**FACULTAD DE POSTGRADO**
**TRABAJO FINAL DE GRADUACIÓN**

# PHISHING Y ROBO DE IDENTIDAD EN HONDURAS: UN ANALISIS DE LA EFICACIA DE LA REPUESTA DEL SISTEMA JUDICIAL PENAL


**SUSTENTADO POR:**

**JUAN FRANCISCO REYES CERNA**


**PREVIA INVESTIDURA AL TÍTULO DE**

**PREGRADO EN DERECHO EMPRESARIAL**


**TEGUCIGALPA, FRANCISCO MORAZAN, HONDURAS, C.A.**

**JULIO, 2025**

# FACULTAD DE DERECHO

# PHISHING Y ROBO DE IDENTIDAD EN HONDURAS: UN ANALISIS DE LA EFICACIA DE LA REPUESTA DEL SISTEMA JUDICIAL PENAL


## JUAN FRANCISCO REYES
## CERNA



**Resumen**

El presente informe analiza la problemática del phishing de datos en Honduras, una amenaza cibernética que ha crecido en los últimos años debido al aumento del uso de tecnologías digitales y la falta de educación en ciberseguridad. El phishing es una técnica de fraude en la que los ciberdelincuentes engañan a los usuarios para que revelen información confidencial, como contraseñas, datos bancarios y documentos personales.

La investigación se centra en identificar los métodos más utilizados por los atacantes, evaluar el nivel de conocimiento de la población sobre este tipo de fraude y proponer estrategias para mitigar sus efectos. Mediante encuestas y entrevistas con expertos en ciberseguridad, se determinó que un alto porcentaje de usuarios en Honduras es vulnerable a ataques de phishing debido a la falta de medidas preventivas y la poca capacitación en seguridad digital.

Entre los hallazgos más relevantes, se identificó que los correos electrónicos fraudulentos, los enlaces maliciosos y las páginas web falsas son las principales herramientas utilizadas para engañar a los usuarios. Asimismo, se evidenció que muchas empresas y entidades gubernamentales no cuentan con protocolos adecuados para prevenir estos ataques, lo que expone tanto a individuos como a organizaciones a riesgos significativos.

Como parte de la solución, se recomienda la implementación de campañas de concienciación, el fortalecimiento de la legislación en ciberseguridad y la adopción de tecnologías avanzadas de protección contra fraudes electrónicos. La educación digital y la capacitación constante en buenas prácticas de seguridad son claves para reducir el impacto del phishing en el país.

Este estudio busca generar conciencia sobre la importancia de la protección de los datos personales y financieros, promoviendo acciones concretas para mejorar la seguridad en el entorno digital de Honduras.

**Palabras claves:** Phishing, Ingeniería Social, Ciberdelito, Marco Legal, Protección de Datos, Ciberseguridad.

R

# GRADUATE SCHOOL

# INSERTE AQUÍ TÍTULO DEL TRABAJO

**JUAN FRANCISCO REYES CERNA**

**Abstract**

This report analyzes the issue of data phishing in Honduras, a cyber threat that has increased in recent years due to the rise in digital technology use and the lack of cybersecurity education. Phishing is a fraud technique where cybercriminals deceive users into revealing confidential information, such as passwords, bank details, and personal documents.

The research focuses on identifying the most common methods used by attackers, assessing the population's level of awareness about this type of fraud, and proposing strategies to mitigate its effects. Through surveys and interviews with cybersecurity experts, it was determined that a high percentage of users in Honduras are vulnerable to phishing attacks due to the lack of preventive measures and limited digital security training.

Among the most relevant findings, it was identified that fraudulent emails, malicious links, and fake websites are the main tools used to deceive users. It was also revealed that many companies and government entities lack proper protocols to prevent these attacks, exposing both individuals and organizations to significant risks.

As part of the solution, the implementation of awareness campaigns, the strengthening of cybersecurity legislation, and the adoption of advanced protection technologies against electronic fraud are recommended. Digital education and ongoing training in security best practices are key to reducing the impact of phishing in the country.

This study seeks to raise awareness about the importance of protecting personal and financial data, promoting concrete actions to enhance digital security in Honduras.

**Key word:** Phishing, Social Engineering, Cybercrime, Legal Framework, Data Protection, Cybersecurit

# DEDICATORIA

Dedico este trabajo de tesis, primeramente, a Dios cuyo amor y guía me han sostenido en cada paso de este camino, permitiéndome superar estos desafíos y alcanzar mis metas. A mis padres, por su incondicional apoyo, ejemplo de esfuerzos y valores y por inspirarme a dar siempre lo mejor de mí. A mis hermanos por su compañía y motivación constante, y a mi sobrino y sobrina quienes representan una fuente de alegría y motivación para seguir adelante. De manera especial a mi novia por su amor incondicional, comprensión y aliento inagotable, quien siempre me ha motivado a luchar por mis sueños y a nunca conformarme hasta alcanzar mi máximo potencial.

A todos ustedes, mi más profundo agradecimiento por estar presentes en cada etapa de este viaje.

# AGRADECIMIENTO

A lo largo de la realización de este proyecto, he conocido con el apoyo incondicional de personas valiosas que han sido fundamentales para alcanzar este importante logro académico. En primer lugar, agradezco profundamente a mis padres cuyo amor, guía, y esfuerzo inquebrantable me ha permitido llegar hasta aquí. Gracias por enseñarme el valor del esfuerzo, la perseverancia, y el compromiso.

A mi novia por su comprensión, motivación constante, y por estar a mi lado en cada paso de este camino, brindándome ánimo, y confianza incluso en los momentos más desafiantes. Extiendo mi más sincero agradecimiento a todas las personas que participaron en mi investigación, respondieron a la encuesta ya que sus opiniones y experiencia fueron esenciales para obtener resultados relevantes y enriquecedores para este estudio.

También expreso mi gratitud a los integrantes de las tres instituciones, que compartieron su tiempo, conocimientos y experiencias durante la entrevista de investigación, contribuyendo de manera invaluable el desarrollo del proyecto.

A todos ustedes, mi agradecimiento por haber posibilitado la culminación de este trabajo, que es el reflejo del esfuerzo conjunto y del aporte de cada uno. OBJ

# ÍNDICE DE CONTENIDO

DEDICATORIA ..... vi
AGRADECIMIENTO ..... vii
ÍNDICE DE CONTENIDO ..... vii
CAPÍTULO I. PLANTEAMIENTO DE LA INVESTIGACIÓN ..... 2
1.1 INTRODUCCIÓN ..... 1
1.2 ANTECEDENTES DEL PROBLEMA ..... 2
1.3 DEFINICIÓN DEL PROBLEMA ..... 5
1.4 OBJETIVOS DEL PROYECTO ..... 9

1.5 JUSTIFICACIÓN ..... 11
CAPÍTULO II. MARCO TEÓRICO ..... 14
2.3 TEORÍAS DE SUSTENTO ..... 29
2.3.1 BASES TEÓRICAS ..... 30
CAPÍTULO III. METODOLOGÍA ..... 54
3.2 ENFOQUE Y MÉTODOS ..... 56
3.3 DISEÑO DE LA INVESTIGACIÓN ..... 57
CAPÍTULO IV. RESULTADOS Y ANÁLISIS ..... 65
CAPÍTULO V. CONCLUSIONES Y RECOMENDACIONES ..... 84
5.1 CONCLUSIONES ..... 84
CAPÍTULO VI. DISCUSION Y CONCLUSION ..... 92
REFERENCIAS BIBLIOGRÁFICAS ..... 98
ANEXOS ..... 101

## ÍNDICE DE FIGURAS

ANTECEDENTES HISTORICO ..... 16
ESTADISTICAS DE MAXIMO HISTORICOS ..... 17
ESTADISTICAS DE ATAQUES DE PHISHING ..... 18
CAPÍTULO I. PLANTEAMIENTO DE LA INVESTIGACIÓN ..... 2
FIGURA 4 ..... 20
FIGURA 5 ..... 20
FIGURA6 ..... 21
FIGURA7 ..... 22
FIGURA 8 ..... 23
FIGURA9 ..... 24
FIGURA10 ..... 27
FIGURA11 ..... 29
FIGURA 12 ..... 65
FIGURA13 ..... 66
FIGURA14 ..... 67
FIGURA 15 ..... 65

FIGURA 16……69
FIGURA 17..... 70
FIGURA 18..... 71
FIGURA 19..... 71
FIGURA 20..... 72

## ÍNDICE DE TABLAS

TABLA 1 ..... 55
TABLA 2 ……...56

## INTRODUCCIÓN

El acelerado crecimiento de las tecnologías digitales en Honduras ha transformado la manera en que los ciudadanos interactúan, realizan transacciones y gestionan su información personal. Esta expansión tecnológica ha aumentado alarmantemente en cibercrímenes, como el phishing de datos, una modalidad de fraude digital que busca engañar a los usuarios para obtener información confidencial, como credenciales bancarias, contraseñas y datos personales. La falta de un marco legal robusto y actualizado, junto con una infraestructura de ciberseguridad limitada, ha dejado a la población hondureña altamente vulnerable ante estos ataques.

Este proyecto de investigación analiza el problema del phishing en Honduras, desglosando sus modalidades más frecuentes, las estrategias empleadas por los cibercriminales y las deficiencias normativas que dificultan la persecución de estos delitos. Con la aplicación de métodos cuantitativos y cualitativos, se ha logrado identificar la percepción ciudadana sobre la ciberseguridad y la incapacidad del sistema de justicia penal para responder eficazmente ante el incremento de estos fraudes. Los resultados obtenidos evidencian no solo la vulnerabilidad tecnológica de las instituciones y los ciudadanos, sino también la pérdida de confianza en las autoridades encargadas de proteger la integridad digital del país.

La investigación propone un enfoque integral para contrarrestar el phishing de datos en Honduras, sustentado en tres pilares clave: la modernización del marco jurídico, la creación de organismos especializados en delitos cibernéticos, y la implementación de programas educativos masivos para la concienciación ciudadana.

Basándose en modelos internacionales exitosos, como el Convenio de Budapest, y adaptándolos al contexto hondureño, se plantean reformas concretas para fortalecer la prevención, detección y sanción del phishing. Además, se resalta la importancia de fomentar la cooperación internacional y regional para mejorar la capacidad de rastrear y desmantelar redes de ciberdelincuentes que operan más allá de las fronteras nacionales.

Este proyecto de investigación analiza el problema del phishing en Honduras, desglosando sus modalidades más frecuentes, las estrategias empleadas por los cibercriminales y las deficiencias normativas que dificultan la persecución de estos delitos. Con la aplicación de métodos cuantitativos y cualitativos, se ha logrado identificar la percepción ciudadana sobre la ciberseguridad y la incapacidad del sistema de justicia penal para responder eficazmente ante el

incremento de estos fraudes. Los resultados obtenidos evidencian no solo la vulnerabilidad tecnológica de las instituciones y los ciudadanos, sino también la pérdida de confianza en las autoridades encargadas de proteger la integridad digital del país.

La investigación propone un enfoque integral para contrarrestar el phishing de datos en Honduras, sustentado en tres pilares clave: la modernización del marco jurídico, la creación de organismos especializados en delitos cibernéticos, y la implementación de programas educativos masivos para la concienciación ciudadana.

Basándose en modelos internacionales exitosos, como el Convenio de Budapest, y adaptándolos al contexto hondureño, se plantean reformas concretas para fortalecer la prevención, detección y sanción del phishing. Además, se resalta la importancia de fomentar la cooperación internacional y regional para mejorar la capacidad de rastrear y desmantelar redes de ciberdelincuentes que operan más allá de las fronteras nacionales.

Este estudio no solo busca proporcionar soluciones técnicas y jurídicas para combatir el phishing, sino también promover una transformación cultural hacia una sociedad digital más informada, resiliente y protegida. La implementación de estas propuestas permitirá a Honduras avanzar hacia un entorno cibernético más seguro y confiable, donde la privacidad y la protección de los datos personales sean derechos garantizados y defendidos de manera efectiva.

