84 397	8,2	96 744	8,6	100 886	8,2
Contra la familia	74 772	6,9	26 652	3,8	55 674	5,4	77 390	6,9	91 531	7,4
Contra la administración pública	62 481	5,8	47 036	6,8	60 017	5,9	61 197	5,4	69 127	5,6
Contra la libertad	59 399	5,5	41 251	5,9	55 294	5,4	56 804	5,0	68 385	5,5
Informáticos (Ley N° 30096)	7 897	0,7	8 674	1,3	18 424	1,8	19 064	1,7	29 580	2,4
Contra la fe pública	23 521	2,2	12 855	1,9	19 035	1,9	24 710	2,2	26 640	2,2
Ambientales	9 969	0,9	7 125	1,0	9 122	0,9	9 641	0,9	12 199	1,0
Contra la tranquilidad pública	3 293	0,3	2 033	0,3	3 309	0,3	2 636	0,2	3 387	0,3
Otros delitos 1/	10 026	0,9	7 471	1,1	9 841	1,0	9 564	0,8	13 889	1,1
No tipificados	3 135	0,3	956	0,1	44 421	4,3	104 224	9,2	33 972	2,8

1/ Comprende delitos contra el Estado y la defensa Nacional, contra el honor, contra el orden económico, contra el orden financiero y monetario, contra el patrimonio cultural, contra la buena fe en los negocios, entre otros.
Nota 1: Delitos registrados a través de denuncias penales, que no incluyen denuncias en estado de derivación, acumulados ni cuadernos.
Nota 2: Información 2022 actualizada, se agregó los delitos no tipificados.
Fuente: Ministerio Público - Sistema de Información de Apoyo al Trabajo Fiscal (SIATF) y Sistema de Gestión Fiscal (SGF).
Elaboración: Instituto Nacional de Estadística e Informática.

Interpretación:

El análisis de los delitos informáticos en Perú, conforme a la Ley N° 30096, revela un **incremento alarmante** en el número de casos ingresados en las fiscalías provinciales penales y mixtas. En **2022**, se registraron **19,064 denuncias**, mientras que en **2023**, la cifra ascendió a **29,580 denuncias**, representando un **crecimiento del 55.2%** en solo un año. Este incremento exponencial sugiere un **aumento en la actividad delictiva cibernética**, impulsada por la mayor digitalización de procesos y la proliferación de delitos como el **fraude electrónico, suplantación de identidad y acceso ilícito a sistemas informáticos**. La creciente incidencia de estos delitos pone de manifiesto la necesidad de **fortalecer las capacidades investigativas y sancionadoras** del sistema de justicia, así como la **implementación de estrategias preventivas y de ciberseguridad** tanto en el sector público como en el privado. Además, es fundamental promover la **educación digital y la concienciación sobre riesgos cibernéticos** entre la ciudadanía para reducir la vulnerabilidad ante este tipo de delitos.