# CAPÍTULO I. PLANTEAMIENTO DE LA INVESTIGACIÓN

## 1.1 ANTECEDENTES DEL PROBLEMA

En los últimos años, Honduras ha sido testigo de un aumento significativo en los ciberataques, siendo el phishing una de las modalidades más frecuentes y perjudiciales. Según un reportaje de La Prensa solo en el año 2023 se registraron más de 1.8 millones de ciberataques en el país, cifra que evidencia una creciente amenaza a la seguridad digital. (La Prensa, 2024, enero 12, Ciber ataques a Honduras superaron 1.8 millones en 2023.)

De estos ataques, una parte considerable corresponde al robo de datos personales a través de técnicas de suplantación de identidad digital, generando pérdidas económicas millonarias tanto para ciudadanos como para instituciones financieras. Incidentes de Ciberseguridad: Durante 2023, se registraron aproximadamente 1.8 millones de ciberataques dirigidos a empresas e instituciones hondureñas, siendo el phishing una de las amenazas más comunes. (La Prensa,2024, enero 12,

Ciberataques a Honduras superaron 1.8 millones en 2023.)

Pérdidas Económicas: Estudios de la Comisión Económica para América Latina y el Caribe (CEPAL) estiman que los ciberataques le cuestan a Honduras alrededor de 150 millones de dólares anuales. (PenTesting Latam. (s.f.). Ciberseguridad en Honduras: retos y avances.)

Fraudes Bancarios: La Comisión Nacional de Bancos y Seguros (CNBS) ha registrado más de 300 reclamos por fraudes en cuentas bancarias, con pérdidas que superan los 400 millones de lempiras. (HCH. (2023, marzo 29). Bancos deben responder: Más de 300 reclamos por fraude a cuentas bancarias registra la CNBS.)

Vulnerabilidad Institucional: Las instituciones públicas son susceptibles por infraestructuras tecnológicas obsoletas y falta de políticas de seguridad cibernética robustas. (Telemás. (2024, agosto 12). Ciberataques en Honduras: 1.8 millones de incidentes en 2023.)

El país aún carece de registros estadísticos públicos sistemáticos por parte de entidades como la Policía Cibernética, lo que limita la posibilidad de dimensionar con precisión el daño total causado por estos delitos.

Actualmente, el fenómeno del phishing se encuentra en una fase de expansión y sofisticación creciente. Esta evolución se manifiesta no solo en la diversidad de métodos utilizados (correos electrónicos, mensajes SMS, llamadas telefónicas automatizadas), sino también en su capacidad para vulnerar sistemas financieros, académicos y gubernamentales. No obstante, el ordenamiento jurídico hondureño no ha evolucionado con la misma celeridad. El Código Penal (Decreto 130-2017), aunque incorpora algunos tipos penales relacionados con delitos informáticos, no incluye una tipificación específica del phishing ni contempla figuras como el uso indebido de identidades digitales, la captación fraudulenta de datos personales o el acceso ilegítimo a credenciales digitales.

La falta de una legislación especializada y actualizada en materia de ciberseguridad y protección de datos impide una respuesta efectiva del Estado. Las víctimas de phishing, por tanto, enfrentan enormes obstáculos para lograr justicia, ya que no existe un marco legal que defina con claridad los mecanismos de investigación, reparación o sanción frente a este delito. Esto afecta directamente el ejercicio de derechos fundamentales como la privacidad, la identidad y la seguridad jurídica, consagrados en la Constitución de la República de Honduras (1982, arts. 76 y

100).

En el ámbito de la ciencia jurídica, esta problemática expone una desconexión entre el avance tecnológico y la aplicación del derecho. La falta de formación técnica de los operadores jurídicos, como los jueces, fiscales, defensores públicos, limita la correcta calificación de estos delitos y obstaculiza la labor probatoria en los procesos penales. Así, la carencia de conocimientos tecnológicos incide directamente en la ineficiencia del sistema judicial para perseguir y sancionar el phishing.

Históricamente, Honduras ha intentado abordar aspectos parciales de esta problemática a través de leyes como la Ley sobre Firma Electrónica (Decreto 149-2013), la ley de Comercio Electrónico (Decreto 243-2011) y la Ley de Protección de Datos Personales (Decreto 41-2021). No obstante, estas normativas resultan limitadas frente a los desafíos actuales. Por ejemplo, la Ley de Protección de Datos no establece procedimientos de reacción inmediata ante incidentes de robo de datos, ni contempla sanciones penales por suplantación digital. Tampoco se ha creado una autoridad de control independiente con funciones claras de supervisión, sanción o apoyo técnico.

Esta ausencia de un enfoque integral deja a la ciudadanía hondureña en una situación de vulnerabilidad digital constante. Los avances tecnológicos, que deberían ser herramientas para el desarrollo, se convierten en vehículos de amenaza cuando el Estado no garantiza un entorno seguro para su uso. La confianza en servicios digitales, desde la banca hasta la educación en línea, se erosiona cada vez que una víctima de phishing queda sin protección legal ni reparación efectiva.

A futuro, si el marco legal no se reforma de manera estructural, el país enfrentará un deterioro mayor en la protección de los derechos digitales y en la gobernanza de internet. Las experiencias de países como México, Argentina y Chile, que ya han promulgado leyes específicas de ciberseguridad y de protección de datos personales con enfoque sancionatorio y preventivo, demuestran que es posible construir sistemas jurídicos adaptados al entorno digital. En este sentido, Honduras requiere con urgencia una respuesta jurídica coherente, especializada y multidisciplinaria, que incluya reformas legislativas, capacitación técnica del personal judicial, cooperación internacional, y el fortalecimiento de las instituciones encargadas de velar por la seguridad informática.

El análisis de la realidad hondureña respecto al phishing evidencia una insuficiencia estructural del marco legal vigente para hacer frente a los desafíos que impone la ciberdelincuencia

moderna. Si bien existen normas relacionadas con la firma electrónica, el comercio digital y la protección de datos personales, ninguna de estas leyes aborda de forma específica y eficaz el delito de suplantación de identidad digital o el robo de datos mediante engaños tecnológicos, lo que deja vacíos normativos sustanciales en la tipificación penal y en la tutela efectiva de los derechos fundamentales.

Desde el punto de vista del derecho penal, la ausencia de una figura legal concreta que sancione el phishing impide a las autoridades judiciales perseguir y castigar con claridad estas conductas, lo que conlleva una impunidad sistemática para los responsables. A nivel procesal, la falta de formación técnica de los operadores del sistema de justicia, así como la carencia de protocolos de investigación digital, agrava aún más la situación, limitando el acceso a la justicia de las víctimas y vulnerando derechos constitucionales como la intimidad, el habeas data y la protección de la identidad.

Asimismo, el contexto evidencia la urgente necesidad de adecuar el marco normativo nacional a los estándares internacionales, tal como lo recomiendan instrumentos como el Convenio de Budapest sobre la Ciberdelincuencia (2001) o los principios establecidos por la Red Iberoamericana de Protección de Datos. La falta de armonización con estas normativas internacionales no solo limita la cooperación transfronteriza, sino que impide una respuesta integral y moderna frente a un fenómeno transnacional y en constante evolución.

En consecuencia, el Estado hondureño tiene la obligación jurídica y constitucional de actualizar su legislación penal, fortalecer las capacidades institucionales y adoptar un enfoque interinstitucional que permita prevenir, sancionar y reparar las violaciones derivadas del phishing. Esta reforma no solo es necesaria para proteger a los ciudadanos en el entorno digital, sino también para garantizar la eficacia del derecho como instrumento de justicia en el siglo XXI.

## 1.2 FORMULACION DEL PROBLEMA

### 1.2.1Problema general

A pesar del avance digital que ha experimentado Honduras en la última década, el país enfrenta una seria deficiencia jurídica en la protección contra delitos cibernéticos, especialmente el phishing. Si bien el Código Penal (Decreto No. 130-2017) tipifica algunos delitos informáticos, su ambigüedad frente a la suplantación de identidad digital y la captación fraudulenta de datos personales impide una respuesta penal adecuada ante estos fenómenos, generando zonas de

impunidad y dificultando la reparación integral del daño para las víctimas (Congreso Nacional, 2017, Decreto No. 130-2017: Código Penal de Honduras Diario Oficial La Gaceta.)

Además, aunque la Constitución de la República reconoce derechos fundamentales como la intimidad personal (art. 76) y la inviolabilidad de las comunicaciones (art. 100), tales garantías no cuentan con un respaldo normativo secundario eficaz que las proteja en entornos digitales. Esta ausencia normativa limita la exigibilidad de estos derechos ante delitos como el phishing, ampliando la brecha entre el derecho formal y su aplicación práctica (Constitución de la República de Honduras, 1982).

En contraste, estos son los países con menores antecedentes de phishing de datos en el mundo, Finlandia, Estonia, Suiza, Japón Singapur. Leyes específicas de estas nacionalidades que regulan el phishing son las siguientes: Finlandia Criminal Code of Finland, Sección 38 – delitos informáticos Estonia Cybersecurity Act y Penal Code (artículos sobre fraude y acceso ilegal) Suiza Swiss Criminal Code, Art. 143 y 147 (fraude digital y acceso indebido) Japón Act on the Prohibition of Unauthorized Computer Access Singapur Computer Misuse and Cybersecurity Act.

Estos países consistentemente reportan bajos niveles de phishing según informes de la Interpol, Europol, ITU (Unión Internacional de Telecomunicaciones) y Kaspersky.

¿Cuáles son las raíces de la efectividad de estos países para mantenerse fuera del radar internacional de este ciberdelito?

**Leyes claras y específicas:** No hay ambigüedad: cada delito digital tiene una definición, pena y procedimiento claro. Infraestructura digital protegida: Gobiernos y empresas invierten mucho en sistemas seguros y actualizados.

**Educación pública constante:** La gente sabe cómo detectar correos falsos, sitios clonados y alertas sospechosas. Respuesta rápida y profesional: Equipos como CERTs (Computer Emergency Response Teams) están siempre listos para actuar. Justicia eficaz: Los fiscales y jueces tienen formación en delitos digitales y actúan sin retrasos ni corrupción.

**Cooperación internacional activa:** países como Argentina han promulgado leyes como la Ley 25.326 de Protección de Datos Personales, que establece principios, sanciones y una autoridad de aplicación especializada (Agencia de Acceso a la Información Pública). México cuenta con la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y el

Reglamento del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), mientras que Chile ha avanzado con la Ley N.º 19.628 sobre Protección de la Vida Privada y trabaja en una ley de ciberseguridad con estándares internacionales (Open Net América Latina, 2021; INAI, 2020).

En contraste, Honduras se mantiene rezagada, lo cual debilita su capacidad de respuesta frente a amenazas digitales transnacionales. Asimismo, la falta de recursos institucionales de información pública y accesible sobre el phishing, como campañas educativas oficiales, estadísticas centralizadas y plataformas de denuncia digital, así como la carencia de recursos humanos especializados, constituye un obstáculo estructural. Se requiere la creación de entidades como un Centro Nacional de Ciberseguridad con una Unidad de Alerta y Respuesta Temprana dedicada al monitoreo y gestión de incidentes digitales, además de contar con personal técnico altamente capacitado: ingenieros en seguridad informática, analistas forenses digitales, criminólogos especializados en delitos tecnológicos, fiscales digitales y juristas con formación en derecho penal tecnológico. Este tipo de estructuras se observan en países como Colombia con su colCERT y en México con CERT.mx, donde se combinan capacidades tecnológicas, legales y de inteligencia para responder a ciber amenazas. (Open Net América Latina, 2021).

Este entorno de inseguridad digital compromete no solo la privacidad y los derechos de los ciudadanos, sino que también debilita la confianza en las plataformas tecnológicas y frena el crecimiento de sectores estratégicos como la banca digital y el comercio electrónico. La ausencia de una respuesta jurídica y técnica integral frente al phishing afecta directamente la legitimidad del Estado como garante de derechos en el entorno digital.

Por tanto, se vuelve urgente revisar críticamente el marco legal hondureño, identificar sus principales vacíos en relación con la protección frente al phishing y proponer soluciones jurídicas integrales que incluyan reformas legislativas, inversión tecnológica y cooperación regional, a fin de construir un entorno digital más seguro, inclusivo y confiable para la ciudadanía hondureña.

## 1.3 PREGUNTAS DE INVESTIGACION

Las siguientes preguntas de investigación derivan directamente del problema general

formulado y buscan desglosar los elementos centrales de la problemática jurídica del phishing en Honduras. Su desarrollo permitirá identificar el alcance del fenómeno, las falencias normativas y las posibles soluciones institucionales y legislativas viables, dentro del marco de una investigación de enfoque jurídico comparado.

A. ¿Qué tipos de cibercrímenes son más frecuentes en Honduras?

   Esta pregunta busca establecer un diagnóstico del panorama actual de los delitos informáticos en el país, con énfasis en el phishing como una modalidad creciente. La respuesta a esta interrogante permitirá contextualizar la gravedad del problema jurídico que representa el phishing dentro de una realidad más amplia de criminalidad digital.

B. ¿Cuáles son las tipologías y modalidades de phishing utilizadas a nivel global y en Honduras?

   Esta pregunta permite comprender el nivel de sofisticación técnica con el que se ejecuta el phishing, tanto a nivel global como nacional, lo cual es fundamental para determinar si el marco legal hondureño actual en particular el Código Penal contempla o no mecanismos adecuados para abordarlo. (Congreso Nacional, 2017). Al analizar las diversas formas que adopta el phishing (por correo electrónico, SMS, redes sociales, suplantación institucional, etc.), se podrá demostrar que la legislación vigente carece de tipificaciones claras, lo cual deja vacíos legales aprovechados por los cibercriminales. (Open Net América Latina, Estado de la ciberseguridad y protección de datos en América Latina. 2021). Esta falta de precisión normativa representa un obstáculo para la persecución penal y la reparación del daño sufrido por las víctimas.

   C. ¿Cuáles son las principales deficiencias del actual marco legal hondureño en comparación con legislaciones más avanzadas en la lucha contra el phishing de datos?

   Esta interrogante constituye el núcleo jurídico de la investigación. Al comparar el marco legal hondureño con normativas más avanzadas, como la Ley de Protección de Datos Personales de Argentina, la Ley Federal de Protección de Datos Personales en Posesión de los Particulares de México o la Ley de Delitos Informáticos de Chile, se podrá evidenciar el rezago normativo del país. En Honduras, aunque el Código Penal (Congreso Nacional, 2017) y la Constitución (1982) establecen principios generales de

protección de la intimidad y las comunicaciones, no existen leyes secundarias específicas en materia de ciberseguridad ni una autoridad nacional de protección de datos personales. Según Open Net América Latina (2021), esta situación coloca a Honduras en una posición de vulnerabilidad jurídica y técnica frente al phishing, dificultando incluso la cooperación internacional en la lucha contra este delito. (Constitución de la República de Honduras. (1982). Constitución de la República de Honduras, Diario Oficial La Gaceta.

## 1.4 OBJETIVOS DE LA INVESTIGACION

### 1.4.1. General

Analizar el problema del phishing de datos en Honduras, identificando sus tipos más frecuentes, las estrategias de los cibercriminales, las deficiencias del marco legal vigente y las oportunidades de mejora, para proponer estrategias legislativas, tecnológicas y de cooperación interinstitucional que contribuyan a reducir este delito en el país.

El objetivo general busca analizar integralmente la problemática del phishing, considerando aspectos técnicos, sociales y jurídicos. Este análisis se encuentra amparado por:

El Artículo 76 y 100 de la Constitución de la República, que garantizan la protección de la intimidad, la imagen, el honor y el secreto de las comunicaciones, sirviendo de base para el reconocimiento del derecho a la privacidad digital en el contexto moderno del cibercrimen.

El Código Penal (Decreto No. 130-2017), específicamente los artículos del 398 al 404, que sancionan el acceso no autorizado, los daños a sistemas, la suplantación de identidad y el abuso de dispositivos, configurando el marco legal vigente frente a delitos informáticos como el phishing.

La Ley de Protección al Consumidor, en sus artículos 9, 48 y 58, que protege los derechos de los usuarios frente a prácticas fraudulentas digitales y transacciones electrónicas engañosas.

La Ley de Firma Electrónica (Decreto 149-2013), que aborda la autenticidad y fiabilidad de las firmas digitales, un aspecto frecuentemente vulnerado en ataques de spear phishing.

### 1.4.2 Específicos

**A.** Identificar y analizar los tipos de cibercrímenes más frecuentes en Honduras,

determinando su impacto en la seguridad digital y evaluando los factores que contribuyen a su proliferación, con el fin de proponer estrategias de prevención y mitigación.

Relación con el Objetivo Específico A:

El Título XXII del Código Penal, que tipifica conductas delictivas relacionadas con la seguridad informática, permite clasificar y evaluar los delitos más comunes en el país, entre ellos el phishing.

La Constitución, en su Art. 100, también permite comprender el impacto de estos delitos sobre los derechos fundamentales de los ciudadanos, como la inviolabilidad de sus datos personales y de sus comunicaciones.

Examinar las estrategias y métodos utilizados por los cibercriminales para ejecutar ataques de phishing en el mundo, y como Honduras se ve afectada ante esta realidad en la actualidad, identificando sus principales técnicas, plataformas de ataque y el nivel de vulnerabilidad de los usuarios, con el propósito de proponer medidas de prevención y concienciación.

**B.** Analizar las principales deficiencias del marco legal hondureño en la lucha contra el phishing de datos, comparándolo con legislaciones más avanzadas a nivel internacional, con el fin de identificar vacíos normativos y proponer mejoras para una regulación más efectiva.

**C**. Proponer estrategias legislativas, tecnológicas y de cooperación interinstitucional que puedan implementarse en Honduras para reducir la incidencia del phishing de datos en los próximos años, tomando como referencia modelos exitosos a nivel internacional y adaptándolos al contexto nacional.

Relación con el Objetivo Específico C:

La ausencia de una ley específica de protección de datos personales y de un marco normativo integral sobre ciberseguridad limita la capacidad del país para enfrentar eficazmente delitos como el phishing.

• La existencia de una ley de ciberseguridad limitada a redes sociales (Ley de Estrategia de Ciberseguridad Nacional de Prevención de Campañas de Odio y Discriminación en Redes Sociales) evidencia la necesidad de revisar y ampliar el marco legal vigente.

• El Decreto 170-2006 (Ley de Transparencia y Acceso a la Información Pública), aunque establece el derecho de los ciudadanos a conocer el uso de sus datos, no protege adecuadamente la privacidad digital ni contempla mecanismos sancionatorios frente al uso indebido de esa información.

• Proponer estrategias legislativas, tecnológicas y de cooperación interinstitucional que puedan implementarse en Honduras para reducir la incidencia del phishing de datos en los próximos años, tomando como referencia modelos exitosos a nivel internacional y adaptándolos al contexto nacional.

Relación con el Objetivo Específico D

•La responsabilidad de las personas jurídicas establecida en el Artículo 403 del Código Penal permite sugerir estrategias para obligar a las empresas a implementar medidas más estrictas de ciberseguridad.

• El Comité Interinstitucional de Ciberseguridad, la CONATEL y el Instituto de Acceso a la Información Pública (IAIP), aunque aún con deficiencias, pueden ser fortalecidos mediante reformas legislativas que integren una estrategia nacional de ciberseguridad inclusiva y efectiva. • La comparación con marcos normativos internacionales y la necesidad de establecer mecanismos de cooperación regional también encuentra sustento en el Artículo 404 del Código Penal, que contempla la jurisdicción extraterritorial frente a delitos cibernéticos.

## 1.5 JUSTIFICACION

El phishing de datos constituye una de las formas de ciberdelito con mayor crecimiento en Honduras. En el contexto de una transformación digital acelerada, los ciberdelincuentes han perfeccionado sus estrategias para suplantar identidades y engañar a los usuarios, con el objetivo de obtener información confidencial como credenciales bancarias, datos personales y accesos a sistemas privados. Esta amenaza se agrava en el país debido a múltiples factores: una baja cultura de ciberseguridad, la debilidad de las infraestructuras tecnológicas, y sobre todo, la falta de un marco legal actualizado y efectivo para combatir estos delitos.

A nivel internacional, los delitos informáticos especialmente el phishing representan una amenaza creciente que afecta tanto a individuos como a empresas, gobiernos e instituciones financieras. En Honduras, esta realidad se ha manifestado en el aumento de fraudes electrónicos,

robos de identidad y pérdida de información confidencial. Además, el avance reciente de tecnologías como la inteligencia artificial ha facilitado la elaboración de correos electrónicos, mensajes de texto y sitios web falsos con una apariencia cada vez más convincente, lo que incrementa la sofisticación de los ataques y disminuye la capacidad de los usuarios para identificarlos.

Desde el punto de vista jurídico, si bien Honduras ha incluido algunas disposiciones sobre delitos informáticos en su Código Penal y ha creado instrumentos como el Comité Interinstitucional de Ciberseguridad y la Ley de Firma Electrónica, aún persisten vacíos normativos importantes. El país carece de una ley de protección de datos personales, de una regulación específica contra el phishing, y de una estrategia nacional integral de ciberseguridad. Esta debilidad legal, unida a la limitada aplicación de la normativa existente, deja a los ciudadanos en situación de vulnerabilidad frente a delitos digitales en constante evolución.

Por ello, esta investigación resulta social, jurídica y tecnológicamente pertinente. A nivel social, contribuirá a la protección de ciudadanos, consumidores y empresas al ofrecer información clara sobre cómo opera el phishing, qué consecuencias puede tener y cómo prevenirlo. A nivel jurídico, aportará una base de análisis comparativo que permitirá identificar mejoras normativas tomando como referencia modelos internacionales exitosos.

Desde el punto de vista tecnológico, analizará el uso de herramientas y estrategias de prevención que pueden adoptar el Estado y el sector privado para reducir la incidencia de estos delitos en el país.

El estudio también será de utilidad para legisladores, reguladores, entidades bancarias, instituciones educativas y organismos de seguridad, al ofrecer recomendaciones prácticas y aplicables para fortalecer la normativa nacional y promover una mayor articulación interinstitucional en materia de ciberseguridad. Asimismo, permitirá fomentar una mayor conciencia ciudadana sobre la importancia de la protección digital y la necesidad de adoptar buenas prácticas en el uso de tecnologías de la información.

Desde el punto de vista metodológico, la investigación adoptará un enfoque comparativo y analítico, contrastando la situación de Honduras con la de países que han implementado políticas eficaces para enfrentar el phishing, como España, Chile o Estonia.

Se utilizarán fuentes normativas, doctrinales y jurisprudenciales, así como datos empíricos y estudios de caso nacionales, para comprender la magnitud del problema y formular propuestas contextualizadas. En términos disciplinares, el estudio contribuirá a la literatura emergente sobre ciberseguridad y derecho digital en Honduras, y establecerá un marco de referencia para futuras investigaciones, proyectos legislativos y políticas públicas en el área.

# CAPÍTULO II. MARCO TEÓRICO

## 2.1 CONCEPTUALIZACION DEL PHSHING

¿Qué es el Phishing?