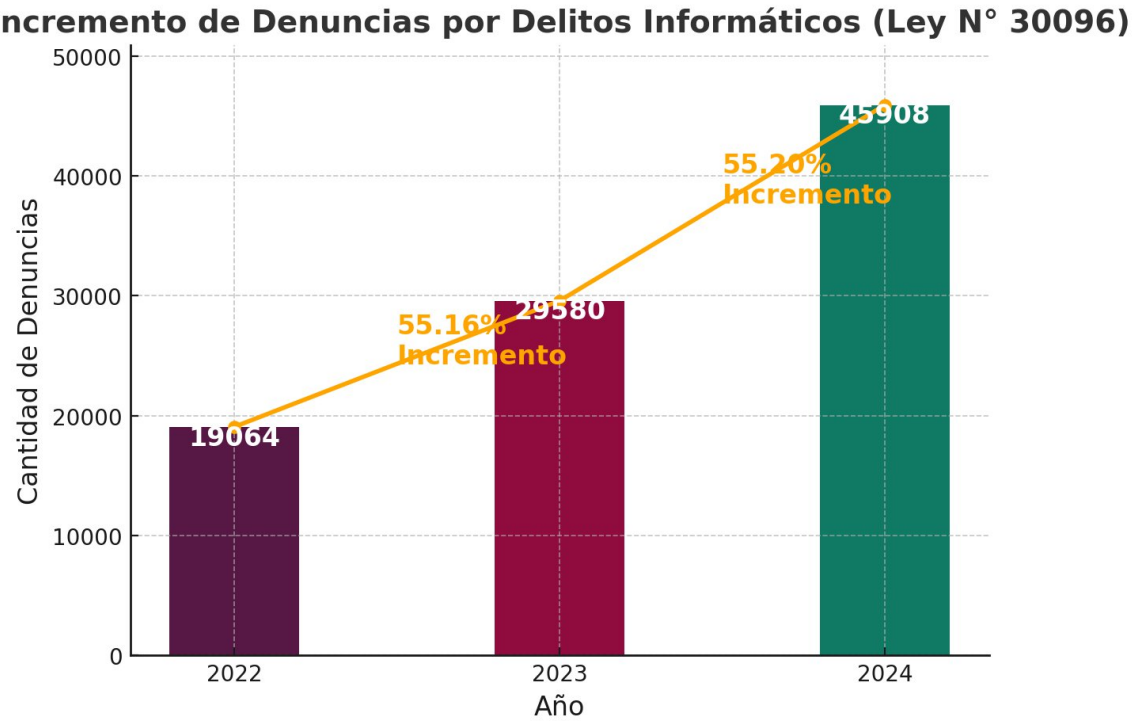


Grafico N° 2

Fuente. Cuadro 2

Elaboración propia

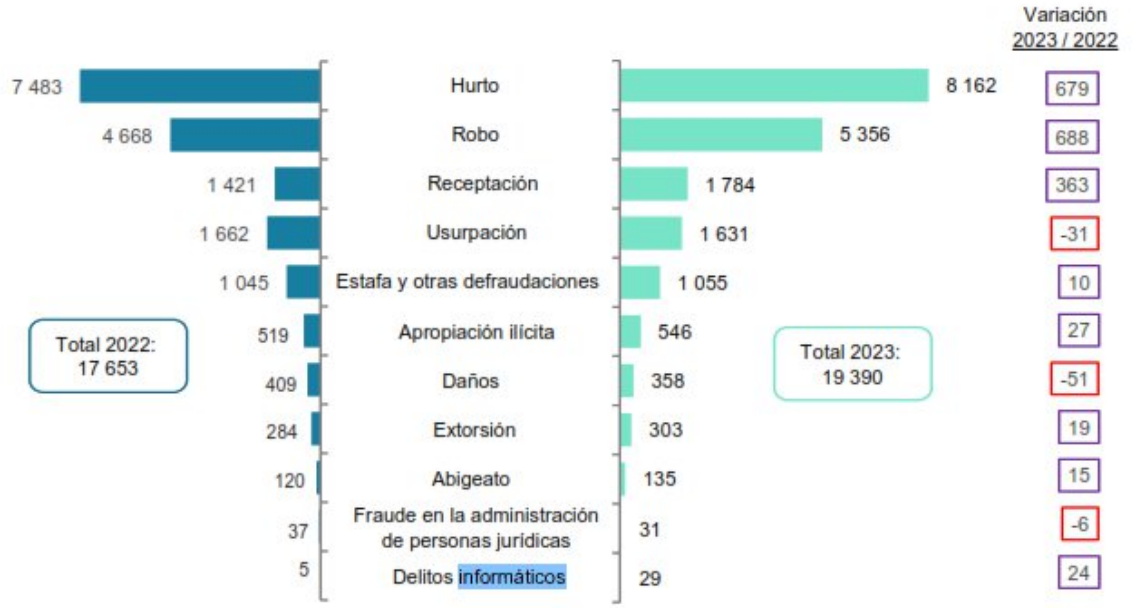
Interpretación:

El análisis de las denuncias por delitos informáticos en el marco de la Ley N° 30096 en Perú evidencia un crecimiento alarmante, con un incremento del 55.16% entre 2022 y 2023, pasando de 19,064 a 29,580 casos registrados en las fiscalías provinciales penales y mixtas. La proyección para 2024 estima un aumento sostenido del 55.20%, lo que llevaría la cifra a 45,908 denuncias. Este ascenso exponencial sugiere un impacto creciente de la criminalidad digital, impulsado por la expansión de la conectividad, la digitalización de procesos y el incremento en la sofisticación de los delitos cibernéticos, como el fraude informático, la suplantación de identidad y la violación de datos personales. El rápido aumento en la incidencia de estos delitos exige una respuesta estratégica por parte del sistema de justicia, enfocada en la modernización de los mecanismos de detección, persecución y sanción penal. Asimismo, es imperativo fortalecer la educación en ciberseguridad, tanto a nivel gubernamental como en el sector privado y la sociedad civil, a fin de mitigar la vulnerabilidad ante estos delitos. La tendencia al alza en las denuncias subraya la urgencia de políticas públicas más eficaces y reducir su impacto en la economía digital y la seguridad ciudadana.

11.1.3. Sentencias Poder Judicial

Cuadro N° 03

Gráfico N° 3.5
PERÚ: PERSONAS CON SENTENCIA CONDENATORIA REGISTRADA POR COMISIÓN DE DELITOS CONTRA EL PATRIMONIO, SEGÚN DELITO ESPECÍFICO, 2022 - 2023



Fuente: Poder Judicial - Registro Nacional de Condenas.
Elaboración: Instituto Nacional de Estadística e Informática.

Interpretación:

El análisis de las sentencias condenatorias por delitos informáticos en Perú, basado en el Registro Nacional de Condenas del Poder Judicial, muestra un incremento sustancial entre 2022 y 2023. En 2022, solo 5 personas fueron condenadas por estos delitos, mientras que, en 2023, la cifra aumentó a 29 condenas, representando una variación absoluta de 24 condenas. Este incremento evidencia un avance en la judicialización y sanción de la ciberdelincuencia, posiblemente impulsado por un mayor reconocimiento de los delitos informáticos dentro del sistema de justicia y el fortalecimiento de las capacidades investigativas. No obstante, pese al crecimiento en el número de condenas, la cifra sigue siendo reducida en comparación con la cantidad de denuncias e investigaciones abiertas en el Ministerio Público, lo que sugiere la necesidad de fortalecer los procesos de prueba digital, agilizar la tramitación de casos y mejorar la formación de operadores de justicia en delitos tecnológicos. Este escenario resalta la importancia de seguir avanzando en la modernización del marco normativo y en la cooperación interinstitucional para garantizar que los delitos informáticos sean sancionados con mayor eficiencia y celeridad.

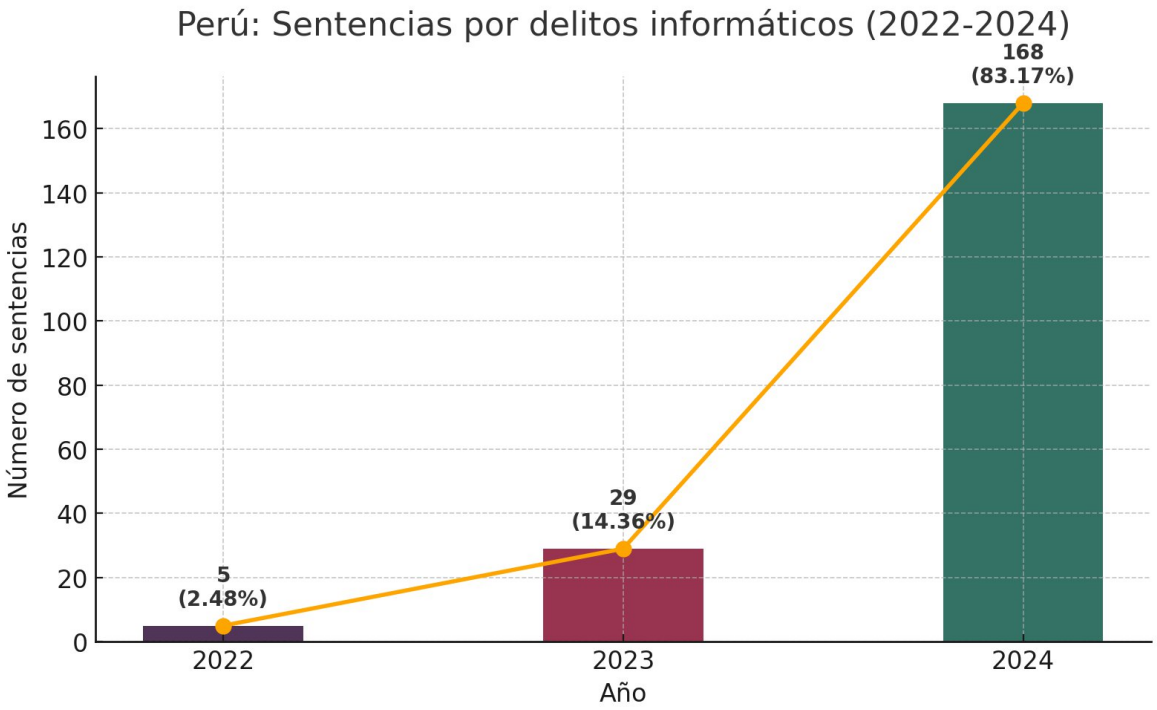


Grafico N° 3

Fuente. Cuadro 3

Elaboración propia

Interpretación:

La evolución de las sentencias condenatorias por delitos informáticos en Perú durante el período 2022-2024 refleja un crecimiento significativo en la aplicación de sanciones relacionadas con este tipo de crimen. En el año 2022, se registraron únicamente 5 sentencias condenatorias, lo que evidencia un bajo nivel de sanción en comparación con otros delitos. Sin embargo, en 2023, la cifra aumentó a 29 sentencias, lo que representa un incremento considerable en la persecución de estos delitos. Este crecimiento puede atribuirse a una mayor fiscalización, avances en la legislación y una mayor conciencia sobre la importancia de sancionar los delitos informáticos. Para el año 2024, se proyecta un aumento aún más pronunciado, con aproximadamente 168 sentencias estimadas, lo que representaría un 83.17% del total en los tres años analizados. Este incremento sugiere que las autoridades están fortaleciendo los mecanismos de detección y sanción de los delitos informáticos, lo que podría derivar en un impacto significativo en la ciberseguridad y la regulación digital en el país. En este contexto, resulta fundamental continuar con el monitoreo de esta tendencia y evaluar el impacto de las políticas implementadas en la lucha contra los delitos informáticos.

11.1.4. Línea de acción 17: Prevención de delitos informáticos

Cuadro N° 04

Plan de Acción Provincial de Seguridad Ciudadana 2024-2027 - Comité Provincial de Seguridad Ciudadana de la Provincia de Barranca - COPROSEC

	OBJETIVO ESTRATÉGICO 05: REDUCIR LOS DELITOS DE COMPLEJIDAD COMETIDOS POR BANDAS CRIMINALES QUE VICTIMIZA A LAPOBLACIÓN																						
	Actividades Estratégicas	Unidad de Medida	2024					2025					2026					2027					Responsable de la ejecución
			TRIM I	TRIM II	TRIM III	TRIM IV	ANUAL	TRIM I	TRIM II	TRIM III	TRIM IV	ANUAL	TRIM I	TRIM II	TRIM III	TRIM IV	ANUAL	TRIM I	TRIM II	TRIM III	TRIM IV	ANUAL	
	Línea de acción 16: Operativos para desarticular bandas criminales																						
51	Operaciones policiales de las comisarías para reducir los delitos y faltas. (bandas criminales)	Operativo policial	1	1	1	1	4	1	1	1	1	4	1	1	1	1	4	1	1	1	1	4	PNP/COMISARIA
52	Inteligencia táctica policial de unidades especializadas de la PNP para desarticular bandas criminales dedicadas al sicariato, proxenetismo, robo y extorsión	Operativo policial	1	1	1	1	4	1	1	1	1	4	1	1	1	1	4	1	1	1	1	4	PNP/DEPINCRI
	Línea de acción 17: Prevención de delitos informáticos																						
53	Gestionar la Implementación de acciones de sensibilización en redes sociales, medios de comunicación y otros canales de difusión con mensajes dirigidos a niños/as y adolescentespara prevenir el abuso sexual a través de internet u otros medios tecnológicos.	Informes	-	1	-	1	2	-	1	-	1	2	-	1	-	1	2	-	1	-	1	2	ST-COPROSEC
54	Difundir información relacionada a los delitos más comunes realizados por internet (sexting, grooming, extorsión, phishing, estafa en línea y otros) y orientación de los canales de denuncias.	Informes	-	1	-	1	2	-	1	-	1	2	-	1	-	1	2	-	1	-	1	2	ST-COPROSEC

Fuente: Secretaria Técnica de Seguridad Ciudadana de la Provincia de Barranca (2023)

Interpretación:

La difusión de información sobre los delitos más comunes cometidos a través de internet, tales como, phishing y fraude, constituye una estrategia fundamental en la prevención y mitigación del impacto de la ciberdelincuencia en la sociedad. En este sentido, la Línea de Acción 17 del COPROSEC de la Municipalidad Provincial de Barranca enfatiza en divulgar contenidos educativos y de orientación sobre los canales de denuncia disponibles, con el propósito de fortalecer la capacidad de respuesta de la población ante estos delitos. Esta iniciativa, planificada con una periodicidad semestral (dos informes anuales), contribuye a la generación de conciencia ciudadana y al empoderamiento de potenciales víctimas, facilitando su acceso a información veraz y mecanismos de protección. Asimismo, la implementación de esta estrategia incidirá positivamente en la reducción de la victimización digital, al incentivar el reconocimiento temprano de amenazas cibernéticas y promover la denuncia oportuna ante las autoridades competentes.

11. 2. Discusión

El presente estudio se centra en el análisis del phishing como un delito informático de creciente impacto en la sociedad, especialmente en el contexto peruano. Este fenómeno es relevante debido a su evolución constante y a la sofisticación de las tácticas utilizadas por los ciberdelincuentes, lo que exige una comprensión profunda para su prevención y control. El análisis de documentos especializados y antecedentes nacionales e internacionales respalda la necesidad de este estudio.

La línea de investigación se enmarca en el ámbito de la seguridad informática y el cibercrimen, enfocándose en las estrategias empleadas por los atacantes y las medidas de protección que pueden implementarse tanto a nivel personal como institucional.

El tema de estudio es el phishing, específicamente su desarrollo, impacto en la sociedad peruana y la ausencia de regulación específica que dificulta su prevención y sanción. La investigación aborda su evolución histórica, las tácticas utilizadas y las posibles estrategias de mitigación.

Este estudio es científicamente relevante ya que aborda una problemática actual que afecta no solo a individuos, sino también a empresas e instituciones financieras. Además, contribuye al entendimiento de las carencias legislativas en Perú y ofrece una base para futuras investigaciones y políticas públicas orientadas a fortalecer la ciberseguridad.

La metodología permitió examinar diversas perspectivas y enfoques sobre el phishing, tanto a nivel nacional como internacional. El enfoque cualitativo: Brindó un entendimiento profundo del fenómeno, identificando no solo sus implicancias técnicas, sino también sociales y legales, permitiendo contextualizar los hallazgos del estudio.

El análisis del phishing como fenómeno delictivo evidencia su naturaleza multifacética y las distintas formas en que se aborda en la literatura. Este balance se centra en integrar las contribuciones de los autores mencionados, destacando sus hallazgos, metodologías y perspectivas para establecer una visión completa del estado actual del conocimiento sobre el tema. Dado que la investigación es cualitativa, la

triangulación de información es esencial para conectar y contrastar los diferentes enfoques y niveles de análisis.