El phishing se refiere al hurto de información personal mediante sitios web engañosos. La persona afectada por este robo se dirige a esta página engañosa, en la que se le pide proporcionar sus datos para verificar su identidad. En ese momento ocurre el hurto, ya que, al proporcionar sus datos, los guarda y usa el hacker encargado de tal ataque para comercializarlos o ingresarlos a las instituciones y realizar hurtos o fraudes. (Andrés Eduardo Moncada, 2020, p.1)

Un artículo colombiano donde se llevó a cabo una investigación para describir que técnicas se han utilizado para atacar a las empresas e instituciones de la región colombiana en el año 2022, nos señala que el Phishing se define en las normas NIST 800-12 Rev. 1 (Guía sobre la gestión de la seguridad de la información, que ayuda a las organizaciones a comprender y aplicar controles de seguridad efectivos para proteger sus sistemas y datos) y en la RFC 4949 Ver2, (Documento técnico titulado "Internet Security Glossary, Versión 2", publicado por la Internet Engineering Task Force (IETF) en agosto de 2007, donde su propósito es proporcionar una recopilación estandarizada de términos y definiciones relacionados con la seguridad en redes e informática.) como una técnica de ingeniería social en la que se intenta adquirir datos confidenciales de las personas, mediante el engaño a través de una solicitud fraudulenta por correo electrónico o por un sitio web, donde el perpetrador busca dar apariencia de legalidad simulando ser el negocio legitimo o ser una persona de confianza o de buena reputación.

### 2.1.2 Tipos de Phishing

Correo Electrónico de Phishing: Es la forma más común. Los atacantes se hacen pasar por una empresa o entidad confiable (bancos, redes sociales, etc.) para engañar al destinatario, en el que se un envía un enlace o se adjunta un archivo malicioso que contiene programa maligno. María Fernanda (Sánchez Negrín). 2024, pág. 28)

• Spear Phishing: Esta variante se enfoca en un objetivo específico, como un empleado de una empresa, investigándolo antes del ataque con el objetivo de utilizar la información personalizada haciendo el ataque más creíble. María Fernanda (Sánchez Negrín). 2024, pág. 28)

• Whaling: Es un tipo de spear phishing que se dirige a personas de alto perfil dentro de

una organización, como directivos o ejecutivos (denominados "whales"). María Fernanda (Sánchez Negrín). 2024, pág. 28)

• Pharming: Está compuesto por los términos “phishing” y “Pharming,”. Contiene códigos maliciosos o sitios web falsos, en la que, a través de la navegación de las víctimas, el atacante infecta el DNS y lo modifica para que el usuario entre a sitios maliciosos en vez de sitios legítimos y así robar la información. María Fernanda (Sánchez Negrín). 2024, pág. 28)

• Vishing y Smishing: El vishing es un tipo de estafa de ingeniería social, en la que se realiza a través de llamadas telefónicas, suplantando la identidad de la víctima, mientras que el smishing usa mensajes de texto a través de un dispositivo móvil, con el objetivo de a las víctimas.

### 2.1.3 Ejemplos de Phishing:

**Fraudes de Soporte Técnico:** Mensajes que aparentan ser de soporte técnico de grandes compañías, solicitando información confidencial o acceso remoto a los dispositivos.

• Correos Electrónicos Falsificados: Ataques como el de "Business Email Compromise" (BEC), en el que los atacantes se hacen pasar por un ejecutivo de una empresa para solicitar transferencias bancarias. Análisis de la situación actual. María Fernanda (Sánchez Negrín). 2024, pág. 28).

### 2.1.4 Clasificación de los ataques de Phishing

De acuerdo con el servicio al que se dirigen:

•Cajas y bancos

• Plataformas de pago online

• Plataformas sociales

• Páginas de anuncios de compraventa o licitaciones

• Juegos online

• Asistencia Técnica / Mesas de apoyo • Guardado en la nube / Almacenamiento virtual

• Organismos o entidades públicas

• Servicios de envío de mensajes

• Falsa y oportunas ofertas laborales (Ciencia y Tecnología. 2020. 13(1):97-104)

### 2.1.5 Métodos más habituales de Phishing

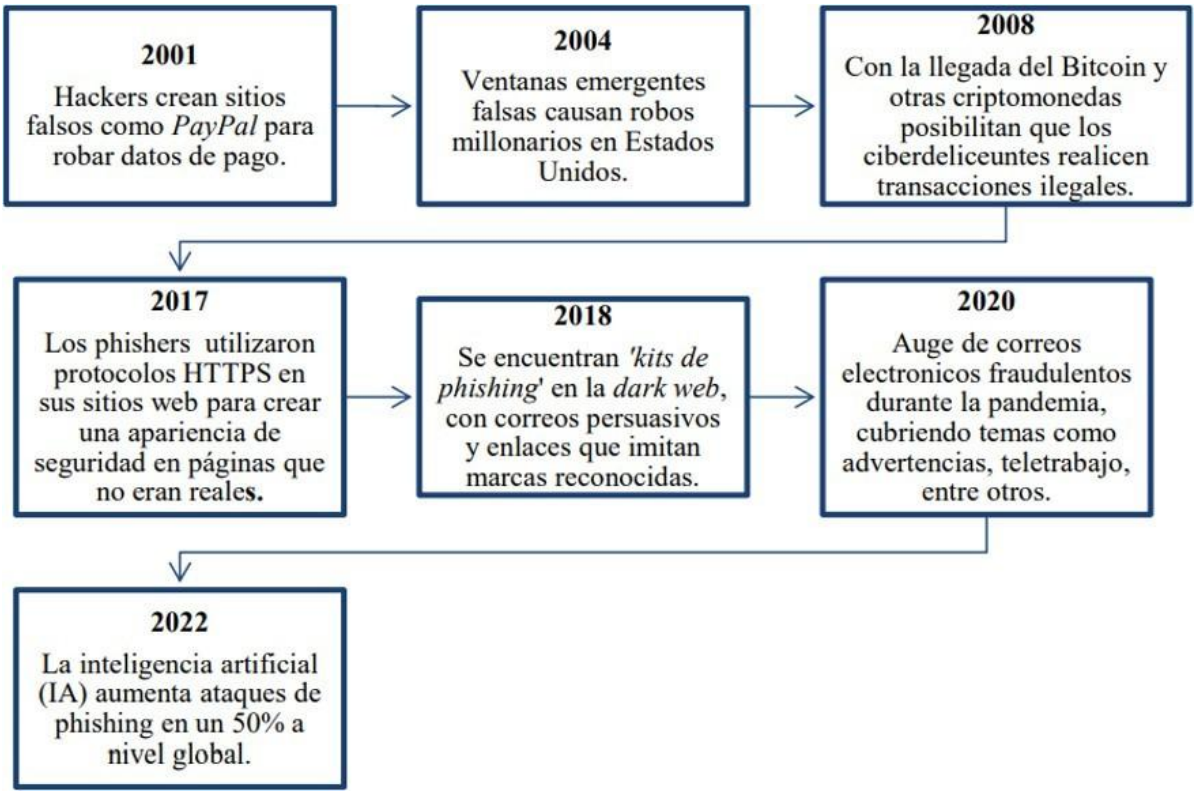
•Correos electrónicos de phishing:

• Anuncios engañosos acerca de premios que exigen proporcionar información privada. Páginas web de phishing: Páginas alteradas parecidas a las auténticas. URL alteradas:

• Ejemplo: http://www.nombredetubancoCE.com (con la letra "CE" insertada)

• Implementación de caracteres específicos, como el carácter @, para evitar confusiones (por ejemplo, http://www.google.com@members.tripod.com).

## 2.2 ANTECEDENTES HISTORICOS




(Gonzales, 2024)

### 2.2.1 Figura 1. Evolución del Phishing

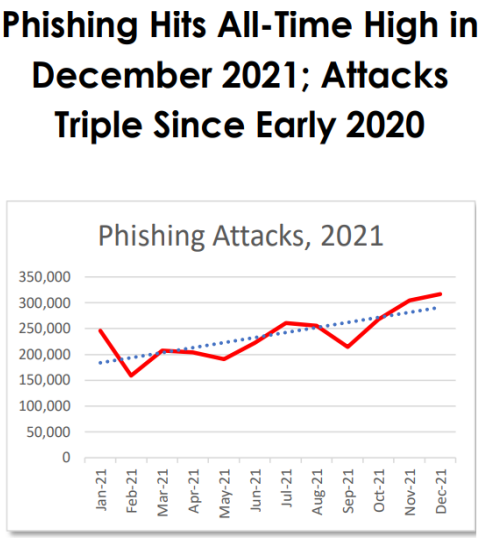
En España, para el 2023, se registró que el 67% de las compañías privadas dentro del sector internacional, fueron víctimas de un ataque de phishing.

En América Latina, las naciones más impactadas hasta ahora han sido Brasil con 134 millones de intentos de phishing, México (43 millones), y Perú (31,5 millones), Colombia (30,9

millones), Ecuador (12,2 millones) y Argentina (9,4 millones). Entre los cuales, los casos de phishing se dirigieron específicamente a datos financieros (Un 42,8% - 28,40% temas bancarios, 9,40% medios de pago y 2,70% servicios financieros).

En 2024, en la región de Perú se contabilizaron 1 millón de nuevos intentos de este delito. (Diaz Pari, A. C. C., & Goitia Cárdenas, 2024, pág. 9)

Un informe de tendencias de actividad del phishing realizado por la APWG (Anti- Phishing Working Group) que en español se traduce como Grupo de trabajo Anti-Phishing, publicado el 23 de febrero del 2022, expuso que los ataques de phishing alcanzaron un máximo histórico en 2021, con más de 300.000 ataques registrados en diciembre en ese año. (Cook, S. (2023, enero 16). Estadísticas y datos sobre el phishing para 2019–2022. Comparitech.)



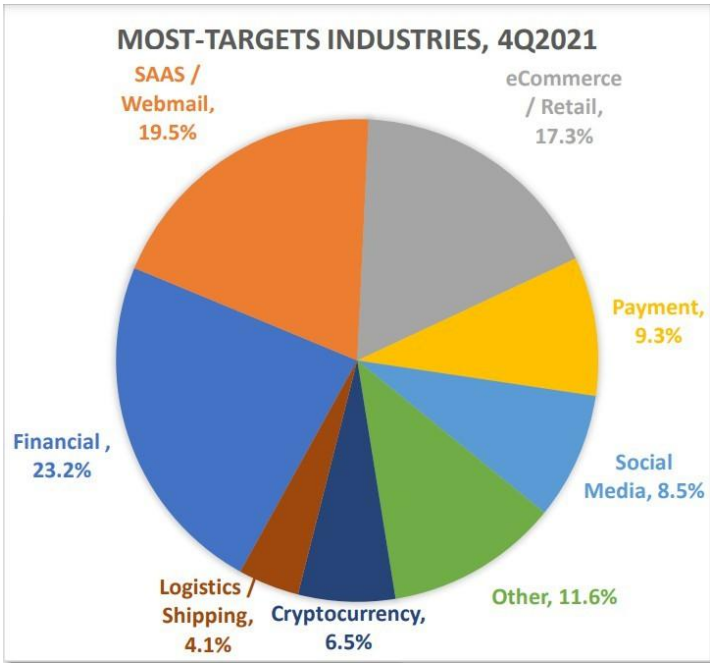

**2.2.2 Figura 2. Estadísticas de máximos históricos del Phishing en 2021**

(Cook, S. (2023, enero 16). Estadísticas y datos sobre el phishing para 2019–2022. Comparitech.)

Durante el cuarto trimestre de 2021, OpSec Security, reveló que los ataques de phishing dirigidos al sector financiero que comprende a los bancos se transformaron en la mayor cantidad de ataques, constituyendo el 23.2 por ciento de todos los ataques de phishing. (Diaz Pari, A. C. C., & Goitia Cárdenas, 2024, pág. 9)

El resto de los ataques se dividió en contra de los proveedores de correo web y el software como servicio (SaaS), donde tuvieron una reducción del 29.1% de todos los ataques en el tercer

trimestre al 19.5 por ciento en el cuarto. El reporte de 2021 también subraya un aumento en la tendencia de ataques de phishing contra compañías de criptomonedas. Estos ataques actualmente constituyen el 6,5 % del total. Todo esto evidencia cómo las organizaciones de ciberdelincuentes modifican sus acciones para lograr las metas más rentables posibles. (APWG Report, 2021)




**2.2.3 Figura 3. Estadísticas de ataques de phishing en los sectores Financieros, registrados en 2021. ((Cook, S. (2023, enero 16). Estadísticas y datos sobre el phishing para 2019–2022. Comparitech.)**

A medidas que nuestras vidas se vuelven cada vez más digitales, las posibilidades de ser víctimas de algún tipo de ciberdelito, específicamente el phishing de datos no deja

de aumentar.

Para esto Surfshark, una de las compañías de servicios de VPN más populares y creada por OpSec Security, la empresa líder en combatir la falsificación y proteger la propiedad intelectual de más de 400 propietarios de marcas a nivel mundial, ha alertado sobre esta amenaza social a través de un estudio global de 5 estadísticas basadas en datos del 2021 llamado ¨El Cybercrime Statics¨, con el propósito de concientizar y arrojar luz sobre el panorama de la ciberdelincuencia a

nivel mundial, para que la sociedad pueda entender de manera más cercana, el panorama completo de la delincuencia en Internet.

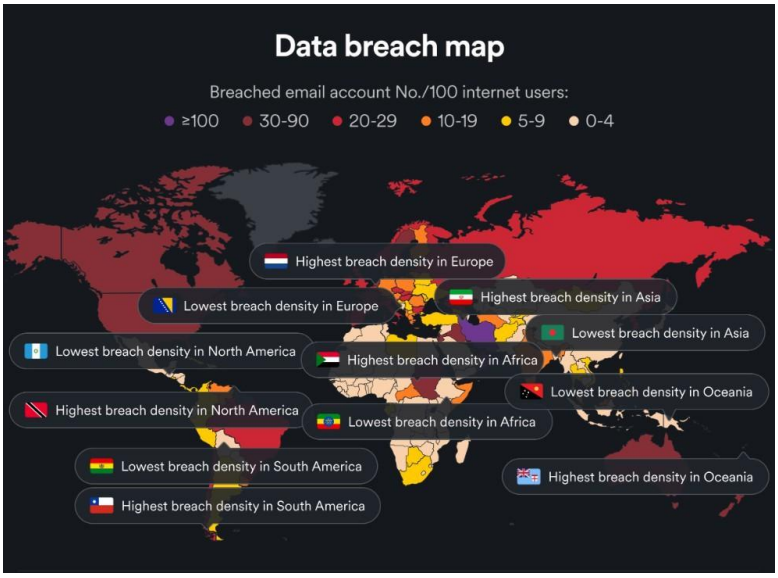
Primero: La compañía menciono que los objetivos de los ciberdelitos no son aleatorios, y que la mayoría de las personas que los sufren es porque las Organizaciones han filtrado previamente sus datos, brindándole la oportunidad a los hackers de realizar sus certeros ciberataques. (Silvia Montes, Escudo Digital, Ciberseguridad, 2022) (Montes, S. (2022, mayo 17),

Segundo: este articulo nos muestra que el mapa de violación de datos a nivel mundial ha clasificado a los países en seis grupos según las cuentas de correo electrónico vulneradas por cada 100 usuarios (densidad de vulneración) y no ha incluido a las naciones con menos de medio millón de usuarios de Internet o con una penetración de uso de internet inferior al 10%.

De acuerdo con su conclusión, el 71,7% de los países estudiados presentan una densidad de infracciones inferior a la media mundial, (16,5 correos electrónicos filtrados por cada 100 usuarios de internet). Esto evidencia que los delincuentes cibernéticos se enfocan más en ciertos países que en otros, siendo Estados Unidos, Irán, Israel, Emiratos Árabes Unidos y Qatar,donde el índice de direcciones de correo electrónico que han sido violadas excede el 50%. Esto implica que más del 50% de los usuarios de internet sufrieron daños debido a la violación de sus cuentas de correo electrónico, mientras que, en cambio, las tasas más bajas de direcciones de correo electrónico que han sido violadas se hallan en África, con 4 cuentas violadas por cada 100 usuarios. (Montes, S. (2022, mayo 17)

Si observamos España, vemos que está clasificada en el tercer nivel más alto, con entre 20 y 29 cuentas de correo electrónico vulneradas por cada 100 usuarios de internet.

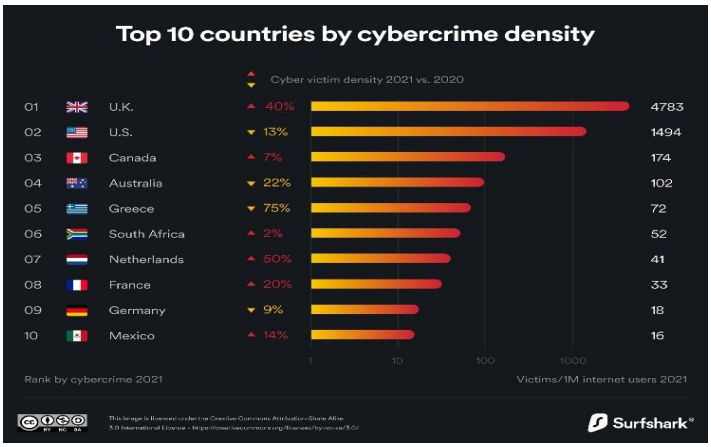
(Montes, S. (2022, mayo 17)




### 2.2.4 Figura 4. Mapa de Violación de Datos a Nivel Mundial

**(Montes, S. (2022, mayo 17)**

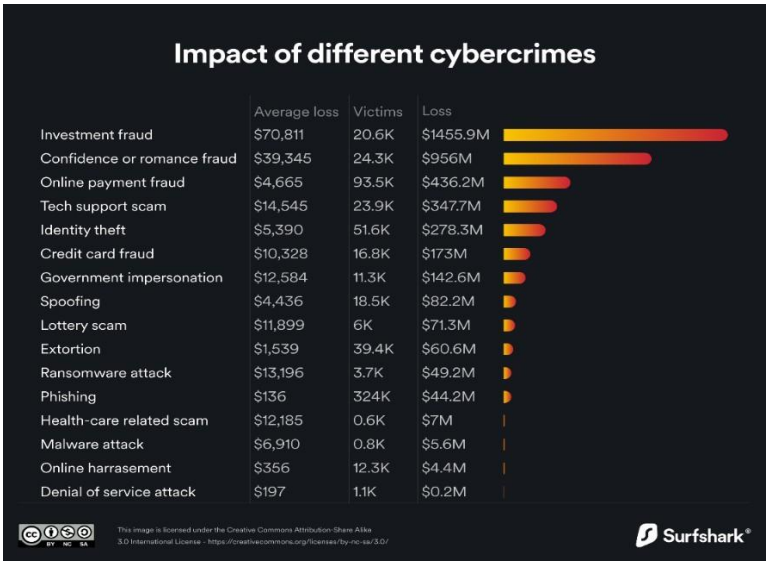
Surfshark también nos muestra la gráfica de los 10 países con mayor densidad de ciberdelincuencia reportada al FBI en 2020 y 2021. Esta clasificación se basa en el número de víctimas afectadas por cada millón de usuarios de Internet.




### 2.2.5 Figura 5. Grafica de los 10 países con mayores datos de ciberdelincuencias reportadas al FBI entre 2020 y 2021 (Cybercrime Statics, 2021, pág. 2)

Como se observa en la tabla, por segundo año consecutivo, Reino Unido lidera la clasificación con 4.783 víctimas, un 40% más con respecto a 2020. Estados Unidos se sitúa en segundo lugar con 1.494 víctimas y pese a que su densidad de ciberdelitos ha disminuido un 13% en comparación a 2020. Canadá en la tercera posición con 174 víctimas por cada millón de usuarios

de internet que suponen un 7% más que el año anterior, y muestra que el mayor aumento interanual de ciberdelitos se registró en los Países Bajos, con un crecimiento del 50% situándolo en la séptima posición de la tabla. (Montes, S. 2022, mayo 17) Esta tabla del Cybercrime Statics 2021, nos muestra que, por tercer año consecutivo, El phishing continúo siendo el cibercrimen más común, afectando a 323,972 usuarios. (Montes, S. 2022, mayo 17).




### 2.2.6 Figura 6. Tabla de impacto de los diferentes cibercrímenes 2021

**(Cybercrime Statics, 2021, pág. 2)**

En el año 2020 durante el COVID 19, Colombia tuvo un incremento en la adopción y transformación digital por parte de sus empresas para continuar sus operaciones. Esto a su vez, genero un crecimiento de los ciberdelitos. Las cifras para el primer semestre del 2022 ya mostraban un incremento del 8% con respecto al año anterior de denuncias asociadas al ciberdelito de phishing, presentado ante SPOA (Sistema Penal Oral Acusatorio de la fiscalía general de la Nación).

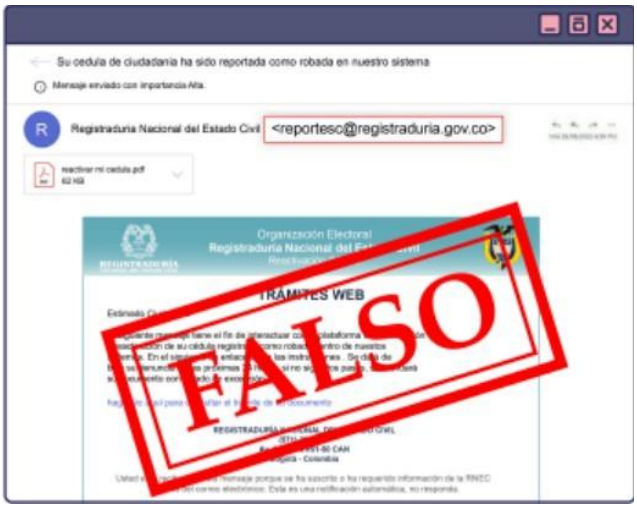
Fig.1. Incremento de denuncias presentadas ante el SPOA tomado de Ciberseguridad en la era de la movilidad digital [2].

**2.2.7 Figura 7. Incremento de denuncias presentadas ante el SPOA tomado de Ciberseguridad en la era de la movilidad digital (Pérez C, Stiven M, 2022, pág. 2)**

En un informe titulado Ciberseguridad en la Era de la Movilidad Digital, presentado por la Cámara Colombiana de Informática y Telecomunicaciones (CCIT), se evidenciaron muchos casos de hurto usando medios informáticos en el primer semestre de 2022. Entre las técnicas más utilizadas por los ciberdelincuentes destacan los ataques de phishing, en los que se despliegan campañas de malware para engañar a los usuarios y obtener información sensible. (Pérez C, Stiven M, 2022, pág. 2)

Un ejemplo concreto de esta práctica fue la suplantación de la cuenta de correo electrónico reportesc@registraduria.gov.co, utilizada por los atacantes para aparentar legitimidad y así inducir a las víctimas a proporcionar datos confidenciales. En estos casos,

el phishing opera mediante enlaces fraudulentos que, al ser seleccionados por los usuarios, permiten a los delincuentes obtener acceso a información privada, simulando provenir de instituciones como la Registraduría Colombiana.




**2.2.8 Figura 8. Antecedente de suplantación de cuenta de correo electrónico del gobierno colombiano. (Pérez C, Stiven M, 2022, pág. 2)**

La publicación Tendencias del cibercrimen 2021 – 2022 por Tictac y la CCIT nos indica que el ransomware, sigue afectando a las empresas en Colombia, en especial a las Pymes.

En 2021, se presentaron más de 500 casos de este tipo de phishing, pero nos refuerza la idea de que los ciberdelincuentes continúan y otros empiezan a trazar estrategias, como nuevas inversiones en innovación tecnológica, para seguir realizando ataques de phishing de datos basados en la ingeniería social para seguir estafando a más usuarios.

En el informe, titulado Panorama de Amenazas en América Latina de 2021 de Kaspersky, que toma en cuenta los 20 programas maliciosos más recurrentes, muestra una tendencia en crecimiento en los ciberdelitos, hablando que, para el caso de Colombia, se presentan 87 casos por minuto y que, de igual manera, muestra que, en el país, los ataques de phishing son altos y se encuentra en un rango medio alto.