Vázquez, Hernández, César y Núñez (2023) analizaron el crecimiento del phishing mediante una metodología de análisis documental, combinando encuestas en línea para comprender cómo la desinformación genera víctimas masivas. Aunque el conocimiento público sobre el phishing ha mejorado, este estudio destaca que su crecimiento no es exponencial debido a una mayor concienciación. Sin embargo, el papel de la desinformación sigue siendo un desafío clave, algo que coincide con lo señalado por Hernández y Baluja (2021), quienes enfatizan que la educación digital puede disminuir ataques, pero su implementación es costosa. Estas perspectivas se complementan al identificar que, aunque la educación es crucial, los recursos económicos y la constancia en su implementación son barreras importantes.

Castillo (2021), en su tesis de maestría, contribuye desde un enfoque jurídico, diferenciando cibercrimen y delitos informáticos. Este autor resalta que el phishing no solo afecta bienes jurídicos concretos, sino que también representa un ámbito de oportunidad criminal que demanda políticas públicas. La perspectiva de Castillo añade un marco normativo a la discusión, destacando la importancia de proteger los derechos de los usuarios en el ciberespacio.

En el contexto peruano, los estudios ofrecen un análisis más detallado y localizado del phishing. Ruiz y Solis (2024) identificaron el uso de correos electrónicos fraudulentos y la suplantación de páginas web bancarias como las estrategias más comunes de los ciberdelincuentes. Este hallazgo es consistente con el análisis de Díaz y Goitia (2024), quienes enfatizan la urgencia de implementar programas de compliance en las instituciones financieras peruanas como una herramienta preventiva para proteger los datos de los usuarios y reducir los riesgos de phishing. Ambas investigaciones coinciden en que el sector financiero es especialmente vulnerable y requiere estrategias específicas de mitigación.

Carrero (2024) analiza la ausencia del phishing en la legislación peruana, subrayando que esta carencia limita la capacidad del sistema judicial para sancionar a los responsables. Este punto es respaldado por Nazario y Villanueva (2022), quienes

encontraron que la falta de normativas específicas generaba impunidad en casos de phishing, lo que afectaba significativamente a la sociedad. Estas investigaciones destacan la necesidad de reformas legislativas en el Perú, un enfoque que también es relevante en los contextos internacionales analizados.

Esparta (2022), en su estudio sobre el phishing en la sociedad peruana, añade una perspectiva técnica al identificar cómo las tácticas de los ciberdelincuentes, como la clonación de páginas web y los correos electrónicos maliciosos, inducen a los usuarios al error. Este análisis es consistente con los estudios de De la Cruz (2021) a nivel regional, quien identificó que las instituciones financieras no asumen responsabilidad en casos de phishing, lo que agrava la situación para las víctimas.

El estado del arte sobre el phishing detalla su evolución y las estrategias actuales de prevención. Ramos (2022) explica cómo el phishing ha evolucionado desde simples tácticas de ingeniería social en los años 90 hasta métodos sofisticados como el spear phishing y el uso de inteligencia artificial. Esta evolución es consistente con las preocupaciones expresadas por Hernández y Baluja (2021) sobre la constante adaptación de los ciberdelincuentes y la necesidad de mantenerse a la vanguardia en términos de prevención.

Por otro lado, Gutiérrez (2019) y Ortega (2024) destacan la importancia de la *autenticación biométrica* como una solución robusta para prevenir el phishing. Estos autores subrayan que las características biométricas, al ser únicas e intransferibles, dificultan los intentos de suplantación de identidad. Sin embargo, también advierten sobre los desafíos de privacidad asociados con el almacenamiento de datos biométricos, lo que sugiere la necesidad de un enfoque equilibrado entre seguridad y protección de datos.

La perspectiva legal también es abordada por Colex (2023), quien analiza la incorporación del phishing como delito tipificado en el Código Penal español. Este avance legislativo contrasta con la situación en Perú, donde, como señalan Carrero (2024) y Nazario y Villanueva (2022), la falta de regulación específica limita la capacidad de las autoridades para enfrentar este delito.

La triangulación cualitativa permite identificar convergencias y divergencias en la literatura: Convergencias: Todos los estudios coinciden en que el phishing se basa en tácticas de ingeniería social para manipular la confianza de las víctimas. Además, se resalta la importancia de la educación digital como una herramienta fundamental para prevenir ataques. En el ámbito jurídico, existe consenso sobre la necesidad de un marco normativo claro y específico para combatir el phishing. Por otra parte, las divergencias: se aprecia que a nivel internacional se observa un enfoque más avanzado en la implementación de tecnologías como la inteligencia artificial y la autenticación biométrica (Ramos, 2022; Gutiérrez, 2019), en Perú se prioriza el fortalecimiento del marco legislativo (Carrero, 2024; Nazario y Villanueva, 2022). Además, la percepción del phishing como un problema social versus un problema técnico varía según el contexto y los autores analizados.

El balance de los antecedentes y el estado del arte refleja la complejidad del phishing como fenómeno global y sus particularidades en el contexto peruano. La integración de enfoques legales, técnicos y educativos es clave para abordar este delito de manera integral. Si bien los avances internacionales en tecnología y legislación ofrecen modelos a seguir, las limitaciones en Perú, especialmente en términos legislativos y educativos, evidencian la necesidad de continuar fortaleciendo estas áreas. Este análisis resalta la importancia de adoptar medidas preventivas multidisciplinarias que combinen educación, legislación y tecnología para combatir el phishing de manera efectiva.

La consistencia en el uso de fuentes confiables y la aplicación rigurosa de la guía de análisis documental garantizan la validez interna del estudio. Además, la triangulación de información entre diferentes autores y enfoques refuerza la solidez de las conclusiones. Por otro lado, los resultados del estudio pueden extrapolarse a otros países con contextos similares al peruano, como México y Colombia, que enfrentan desafíos parecidos en términos de phishing y legislación. Sin embargo, deben considerarse las particularidades culturales y normativas al aplicar los hallazgos en otros escenarios.

La literatura existente revela avances significativos en la comprensión del phishing, pero también pone en evidencia lagunas importantes. Mientras que en países como España, el phishing está claramente tipificado en el Código Penal (Colex, 2023),

en Perú, investigaciones como la de Carrero (2024) muestran que esta modalidad delictiva no se encuentra explícitamente regulada, lo que limita la capacidad de las autoridades para combatirla eficazmente. Ademas, los estudios de Hernández y Baluja (2021) destacan la educación digital como una medida preventiva clave, aunque costosa, mientras que Díaz y Goitia (2024) subrayan la importancia de programas de compliance en el sector financiero. Esta diversidad de enfoques refleja la necesidad de un abordaje multidisciplinario que combine educación, tecnología y legislación.