Colombia en esta materia esta de color naranja con un caso 3 de 11.09% de usuarios que registraron algún intento de ataque por este método. (Pérez C, Stiven M, 2022, pág. 2)

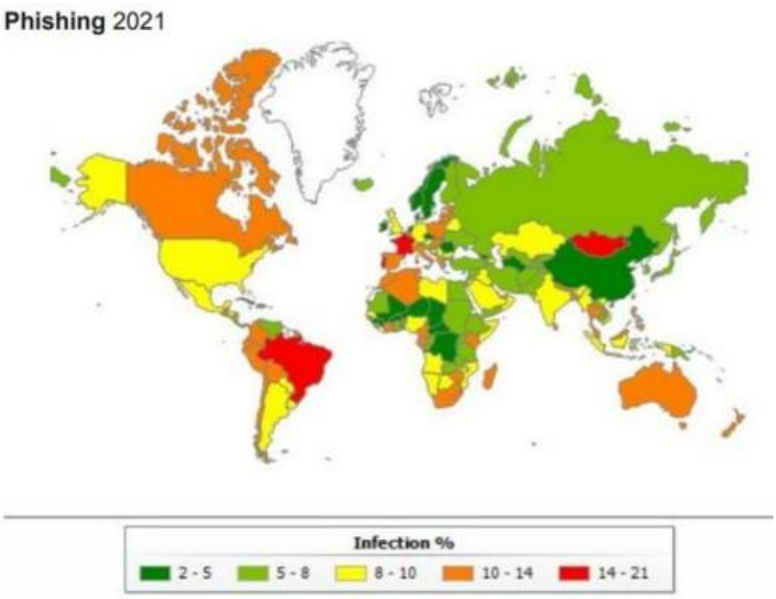


Fig.4. mapa de colores de ataques de Phishing a nivel mundial 2021 [4].

**2.2.9 Figura 9. Mapa de colores de ataques de phishing a nivel mundial 2021. (Pérez C, Stiven M, 2022, pág. 2)**

Kaspersky dentro de su informe, analiza otro de los contextos que se dieron durante

de la pandemia, y fueron los intentos de acceso por el protocolo RDP, un protocolo de Microsoft que permite controlar computadoras a distancia, esto debido a que muchas empresas no migraron a un entorno seguro de teletrabajo o se presentaron ataques donde su acceso inicial fue a través de un phishing, dejándolas expuestas a posibles eventos e impactos, mostrándonos de esta manera, que, por solo ataques de escritorio remoto, en Colombia se presentaron 1.8 millones de intentos en el año 2021. (Pérez C, Stiven M, 2022, pág. 2)

2.3 Los ciberataques alcanzan cifras históricas por la guerra de Ucrania

Datos 01, una empresa tecnológica española que ofrece servicios de copias de seguridad, almacenamiento, sincronización y ciberseguridad para empresas, ha llevado a los ciberataques a máximos históricos.

En 2022 se registró que los ataques de ransomware aumentaron hasta un 253% en comparación con las cifras registradas en aquel entonces en 2021, donde, las pymes, eran el objetivo principal de los ciberdelincuentes y estas microempresas recibían enormes tasas de correos electrónicos maliciosos para asaltar a sus servidores y plataformas con la finalidad de

obtener información de relevancia para obtener beneficios económicos. De acuerdo con INCIBE, el robo de datos por ciberataques puede suponer pérdidas para las pymes de entre 2.000 y 5.000 euros y, según datos de IBM, la cifra asciende a 3,6 millones de euros de media en el caso de las empresas grandes.

Tras la Invasión Rusa de Ucrania, se detectaron ataques de denegación de servicios a Organismos Estatales y Administraciones públicas, buscando el colapso de servidores para realizar hackeos de todo tipo y que las entidades no pudieras gestionar este delito en masa. (Cifras Históricas Ciberataques por guerra de Ucrania, 2021, Escudo Digital)

### 2.3.1 Datos Personales

Las cifras de ciberataques han aumentado tanto para empresas privadas como para organismos públicos y estamos detectando un mayor volumen de recuperación de datos desde el comienzo de la crisis de Ucrania. Lo que conlleva un esfuerzo adicional y estar atentos a esta situación", ha afirmado Juan Llamazares, CEO de Datos101.

Ecuador

El 8 de octubre del 2020 en la Unidad Pedro Vicente Maldonado al noroccidente de Quito, el en ese entonces fiscal Hugo Pérez, abrió una instrucción fiscal por presunto “phishing”, como infractores se obtuvieron a seis personas procesadas, (casi todos de una misma familia) a los cuales se los conoce como alías mamá, papá, neutrón, chino, topo y taz, los 45 mismos que utilizaban números de tarjetas y códigos robados en Estados Unidos y Europa para poder adquirir cuentas de streaming y mercadería en línea. A través de estas actividades, generaron beneficios económicos de $80.000 y lograron adquirir tres vehículos

para su organización dedicada a la ciberdelincuencia. Cabe señalar que el fiscal que llevó el caso lo adecuó en base al artículo 190 del COIP puesto que es el artículo que más se asemejaba a este delito informático (Fiscalía general del Estado Quito, 2020).

En Honduras, la jurisdicción enfrenta varios desafíos en relación con las estafas cibernéticas. Uno de los principales problemas es la rápida evolución de las técnicas utilizadas por los ciberdelincuentes, lo que dificulta la identificación y prevención de estos delitos. Además, existe una falta de concienciación y educación en la población sobre las medidas de seguridad en línea, lo que incrementa la vulnerabilidad ante estas estafas.

Para abordar estos desafíos, se han implementado diversas soluciones. La Comisión Nacional de Bancos y Seguros (CNBS) ha establecido lineamientos mínimos que las instituciones financieras deben seguir para prevenir y mitigar la ocurrencia de fraudes y estafas cibernéticas contra los usuarios financieros. Estos lineamientos incluyen la identificación de nuevas tipologías de fraudes, la implementación de controles preventivos y correctivos, y la notificación en tiempo real de transacciones a los usuarios. (circulares.cnbs.gob.hn)

En cuanto a la legislación, Honduras cuenta con el Código Penal contenido en el Decreto 130-2017, que en su Título XXII aborda la "Seguridad de las Redes y de los Sistemas Informáticos". Este título tipifica diversos delitos informáticos, incluyendo las estafas cibernéticas, y establece sanciones para quienes cometan estos ilícitos. (OAS.ORG)

Además, la CNBS ha emitido resoluciones que refuerzan las medidas de seguridad en el sector financiero. Por ejemplo, la Resolución GRD No.247/23-03-2023 establece lineamientos específicos para que las instituciones supervisadas implementen controles mínimos destinados a prevenir y mitigar fraudes y estafas cibernéticas. (circulares.cnbs.gob.hn)

En la entrevista publicada el 23 de noviembre de 2024 en Televicentro, Carlos Castañeda, especialista en comunicaciones y redes sociales, advierte sobre nuevas modalidades de estafas y hackeos que están afectando a los hondureños. Los ciberdelincuentes emplean tácticas cada vez más sofisticadas para engañar a las personas y obtener sus datos personales y financieros. (Televicentro.com)

Entre las estafas más comunes mencionadas por Castañeda se encuentran:

• Ofertas de empleo falsas: Anuncios en Facebook que prometen salarios elevados para atraer a víctimas y obtener su información personal.

• Encuestas engañosas en WhatsApp: Mensajes que solicitan datos sensibles a cambio de supuestos premios o descuentos.

• Multas falsas con códigos QR: Mensajes que aparentan ser de la Policía Nacional, instando a las personas a pagar multas inexistentes mediante códigos QR.

• Páginas falsas del Banco Central de Honduras: Sitios web que utilizan logotipos oficiales para promover inversiones fraudulentas y robar dinero.

Castañeda destaca que los estafadores se aprovechan de las emociones y necesidades

económicas de las personas, explotando su credulidad y falta de verificación. Además, señala la falta de regulación en el Código Penal hondureño respecto a las estafas en redes sociales, lo que dificulta la investigación y sanción de los responsables. También menciona la carencia de esfuerzos especializados por parte del Ministerio Público para abordar este tipo de delitos.

Para protegerse de estas estafas, Castañeda recomienda:

• Desconfiar de ofertas que parecen demasiado buenas para ser ciertas.

• Verificar la autenticidad de los sitios web antes de compartir información personal.

• Confirmar directamente con amigos o conocidos si reciben mensajes solicitando dinero o datos.

• No responder a llamadas telefónicas sospechosas que soliciten transferencias o información bancaria.

La prevención es clave. Es importante desconfiar, investigar y no compartir datos sensibles sin verificar primero. La ciberseguridad es una responsabilidad compartida entre ciudadanos y autoridades, por lo que es vital tomar medidas para proteger la información personal y evitar ser víctima de estas prácticas fraudulentas.


**2.3.2 Figura 10. Alerta por parte de la DNTV a la ciudadanía sobre ciberestafas mediante Códigos QR (Televicentro.com)**

En Honduras, según la DPI, cada día se reportan entre 3 y 4 casos de ciberestafas, siendo el phishing la estafa más común; técnica que utilizan los ciberdelincuentes para

obtener información persona de los individuos -como relata el caso de María-, a través de correos, llamadas, mensajes texto y redes sociales. (Bancatlan.hn)

En Honduras, la ciberseguridad se ha convertido en una preocupación importante para las autoridades. Según la Dirección de Investigación Policial (DPI), cada día se reportan entre 3 y 4 casos de ciberestafas, siendo el "phishing" la estafa más común.

El "phishing" es una técnica que utilizan los ciberdelincuentes para obtener información personal de los individuos, como contraseñas, números de tarjetas de crédito, entre otros, a través de correos electrónicos, llamadas, mensajes de texto y redes sociales.

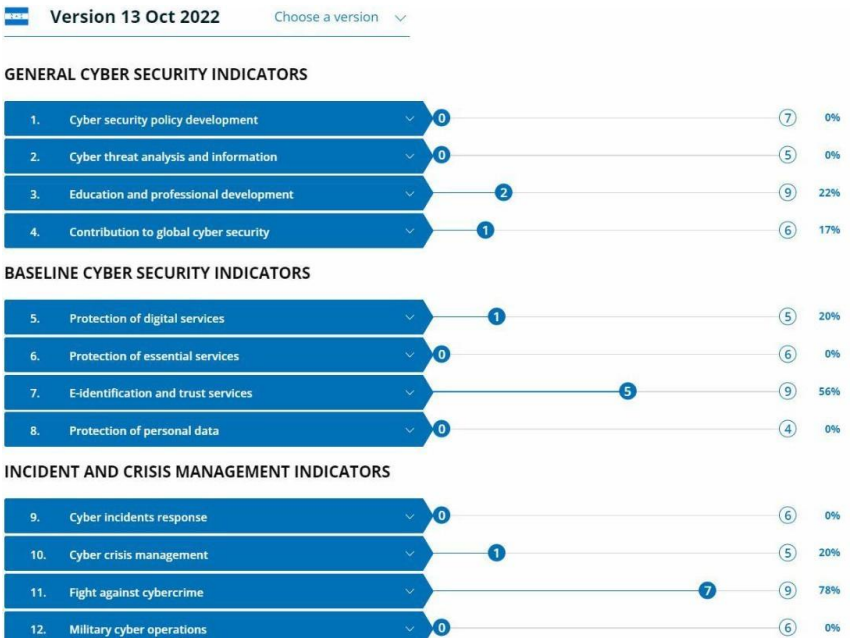
La Policía de Honduras cuenta con un equipo dedicado exclusivamente a la ciberseguridad, y el Código Penal penaliza el "phishing" y otros delitos informáticos. Sin embargo, a pesar de los esfuerzos, el país ocupa la posición 120 de 175 en el Índice Global de Seguridad Nacional en Ciberseguridad (NCSI), siendo el último a nivel centroamericano en comparación con Costa Rica (77), Nicaragua (107), Guatemala (118) y El Salvador

(119). (La Prensa phishing, 16 feb 2025)

Banco Azteca define al Phishing como una nueva forma de fraude que se está llevando a cabo por medio de Internet, utilizando el envío de correos electrónicos, los cuales buscan inducir a las personas a revelar datos personales y confidenciales. (Bancoaztecahn.com)

Para este reporte, la organización con sede en Estonia contó con la colaboración informativa de la Comisión Nacional de Telecomunicaciones

(Conatel, Ciberseguridad, 2023).




**2.3.3 Figura 11. Reporte Conatel 2022 de indicadores de ciber seguridad**

**(La Prensa phishing, 16 feb 2025)**

Según expertos en ciberseguridad en el 2023, se registraron 1.8 millones de ataques dirigidos a los sistemas tecnológicos de empresas e instituciones hondureñas.

Se reportan diariamente más de 500 ataques en la región centroamericana, de los cuales cerca del 20% están dirigidos a Honduras. Esto significa que se contabilizan alrededor de 100 ciberataques diarios en el país, de acuerdo con los especialistas.

Los ámbitos más impactados por ciberataques son el gobierno, el sector financiero, la educación, la manufactura, los centros de llamadas y la producción. Sin embargo, uno de los grupos más susceptibles son las entidades estatales que aumentan por la falta de estrategias de protección modernas que las exponen a amenazas cibernéticas que podrían acarrear repercusiones para la seguridad nacional, la economía y la privacidad de los ciudadanos.

En los meses recientes, diversas instituciones han sufrido ataques a sus sistemas, incluyendo al Instituto Hondureño de Transporte Terrestre (IHTT); en marzo, los hackers fueron los responsables de su base de datos y bloquearon su acceso. (Diario El Heraldo, Instituciones del Estado, las más vulnerables a los ciberataques, Feb 2025)

## 2.3 TEORÍAS DE SUSTENTO

### 2.3.1 BASES TEÓRICAS

**Modelo de Ciberseguridad** Este es un plan o marco de seguridad cibernética que utiliza una organización para medir el nivel de madurez y la capacidad de la organización para identificar amenazas y riesgos de ciberseguridad, y para orientar la selección de políticas y estrategias para defensa de amenazas y mitigación de riesgos.

En una investigación de la universidad EIA, en 2024, se propuso un modelo de ciberseguridad enfocado en la detención temprana de ataques de phishing, usando inteligencia artificial y procesamiento de lenguaje natural. Su propósito era crear un sistema que identifique ataques de phishing mediante el análisis

de cabecera de correos electrónicos.

Este modelo se implementó a través de metodología ASUM-DM de IB. Este modelo se valida y entrena empleando redes neuronales y otras técnicas de Machine Learning, logrando un alto nivel de precisión en la identificación de correos electrónicos maliciosos.

(Universidad EIA (2024). Desarrollo de modelos de inteligencia artificial para la detección de ataques de phishing.)

**Teoría de Ingeniería Social** La ingeniería social es una estrategia de manipulación psicológica utilizada por atacantes para obtener información confidencial de las víctimas sin el uso directo de herramientas tecnológicas, sino a través del engaño y la explotación de la confianza humana. Kevin Mitnick, en su libro The Art of Deception (2002), expone diversos métodos empleados por los ciberdelincuentes, destacando que la seguridad tecnológica es ineficaz si no se considera el factor humano. Mitnick argumenta que los ataques de phishing explotan la ingenuidad de las personas mediante correos electrónicos, llamadas telefónicas y sitios web falsificados.

Mitnick (2002) explica que los ataques de ingeniería social siguen patrones predecibles basados en vulnerabilidades psicológicas humanas. En la psicología y la ciberseguridad se estudiaron estos patrones. La ingeniería social se basa en cuatro principios psicológicos fundamentales:

• Autoridad: Los ciberdelincuentes fingen ser figuras de autoridad confiables, como empleados de bancos, compañías tecnológicas o agencias gubernamentales. La confianza en la autoridad reduce la probabilidad de cuestionar la autenticidad de la solicitud.

• Urgencia: Los atacantes crean una sensación de urgencia para evitar que la víctima reflexione. Mensajes como "su cuenta será suspendida si no responde en 24 horas" presionan a los usuarios para que actúen impulsivamente.

• Escasez: Se usa la percepción de una oportunidad limitada para inducir a la acción. Por ejemplo, promociones falsas o advertencias sobre problemas de seguridad que requieren intervención inmediata.

• Familiaridad: Se utilizan referencias a experiencias previas de la víctima para generar confianza. Correos electrónicos que imitan el estilo de comunicación de una empresa conocida aumentan la probabilidad de éxito del engaño.

Estos principios permiten a los atacantes crear situaciones verosímiles que persuaden a los usuarios a entregar datos personales o financieros sin sospecha. En el contexto del phishing, la ingeniería social se manifiesta en correos electrónicos que imitan a entidades legítimas, engañando a los usuarios para que revelen credenciales o descarguen malware.

Mitnick enfatiza que las soluciones técnicas por sí solas no pueden detener la ingeniería social; la educación del usuario es esencial. Estrategias de concienciación como la capacitación en detección de phishing, el uso de autenticación multifactorial y la verificación de enlaces sospechosos son claves para contrarrestar estas amenazas.

(Mitnick, K. D. (2002). The Art of Deception: Controlling the Human Element of Security. Wiley.)

**Teoría del comportamiento del usuario en Ciberseguridad** El comportamiento de los usuarios en ciberseguridad ha sido estudiado bajo varios modelos psicológicos. Dos de los más relevantes en el contexto del phishing son el Protection Motivation Theory (PMT) y el Technology Acceptance Model (TAM).

a) Protection Motivation Theory (PMT)

La Protection Motivation Theory (Rogers, 1975) explica cómo los individuos responden ante amenazas percibidas. Se basa en cuatro factores clave:

• Severidad percibida: La gravedad de la amenaza y su impacto potencial en la víctima.

• Vulnerabilidad percibida: La probabilidad de que la amenaza afecte al individuo.

• Eficacia de la respuesta: La percepción de que una acción específica puede reducir el riesgo.

• Autoeficacia: La confianza en la capacidad personal para ejecutar la acción protectora.

Los ataques de phishing pueden contrarrestarse si los usuarios perciben el riesgo como alto y creen que pueden tomar medidas efectivas para prevenirlo, como el uso de autenticación multifactor o la verificación de enlaces sospechosos. Esta teoría se aplica en campañas de concienciación en ciberseguridad que buscan cambiar el comportamiento del usuario para que adopten hábitos seguros en línea.

b) Technology Acceptance Model (TAM)

El Technology Acceptance Model (Davis, 1989) analiza la aceptación de nuevas tecnologías y su impacto en la seguridad. Sus variables clave son:

• Utilidad percibida: Cuán efectiva es una tecnología para resolver un problema.

• Facilidad de uso percibida: Cuán intuitivo es su manejo.

Los usuarios que encuentran difíciles las medidas de ciberseguridad (como contraseñas complejas) pueden evitarlas, lo que los hace vulnerables a ataques de phishing. La aplicación de este modelo en la prevención del phishing se centra en diseñar soluciones de seguridad que sean fáciles de usar y que los usuarios adopten sin resistencia, como autenticación biométrica y gestores de contraseñas.

(Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. Journal of Psychology, 91(1), 93-114.

(Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user

acceptance of information technology. MIS Quarterly, 13(3), 319-340.

**Modelo de detección de phishing** Los modelos de detección de phishing han evolucionado con el tiempo para contrarrestar las técnicas avanzadas de los ciberdelincuentes. Se dividen en enfoques heurísticos, basados en listas negras y basados en inteligencia artificial (AI).

1. Listas negras y listas blancas: Bases de datos de sitios web maliciosos que bloquean

accesos sospechosos. Aunque efectivas, estas listas pueden ser vulnerables a nuevas amenazas que aún no han sido registradas.

2. Heurísticas: Reglas predefinidas que analizan patrones en URL, encabezados de correos y textos para identificar anomalías. Este enfoque es útil, pero tiene altas tasas de falsos positivos.

3. Inteligencia Artificial y Machine Learning: Algoritmos que identifican patrones de phishing en grandes volúmenes de datos mediante Natural Language Processing (NLP) y detección de anomalías. Según Jain & Gupta (2018), estos modelos pueden predecir ataques emergentes con mayor precisión.

Los sistemas modernos combinan estos enfoques para mejorar la precisión en la detección de amenazas. En particular, la inteligencia artificial ha demostrado ser una de las soluciones más efectivas para mitigar el phishing, ya que puede aprender de grandes cantidades de datos y detectar nuevas amenazas en tiempo real.

(Jain, A. K., & Gupta, B. B. (2018). Phishing detection: Analysis of visual similarity-based approaches. Security and Privacy, 1(2), e23.)

**Teoría del riesgo de ciberseguridad** La evaluación de riesgos en ciberseguridad se basa en marcos estandarizados como el NIST Cybersecurity Framework y la norma ISO 27001.

a) NIST Cybersecurity Framework

El National Institute of Standards and Technology (NIST, 2014) establecen cinco funciones esenciales:

1. Identificar: Detectar activos críticos y amenazas.

2. Proteger: Implementar controles de seguridad.

3. Detectar: Monitorear actividades sospechosas.

4. Responder: Actuar ante incidentes.

5. Recuperar: Restaurar sistemas comprometidos.

b) ISO 27001

La norma ISO 27001 (ISO, 2013) establece un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la gestión de riesgos, incluyendo:

• Control de acceso.

• Encriptación de datos.

• Auditorías de seguridad periódicas.

Estos marcos permiten a las organizaciones evaluar y mitigar los riesgos del phishing, reduciendo la vulnerabilidad de sus sistemas y protegiendo la información sensible.

(National Institute of Standards and Technology (NIST). (2018) Framework for Improving Critical Infrastructure Cybersecurity. Version 1.1.

(International Organization for Standardization (ISO). (2013) ISO/IEC 27001:2013 Information security management systems — Requirements.

**Teoría del crimen del ciberespacio** El phishing puede analizarse desde el punto de vista criminológico utilizando la Teoría de la Oportunidad y la Teoría de la Rutina.

• Teoría de la Oportunidad (Clarke, R. V. (1997): Explica que los ciberdelincuentes atacan cuando encuentran vulnerabilidades fácilmente explotables, como credenciales débiles o la falta de educación en ciberseguridad. Este enfoque sugiere que mejorar las defensas técnicas y la concienciación de los usuarios puede reducir significativamente la frecuencia de ataques exitosos.

• Teoría de la Rutina (Cohen & Felson (1979): Sugiere que los ataques de phishing ocurren porque las víctimas tienen patrones de comportamiento

predecibles en línea, como revisar correos electrónicos diariamente sin verificaciones de seguridad.

Cambiar estos hábitos, como verificar enlaces antes de hacer clic o utilizar autenticación multifactorial, puede disminuir la efectividad de los ataques.

Estas teorías ayudan a comprender por qué los ataques de phishing son efectivos y cómo pueden prevenirse mediante cambios en el comportamiento y medidas de seguridad adecuadas. La combinación de estrategias de prevención, educación y monitoreo continuo es clave para minimizar los riesgos en el ciberespacio.

(Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. American Sociological Review, 44(4), 588-608.)

(Clarke, R. V. (1997). Situational Crime Prevention: Successful Case Studies.

Harrow and Heston.)

### 2.3.2 BASES LEGALES

Aunque Honduras no cuenta con un equipo nacional dedicado exclusivamente a la ciberseguridad, sí existen entidades y esfuerzos en marcha para abordar el tema. La Comisión Nacional de Telecomunicaciones (CONATEL) actúa como regulador del sector de las telecomunicaciones, y en 2018 se anunció una ley para crear una comisión y estrategia nacional de ciberseguridad. Además, existe un Comité Interinstitucional de Ciberseguridad, aunque se ha formado a partir de acciones gubernamentales y no garantiza la representación de la sociedad civil o los consumidores.

La única ley existente para proteger la ciberseguridad se aplica solamente a las redes sociales (Ley de Estrategia de Ciberseguridad Nacional de Prevención de Campañas de Odio y Discriminación en Redes Sociales).2 También, Honduras no cuenta con una ley de datos personales. En 2006, Honduras aprobó la Ley de Transparencia y Acceso a la Información Pública (Decreto 170-2006), 3 que estableció el Instituto de Acceso a la Información Pública (IAIP). Individuales interesados pueden solicitar el Instituto de Acceso a la Información Pública sobre qué agencias públicas tiene acceso a cuáles datos personales.