El análisis de los datos proporcionados resalta un incremento significativo en los indicadores relacionados con los delitos informáticos en Perú entre los años 2022 y 2023, abarcando denuncias, casos ingresados a fiscalías y sentencias condenatorias. Este crecimiento se observa en tres niveles:

Denuncias Policiales: El aumento de denuncias por delitos informáticos pasó de 1,850 en 2022 a 2,125 en 2023, un incremento del 14.9%. Esta variación positiva refleja tanto un aumento en la incidencia de ciberdelitos como una mayor disposición de las víctimas para reportarlos.

Denuncias Ingresadas en Fiscalías: En el marco de la Ley N° 30096, los casos ingresados en las fiscalías provinciales crecieron de 19,064 a 29,580 entre 2022 y 2023, evidenciando un crecimiento alarmante del 55.2%. Este incremento es indicativo de la creciente actividad delictiva cibernética.

Sentencias Condenatorias: Las sentencias por delitos informáticos aumentaron de 5 en 2022 a 29 en 2023, lo que representa un crecimiento significativo, aunque limitado en comparación con la cantidad de denuncias.

Además, el comportamiento ascendente en estos indicadores puede explicarse por varios factores, entre ellos:

La expansión de la digitalización en actividades cotidianas, que aumenta la superficie de ataque para ciberdelitos.

Mayor conciencia de los ciudadanos sobre la importancia de denunciar este tipo de crímenes.

Avances en la capacidad institucional para procesar denuncias e identificar a los responsables.

Sin embargo, a pesar de los avances observados, el contraste entre las denuncias ingresadas y las sentencias condenatorias refleja la existencia de limitaciones en los sistemas de investigación, judicialización y sanción de los delitos informáticos. Esto pone de manifiesto la necesidad de reforzar las capacidades investigativas y de prueba digital dentro del sistema de justicia.

De igual modo se explica el crecimiento exponencial en los delitos informáticos responde a un contexto global de mayor sofisticación en las estrategias empleadas por los ciberdelincuentes, como phishing, fraude electrónico y suplantación de identidad. Las medidas de sensibilización, como las promovidas por la Línea de Acción 17 del COPROSEC, son fundamentales para educar a la población y reducir la victimización. La implementación de informes regulares, con contenidos educativos y de orientación, fomenta la confianza en las autoridades y fortalece la capacidad de denuncia.

Para el año 2024, las proyecciones estiman un aumento sostenido en los casos y sentencias, destacando la urgencia de políticas públicas orientadas a:

Modernizar la legislación en materia de ciberdelincuencia.

Promover la capacitación en ciberseguridad tanto en el sector público como en el privado.

Fortalecer la cooperación interinstitucional para mejorar la eficiencia en la persecución penal.

Este análisis evidencia que, aunque existen avances en la respuesta frente a los delitos informáticos, persisten desafíos críticos que deben ser abordados con

estrategias integrales para proteger a la población y mitigar el impacto de la criminalidad digital en la sociedad.

En consecuencia, este estudio subraya la urgencia de implementar políticas públicas que refuercen la ciberseguridad en Perú, incluyendo la educación digital, la actualización legislativa y la cooperación internacional. Además, destaca la importancia de integrar tecnologías avanzadas, como la autenticación biométrica, para prevenir ataques.

XII. CONCLUSIONES Y RECOMENDACIONES

12.1. Conclusiones

First. Del objetivo general. Se concluye, que la investigación permitió evidenciar que, aunque el phishing es una modalidad del fraude informático reconocida por su impacto creciente en la protección de datos personales, aún existen vacíos legales que limitan su regulación efectiva; por lo tanto, resulta fundamental establecer normativas específicas que tipifiquen este delito y fortalezcan las capacidades investigativas y sancionatorias del sistema de justicia. Asimismo, es crucial implementar estrategias educativas y de sensibilización para reducir la vulnerabilidad de la población frente a este tipo de cibercrimen, promoviendo así un entorno digital más seguro y confiable.

Second. Del objetivo específico 1. Se logró describir la regulación del phishing como modalidad de fraude informático en el Distrito de Barranca, identificando que la legislación actual, si bien aborda aspectos generales de los delitos informáticos, carece de disposiciones específicas que permitan enfrentar eficazmente este tipo de delito. Esta ausencia normativa genera vacíos legales que dificultan la persecución penal y aumentan la vulnerabilidad de los ciudadanos frente a la sustracción de datos personales y financieros. Por lo tanto, es imperativo actualizar el marco regulatorio, incluyendo el phishing como un delito claramente tipificado, a fin de garantizar una protección más efectiva de los datos personales y promover la seguridad digital en la región.

Third. En conclusión, al clasificar la determinación en la regulación del phishing para la protección de datos personales en el Distrito de Barranca, se evidenció que esta modalidad de fraude informático requiere un enfoque normativo que priorice la identificación de los bienes jurídicos vulnerados, como el patrimonio y la privacidad de las víctimas. Asimismo, se determinó que la falta de una regulación específica limita la capacidad de sancionar de manera efectiva estas conductas, lo que pone en riesgo la integridad de los datos personales. Por ende, es necesario fortalecer las disposiciones legales

existentes para garantizar una protección más integral y eficiente frente a las amenazas cibernéticas, incluso instrumentadas con IA[4].

[4] Inteligencia artificial

12.2. Recomendaciones

Al Congreso de la República

Aprobar un marco legal que permita atribuir responsabilidad a las personas naturales y/o jurídicas en el ámbito de los ciberdelitos, alineado con las disposiciones del artículo 12 del Convenio sobre Ciberdelincuencia del Consejo de Europa (ver anexo 3).

Implementar una normativa que garantice la conservación inmediata y segura de los almacenados en sistemas informáticos, conforme a las directrices establecidas en el artículo 29 del Convenio sobre Ciberdelincuencia del Consejo de Europa.

Al Ministerio de Relaciones Exteriores

Impulsar la adhesión, aprobación y ratificación por parte del Estado peruano de los dos protocolos adicionales del Convenio sobre Ciberdelincuencia del Consejo de Europa. Estos protocolos, adoptados en 2003 y 2022, abordan respectivamente la criminalización de conductas de carácter racista y xenófobo cometidas mediante sistemas informáticos y el fortalecimiento de la cooperación internacional, así como la mejora en la gestión y divulgación de pruebas electrónicas.

Al Ministerio de Transportes y Comunicaciones y otras interinstituciones

En el Perú, **ordenar y regular** el uso de la autenticación biométrica como medida de protección contra el phishing, por parte del Ministerio de Transportes y Comunicaciones (MTC) a través de la Dirección General de Políticas y Regulación en Comunicaciones, que establece lineamientos para la seguridad en comunicaciones digitales. Asimismo, el Ministerio de Justicia y Derechos Humanos, mediante la Autoridad Nacional de Protección de Datos Personales (ANPDP), tiene un rol clave en garantizar que las medidas relacionadas con la autenticación biométrica cumplan con la Ley N.° 29733, Ley de Protección de Datos Personales.

Además, entidades como la Superintendencia de Banca, Seguros y AFP (SBS) y el Banco Central de Reserva del Perú (BCRP), **emitir** disposiciones específicas para el sector financiero, promoviendo el uso de autenticación biométrica para prevenir fraudes como el phishing en operaciones bancarias y financieras. Su implementación también debe ser

coordinada con la Presidencia del Consejo de Ministros (PCM) a través de la Secretaría de Gobierno y Transformación Digital para garantizar su alineación con las políticas nacionales de transformación digital y ciberseguridad.

XIII. REFERENCIAS BIBLIOGRÁFICAS

Carrero Pérez, J. (2024). *Incorporación de la modalidad del Phishing en la Ley de Delitos Informáticos* [Tesis de pregrado, Universidad Católica Santo Toribio de Mogrovejo]. Repositorio USAT. http://hdl.handle.net/20.500.12423/7300

Castillo, O. (2021). *Phishing: Día de pesca*. [Tesis de maestría, Universidad Externado de Colombia]. https://doi.org/10.57998/bdigital.handle.001.4353

Colex. (2023). *La defensa frente al phishing: Guía práctica sobre el phishing y la defensa que frente al mismo ofrece nuestro ordenamiento jurídico*. Editorial Colex S.L.

Cortes, J., y Álvarez, S. (2017). *Manual de redacción de tesis jurídica*. Amate. https://sistemabibliotecario.scjn.gob.mx/sisbib/2018/000292104/000292104.pdf

De La Cruz, D. (2021). *Operaciones financiadas por internet y su relación con la responsabilidad civil de los bancos en la Provincia de Huaura - Huacho 2018*. [Tesis de pregrado, Universidad Nacional José Faustino Sánchez Carrión]. https://repositorio.unjfsc.edu.pe/bitstream/handle/20.500.14067/4960/DIEGO%20ALBERTO%20DE%20LA%20CRUZ%20S%C3%81NCHEZ.pdf?sequence=1

Defensoría del Pueblo. (2023). *Informe Defensorial N° 001-2023-DP/ADHPD: La ciberdelincuencia en el Perú: Estrategias y retos del Estado*. https://cdn.www.gob.pe/uploads/document/file/4557288/INFORME%20DEF%20001-2023-DP-ADHPD%20-%20Ciberdelincuencia.pdf?v=1684168103

Díaz Pari, A., & Goitia Cárdenas, S. (2024). *El delito de phishing en las entidades financieras del Perú* [Trabajo de investigación, Universidad Autónoma del Perú]. Repositorio UAP. https://hdl.handle.net/20.500.13067/3416

Esparta, C. (2022). *Mecanismos de prevención y protección del bien jurídico tutelado frente a la modalidad delictiva Phishing en el ordenamiento jurídico penal peruano*. [Tesis de pregrado, Universidad Inca Garcilaso de la Vega]. http://repositorio.uigv.edu.pe/handle/20.500.11818/6595

Garrido, K. (2021). *Modificación de la ley 30096 para incorporar los delitos de Phishing, Pharming y Carding como delitos penalizables con prisión, para reducir la ciberdelincuencia, Lima 2029*. [Tesis de pregrado, Universidad Señor de Sipán]. https://repositorio.uss.cdu.pe/handlc/20.500.12802/8345

Gavancho, O. (2015). El derecho a la protección de datos personales en el ámbito del procedimiento administrativo sancionador. *Actualidad Jurídica*, (264). Editorial el Búho E.I. R. L.

Gutiérrez, P. (2019). *El libro blanco del Hacker*, (2° ed.). https://books.google.es/books?hl=es&lr=lang_es&id=m8-4EAAAQBAJ&oi=fnd&pg=PT7&dq=libros+phishing+gratis&ots=j4H1uFPw6U&sig=82xj0RQYZNr1-RlmIqre45uz5OM#v=onepage&q=libros%20phishing%20gratis&f=false

Hernández, A., & Baluja, W. (2021). Principales mecanismos para el enfrentamiento al phishing en las redes de datos. *Revista Cubana de Ciencias Informáticas*, 15, 413-441. https://www.redalyc.org/articulo.oa?id=378370462024

Hernández, R., y Mendoza, C. (2018). *Metodología de la investigación. Las rutas cuantitativa, cualitativa y mixta*. McGraw-Hill Interamericana Editores S.A. http://repositorio.uasb.edu.bo:8080/handle/54000/1292

Hidalgo, C. y Solano G. (2021). *El Phishing como conducta delictiva no regulada en el ordenamiento jurídico peruano. Propuesta de incorporación del artículo 7-A en la ley de delitos informáticos 30096*. [Tesis de pregrado, Universidad Nacional del Santa]. https://repositorio.uns.edu.pe/bitstream/handle/20.500.14278/3849/52376.pdf?sequence=1&isAllowed=y

Instituto Nacional de Estadística e Informática-INEI. (2023). *Anuario estadístico de la criminalidad y seguridad ciudadana 2019-2023*. https://cdn.www.gob.pe/uploads/document/file/7512284/6389092-peru-anuario-estadistico-de-la-criminalidad-y-seguridad-ciudadana-2019-2023.pdf?v=1737393934

Nazario Delgado, N., & Villanueva Sánchez, L. (2022). *Fraude informático en la modalidad de phishing y la necesaria actualización de la legislación para una eficiente persecución y sanción penal* [Tesis de pregrado, Universidad Señor de Sipán]. Repositorio USS. https://repositorio.uss.edu.pe/handle/20.500.12802/10002

Ortega, J. (2024). *Ciberseguridad: Manual Práctico*. Ecoe Ediciones. https://books.google.es/books?hl=es&lr=lang_es&id=oWT7EAAAQBAJ&oi=fnd&pg=PA1&dq=libros+phishing+gratis&ots=Bb6l-CQxLc&sig=2COZJvPlPGEYUv-aB5NQlWYbCS4#v=onepage&q&f=false

Ramos, J. (2022). *Como protegerte del phishing evita que te roben tu información*. Verlag GD Publishing Ltd.& Co KG, Berlin. https://www.google.com.pe/books/edition/C%C3%B3mo_protegerte_del_phishing/0kaFEAAAQBAJ?hl=es&gbpv=1&dq=phishing+libros&printsec=frontcover

Rosas, G. (2014). Los delitos informáticos y la búsqueda de pruebas de cargo a la luz del Código Procesal Penal de 2004. *Actualidad Jurídica*, (253). Editorial el Búho E.I. R. L.

Ruiz, P., & Solis, J. (2024). Fraude informático en la modalidad de phishing en Lima. *Revista Escpogra PNP* , *3* (2), 143–155. https://doi.org/10.59956/escpograpnpv3n2.12

Secretaria Técnica de Seguridad Ciudadana. (2023). *Plan de Acción Provincial de Seguridad Ciudadana 2024-2027–COPROSEC Barranca*. https://www.munibarranca.gob.pe/codisec/views/listaPlan.php

Universidad Nacional de Barranca. (2016). *Código de Ética para la Investigación*, aprobado con Resolución de Comisión Organizadora N° 573-2016-CO-UNAB.

Vázquez, M., Hernández, W., Cesar, O., & Núñez, B. (2023). El análisis del crecimiento de phishing en los últimos años. *Revista Digital De Tecnologías Informáticas Y Sistemas*, *6* (1), 7. https://doi.org/10.61530/redtis.2022.6.6.132.7

Vesga, P. (2024). *Delitos informáticos y la vulneración al derecho a la intimidad personal en la Provincia de Barranca, 2023*. [Tesis de pregrado, Universidad Nacional José Faustino Sánchez Carrión]. http://hdl.handle.net/20.500.14067/8991

Zegarra, A. (2015). La informática como medio delictivo y como objeto material en la cibercriminalidad. *Actualidad Jurídica*, (263). Editorial el Búho E.I. R. L.

XIV. ANEXOS

Anexo 01: Matriz de consistencia

TÍTULO	PROBLEMA	OBJETIVO	HIPÓTESIS	CATEGORÍAS	METODOLOGÍA
Determinación regulativa del phishing como modalidad del fraude informático para protección de datos en el Distrito de Barranca, 2022-2023	**Problema general** ¿Para qué determinar la regulación del phishing como modalidad del fraude informático en la protección de datos en el Distrito de Barranca, 2022-2023? **Problemas específicos** **Pe.1.** ¿Cómo, determinar la regulación del phishing en la modalidad de fraude informático en el Distrito de Barranca, 2022-2023? **Pe.2.** ¿Qué regular en el phishing para la protección de datos personales en el Distrito de Barranca, 2022-2023?	**Objetivo general** Analizar la determinación de la regulación del phishing como modalidad del fraude informático en la protección de datos en el Distrito de Barranca, 2022-2023 **Objetivos específicos** **Oe.1.** Describir la regulación del phishing en la modalidad de fraude informático en el Distrito de Barranca, 2022-2023 **Oe.2.** Clasificar la determinación en la regulación del phishing para la protección de datos personales en el Distrito de Barranca, 2022-2023	**Hipótesis general** La determinación de la regulación del phishing como modalidad de fraude informático protege los datos personales en el Distrito de Barranca, 2022-2023 **He.1.** La regulación en el Código Penal del phishing en la modalidad de fraude informático, si se protege los datos personales en el Distrito de Barranca, 2022-2023 **He.2.** Determinando el bien jurídico económico, social y jurídico en la regulación del phishing, se protege los datos personales en el Distrito de Barranca, 2022-2023	**Categoría X:** - Determinación phishing, e - Regulación phishing **Categoría Y:** - Fraude informático, e - Protección de datos	**1.** Tipo de investigación: por su finalidad básica y alcance descriptivo **2.** Diseño de investigación: no experimental, y transversal. **3.** Enfoque de la investigación: cualitativo. **4.** Población: Acervo documentario especializado en phishing. **5.** Muestra: Documentales de revistas, libros, encuesta INEI, informes PNP. **6.** Técnica: análisis documental. **7.** Instrumento: guía de análisis documental.

Fuente: Los autores

Anexo 02: Guía de análisis de documentos

INSTRUMENTO: GUÍA DE ANÁLISIS DE DOCUMENTOS

Objetivo: Analizar documentos relacionados con la regulación del phishing y la protección de datos en el Distrito de Barranca durante 2022-2023, identificando normativas, vacíos legales, medidas implementadas y fundamentos teóricos relevantes.

Criterios de Análisis	Preguntas Orientadoras	Respuestas/Observaciones
1. Identificación del documento	- ¿Cuál es el título del documento?	
	- ¿Qué institución o autor lo elaboró?	
	- ¿Cuál es la fecha de publicación?	
2. Relevancia del contenido	- ¿El documento aborda el phishing como modalidad de fraude informático?	
	- ¿Se mencionan normativas específicas sobre delitos informáticos o protección de datos?	
	- ¿Incluye datos estadísticos relevantes sobre la incidencia del phishing?	
3. Fundamentos teóricos y doctrinas	- ¿Qué definiciones de phishing o delitos informáticos se incluyen?	
	- ¿Se citan doctrinas o enfoques teóricos sobre la regulación del phishing?	
	- ¿Existen referencias a convenios internacionales o legislaciones extranjeras?	
4. Aspectos normativos	- ¿Qué leyes o regulaciones nacionales o internacionales se mencionan en el documento?	
	- ¿Existen vacíos legales identificados relacionados con el phishing?	
	- ¿El documento propone recomendaciones legislativas?	
5. Aspectos de implementación	- ¿El documento describe acciones concretas realizadas para combatir el phishing?	
	- ¿Se mencionan mecanismos para la protección de datos personales?	

	- ¿Incluye estrategias de prevención implementadas en otros países?	
6. Impacto y resultados esperados	- ¿Qué impacto se menciona en la regulación del phishing para la protección de datos personales?	
	- ¿El documento sugiere indicadores de éxito o medición del impacto de las medidas propuestas?	
	- ¿Incluye recomendaciones basadas en estudios de casos o evaluaciones previas?	
7. Observaciones adicionales	- ¿Hay información relevante no contemplada en los criterios anteriores?	

Elaboración propia

Instrucciones de Uso:

1. Completa la tabla con base en cada documento analizado.
2. Registra observaciones claras y precisas para cada criterio.
3. Organiza los resultados en el capítulo correspondiente de tu tesis.

Anexo 03: Anteproyecto de ley

ANTEPROYECTO DE LEY

LEY PARA LA PREVENCIÓN, SANCIÓN Y ERRADICACIÓN DEL PHISHING EN PERÚ

Exposición de Motivos

El avance de la digitalización ha facilitado el desarrollo de nuevas tecnologías y el acceso a servicios en línea; sin embargo, también ha incrementado los delitos informáticos, entre los cuales el phishing se ha convertido en una de las amenazas más recurrentes. Actualmente, la legislación peruana carece de un marco normativo específico que regule y sancione de manera efectiva este tipo de fraude informático, lo que genera vacíos legales que limitan la capacidad de las autoridades para perseguir y castigar a los responsables. Este anteproyecto tiene como finalidad llenar dichas lagunas normativas mediante la tipificación clara del phishing, el establecimiento de sanciones proporcionales y la creación de mecanismos preventivos y educativos para mitigar su impacto en la sociedad.

TÍTULO I: DISPOSICIONES GENERALES

Artículo 1. Objeto de la Ley

La presente Ley tiene por objeto prevenir, sancionar y erradicar el delito de phishing en el territorio nacional, estableciendo medidas específicas para su regulación y castigo, así como estrategias de concienciación y protección de los ciudadanos en entornos digitales.

Artículo 2. Ámbito de Aplicación

Las disposiciones de la presente Ley son aplicables a cualquier persona natural o jurídica, nacional o extranjera, que realice actividades ilícitas relacionadas con el phishing en perjuicio de ciudadanos, empresas o entidades del Estado peruano.

Artículo 3. Definición del Phishing

Se considera phishing a cualquier maniobra fraudulenta realizada a través de medios electrónicos, digitales o de telecomunicaciones con el propósito de engañar a una persona para obtener información confidencial, credenciales de acceso, datos financieros u otra información sensible, utilizando identidades falsas, correos electrónicos fraudulentos, sitios web apócrifos o cualquier otro medio digital engañoso.

TÍTULO II: DELITOS Y SANCIONES

Artículo 4. Tipificación del Delito de Phishing

Se incorpora a la Ley N° 30096, Ley de Delitos Informáticos, el siguiente texto como artículo 8-B:

"El que, mediante el uso de medios electrónicos, digitales o tecnológicos, simule ser una entidad legítima con el fin de inducir a error a una persona y obtener, sustraer o utilizar sin autorización sus datos personales, bancarios o financieros será reprimido con pena privativa de libertad no menor de cuatro (4) ni mayor de ocho (8) años y con 180 a 365 días multa."

Cuando la conducta descrita en el párrafo anterior incluya la suplantación de interfaces o páginas web, se aplicará la misma pena prevista en el artículo 8 de la presente ley."

Artículo 5. Agravantes

La pena privativa de libertad será no menor de ocho (8) ni mayor de doce (12) años cuando:

a) El delito sea cometido en perjuicio de menores de edad, adultos mayores o personas en situación de vulnerabilidad.

b) Se utilicen datos obtenidos ilícitamente para la comisión de otros delitos como estafa, fraude financiero o robo de identidad.

c) Se cause daño económico significativo, determinado en base a los montos fijados por la Superintendencia de Banca, Seguros y AFP (SBS).

d) El delito sea cometido por una organización criminal.

TÍTULO III: MEDIDAS PREVENTIVAS Y MECANISMOS DE PROTECCIÓN

Artículo 6. Responsabilidades de las Entidades Financieras y Empresas de Tecnología

Las entidades financieras y empresas tecnológicas que brinden servicios de comunicación digital deberán:

a) Implementar sistemas de autenticación robusta para prevenir accesos no autorizados.

b) Desarrollar campañas educativas dirigidas a sus clientes sobre los riesgos y prevención del phishing.

c) Reportar de manera inmediata a la Autoridad Nacional de Protección de Datos Personales cualquier incidente de seguridad relacionado con este delito.

Artículo 7. Creación de la Unidad Especializada en Ciberdelincuencia

El Ministerio del Interior creará una Unidad Especializada en Ciberdelincuencia con competencia para investigar, perseguir y sancionar delitos de phishing y otras formas de fraude digital.

Artículo 8. Plataforma Nacional de Denuncias Digitales

Se implementará una Plataforma Nacional de Denuncias Digitales a cargo de la Policía Nacional del Perú, en la cual los ciudadanos podrán reportar de manera segura y eficiente cualquier intento de phishing.

TÍTULO IV: COSTO-BENEFICIO SOCIAL

Artículo 9. Evaluación del Costo-Beneficio Social

La implementación de la presente Ley tendrá un impacto positivo en la sociedad al fortalecer la seguridad digital, reducir las pérdidas económicas derivadas de fraudes informáticos y mejorar la confianza de los ciudadanos en el uso de tecnologías digitales. Si bien la creación de unidades especializadas y plataformas digitales implica costos iniciales para el Estado, estos se justifican ampliamente por los beneficios tangibles e intangibles generados, como:

Prevención de daños económicos: La reducción de casos de phishing disminuirá significativamente las pérdidas financieras de ciudadanos y empresas, estimadas en millones de soles anuales.

Fortalecimiento institucional: La creación de la Unidad Especializada en Ciberdelincuencia y la Plataforma Nacional de Denuncias Digitales contribuirá a modernizar y hacer más eficiente la persecución penal de delitos informáticos.

Impacto social positivo: Las campañas educativas generarán mayor conciencia pública sobre los riesgos del phishing, empoderando a los ciudadanos para proteger su información.

Incremento de la confianza digital: La aplicación de la Ley fortalecerá la confianza de los ciudadanos y las empresas en las transacciones digitales, fomentando el crecimiento económico.

En conclusión, el costo inicial de implementación de esta Ley es marginal en comparación con los beneficios de largo plazo en la protección de los derechos de los ciudadanos y la estabilidad económica del país.

DISPOSICIONES COMPLEMENTARIAS FINALES

Primera. Adecuación del Código Penal y otras Normas

El Poder Ejecutivo, en un plazo no mayor de seis (6) meses desde la publicación de la presente Ley, adecuará las normas complementarias necesarias para su efectiva implementación.

Segunda. Campañas de Sensibilización

El Ministerio de Justicia y Derechos Humanos, en coordinación con el Ministerio de Transportes y Comunicaciones y la Autoridad Nacional de Protección de Datos Personales, desarrollará campañas masivas de sensibilización sobre los riesgos del phishing y las medidas de prevención.

Tercera. Cooperación Internacional

El Estado peruano fomentará la cooperación internacional con organismos especializados en ciberseguridad para el intercambio de información y mejores prácticas en la lucha contra el phishing y otros delitos informáticos.

DISPOSICIÓN FINAL

La presente Ley entrará en vigencia al día siguiente de su publicación en el Diario Oficial El Peruano.

Dado en la ciudad de Lima, a los ___ días del mes de _____ del año 2025.