**Constitución de la Republica**

Artículo 76: Garantiza la protección al honor, la intimidad personal y familiar, y la propia imagen. Este precepto constitucional sienta las bases para la protección de datos personales y la privacidad de las comunicaciones.

Artículo 100: Establece el derecho a la inviolabilidad y al secreto de las comunicaciones, incluyendo las postales, telegráficas y telefónicas, salvo resolución judicial. Aunque no menciona explícitamente las comunicaciones digitales, este artículo puede interpretarse en el contexto actual para incluirlas, dada la evolución tecnológica.

(Constitución de la República, Decreto n 131, 11 de enero 1982, págs. 40-45)

**Código Penal de Honduras (Decreto No. 130-2017)**

Título XXII Seguridad de las Redes y de los Sistemas Informáticos Artículo 398. Acceso no autorizado a sistemas informáticos Definición y Aplicabilidad

El Artículo 398 sanciona a quienes acceden sin autorización a sistemas informáticos vulnerando medidas de seguridad. En el contexto del phishing, este delito puede configurarse cuando el atacante accede a bases de datos sin permiso o compromete cuentas ajenas mediante credenciales obtenidas de forma fraudulenta.

Ejemplo Práctico

Un ciberdelincuente envía un correo falso suplantando a una entidad financiera,

logrando que la víctima ingrese sus credenciales en un sitio web fraudulento. Posteriormente, el atacante usa estas credenciales para acceder a la cuenta bancaria sin autorización, configurando el delito descrito en el Artículo 398.

Sanciones y Agravantes

La pena es de 6 a 18 meses de prisión o multa de 100 a 200 días. Si el ataque afecta infraestructuras críticas, la pena aumenta en un tercio.

Artículo 399. Daños a datos y sistemas informáticos

Definición y Aplicabilidad

Este artículo sanciona la alteración, supresión o inhabilitación de sistemas informáticos sin autorización. En el phishing, esto ocurre cuando el atacante manipula datos para engañar a la víctima o cuando compromete el sistema de la empresa atacada.

Ejemplo Práctico

Un atacante suplanta la identidad de una entidad bancaria y redirige a los usuarios a un sitio web falso. Allí, captura datos y posteriormente, borra transacciones para encubrir el fraude.

Sanciones y Agravantes

Las penas varían entre 1 y 3 años de prisión o multas de 100 a 400 días. Si se causa un grave daño económico, la pena se aumenta en un tercio.

Artículo 400. Abuso de dispositivos

Definición y Aplicabilidad

Este artículo penaliza la fabricación, venta o distribución de software y herramientas destinadas a cometer delitos informáticos. En phishing, esto aplica a quienes crean o venden kits de phishing y herramientas para evadir la seguridad en línea.

Ejemplo Práctico

Un individuo diseña un software que genera sitios web falsos idénticos a los de bancos y los vende a ciberdelincuentes. Este delito configura abuso de dispositivos.

Sanciones

La pena es de 6 meses a 1 año de prisión o multa de 100 a 200 días

Artículo 401. Suplantación de identidad

Definición y Aplicabilidad

El phishing está directamente relacionado con la suplantación de identidad, ya que los atacantes se hacen pasar por empresas, bancos o individuos para engañar a sus víctimas.

Ejemplo Práctico

Un estafador envía correos electrónicos fingiendo ser un ejecutivo bancario y solicita a los clientes que actualicen sus datos en un enlace falso, obteniendo información crítica.

Sanciones

Este delito se castiga con 6 meses a 1 año de prisión o multa de 100 a 300 días.

Artículo 402. Circunstancias agravantes

Si el delito es cometido por una persona con acceso autorizado a sistemas o en el marco de un grupo delictivo, las penas aumentan en un tercio. En phishing, esto aplica a empleados desleales o bandas organizadas de ciberdelincuencia.

Artículo 403. Responsabilidad de las personas jurídicas

Si una empresa facilita o permite el uso de su infraestructura para phishing, podría enfrentar sanciones, como la suspensión de actividades de 3 a 5 años y multas de 300 a 500 días.

Artículo 404. Reglas especiales de jurisdicción

El Código Penal hondureño permite perseguir estos delitos, aunque los ataques provengan

del extranjero, garantizando la protección de los ciudadanos ante amenazas globales.

**Ley de Firma Electrónica (Decreto No. 149-2013)**

Artículo 8: Requisitos o Atributos Jurídicos de Firma Electrónica y su Relación con el Phishing

1. Introducción La Ley de Firma Electrónica en Honduras, establecida en el Decreto No. 149-2013, regula el uso de firmas digitales y electrónicas,

garantizando su validez y fiabilidad. Sin embargo, el uso indebido de esta tecnología ha generado vulnerabilidades que los ciberdelincuentes explotan mediante ataques de phishing y, en particular, spear phishing. Este documento analiza los requisitos de la firma electrónica establecidos en el Artículo 8 y su relevancia en la prevención del fraude digital.

2. Requisitos Jurídicos de la Firma Electrónica

El Artículo 8 de la Ley de Firma Electrónica establece que una firma digital o electrónica es válida si cumple con los siguientes criterios:

1. Se emplea un método fiable para identificar a la parte firmante y su intención respecto del documento firmado.

Dicho método debe:

a.) ser lo suficientemente fiable según el contexto en que se use.

b.) b) Haber demostrado en la práctica su eficacia en la identificación del firmante.

Además, la firma electrónica se considera fiable si:

1. Los datos de creación de la firma corresponden exclusivamente al firmante.

2. La firma es verificable.

3. La clave de firma es controlada solo por el firmante en el momento de

la firma.

4. Se puede detectar cualquier alteración posterior.

5. Está ligada a la información firmada, de modo que, si se cambia, la firma se invalida.

6. Cumple con las regulaciones aceptadas.

Riesgos del Phishing y Spear Phishing en Firmas Electrónicas

El phishing es una amenaza creciente en Honduras y a nivel mundial. En el contexto de la firma electrónica, los atacantes pueden utilizar estrategias de spear phishing para obtener firmas ilegítimas en documentos sensibles. Estos ataques suelen seguir el siguiente esquema:

1. Suplantación de Identidad: El atacante se hace pasar por un superior jerárquico, cliente o entidad de confianza.

2. Urgencia Falsa: Se induce a la víctima a firmar un contrato, autorización o factura con premura, evitando verificaciones adicionales.

3. Compromiso de Datos: Al firmar, la víctima entrega involuntariamente una firma electrónica válida, permitiendo a los atacantes comprometer cuentas, realizar transacciones fraudulentas o modificar documentos.

4. Medidas Preventivas: Para minimizar el impacto del phishing en el uso de firmas electrónicas, se recomienda:

• Verificación de Identidad: Confirmar por vías alternativas (llamadas, reuniones presenciales) la autenticidad de solicitudes de firma.

• Uso de Doble Autenticación: Implementar factores de autenticación adicionales antes de validar una firma.

• Capacitación a Usuarios: Educar a empleados y directivos sobre riesgos de phishing y protocolos seguros de firma digital.

• Revisión de Documentos: No firmar documentos sin una verificación exhaustiva del contenido y remitente. (Congreso Nacional de Honduras: Decreto No. 149-2013 (Ley de Firma Electrónica).

**Ley de Protección al Consumidor de Honduras**

l phishing es una técnica fraudulenta en la que ciberdelincuentes suplantan identidades de empresas, bancos o entidades oficiales para engañar a los consumidores y obtener información personal o financiera. La Ley de Protección al Consumidor de Honduras establece derechos fundamentales para los consumidores, los cuales pueden verse vulnerados por esta modalidad delictiva. En este análisis, se abordarán los artículos relevantes de la Ley de Protección al

Consumidor que pueden servir como base legal para la protección contra el phishing y fraudes electrónicos en Honduras. Derechos de los Consumidores Relacionados con el Phishing Sección I. Derechos de los Consumidores Artículo 9. Derechos Básicos del Consumidor Este artículo garantiza la protección de los consumidores ante prácticas abusivas y engañosas en el mercado. En relación con el phishing, destacan los siguientes numerales: Numeral 6: Protección contra la publicidad engañosa o falsa, las modalidades de ventas coercitivas o discriminatorias y las prácticas abusivas en perjuicio de los intereses económicos del consumidor. Relación con el Phishing:

o Muchos ataques de phishing se presentan como ofertas fraudulentas, premios falsos o promociones engañosas, haciendo que el consumidor proporcione datos personales y financieros sin saber que está siendo víctima de un fraude.

o Este numeral permite que las víctimas de phishing exijan protección contra estos fraudes y que las autoridades sancionen a quienes realicen este tipo de engaños.

• Numeral 11: Derecho a la prevención y reparación de daños patrimoniales o de cualquier índole, además de la indemnización integral por perjuicios ocasionados al consumidor. Relación con el Phishing: o Si una persona es víctima de phishing y pierde dinero debido a una estafa electrónica, este artículo le otorga el derecho de exigir reparación del daño. o Las empresas cuyos nombres sean usados en fraudes de phishing podrían ser obligadas a tomar medidas para evitar que los consumidores sean engañados bajo su identidad.

o Se refuerza el acceso a órganos administrativos y judiciales para que las víctimas puedan presentar denuncias contra quienes utilicen tácticas fraudulentas en entornos digitales. Regulaciones sobre Contrataciones y Ventas Electrónicas Sección V. Prestación de Servicios Artículo 48. Modalidades para rescindir contratos electrónicos "Cuando la contratación de un servicio haya sido realizada de forma telefónica, electrónica o similar, podrá ser rescindida a elección del consumidor o usuario, mediante el mismo medio utilizado en la contratación." Relación con el Phishing:

• Muchos ciberdelincuentes utilizan suscripciones falsas o renovaciones automáticas fraudulentas obtenidas mediante phishing para sustraer dinero de sus víctimas. • Este artículo protege al consumidor al permitirle rescindir contratos electrónicos fraudulentos mediante el mismo medio en que fueron aceptados, sin trabas abusivas.

• Obliga a las empresas a registrar fehacientemente las solicitudes de cancelación y comunicarlo al consumidor. Sección VII. Venta por Correspondencia y Medios Electrónicos Artículo 58. Venta por correspondencia y otros similares "Es aquella propuesta de venta de bienes o servicios efectuada por medio postal, telecomunicaciones, electrónico o similar y cuya aceptación se realiza por iguales medios." Relación con el Phishing: • Este artículo regula transacciones electrónicas, asegurando que cualquier venta en línea debe cumplir con normativas claras y verificables.

• Evita que los estafadores utilicen correos electrónicos falsos o sitios fraudulentos para engañar a los consumidores y robarles información personal o financiera.

• Se prohíbe el uso de números postales para domicilios de proveedores, lo que dificulta el rastreo de estafadores en operaciones fraudulentas. Implicaciones Legales del Phishing en el Marco de la Ley de Protección al Consumidor El phishing, al ser un método de fraude que afecta la integridad económica de los consumidores, puede ser sancionado mediante los artículos analizados. Las principales implicaciones legales incluyen: 1. Responsabilidad de Empresas y Bancos: o Las entidades que operan en línea deben implementar mecanismos de autenticación y seguridad para prevenir fraudes. o Si un consumidor es víctima de phishing utilizando la imagen o identidad de una empresa, esta puede ser responsable indirectamente si no tomó medidas de seguridad adecuadas. Derecho del Consumidor a la Indemnización:

o Las víctimas de phishing pueden reclamar compensaciones por daños económicos sufridos como resultado del engaño. o Los proveedores de servicios electrónicos deben garantizar mecanismos efectivos para detener transacciones fraudulentas y reembolsar fondos en casos de estafa. Obligación de Regulación de Ventas Electrónicas: o La ley establece que todas las contrataciones y ventas electrónicas deben cumplir con estándares claros, lo que significa que cualquier intento de phishing que simule una venta legítima podría ser sancionado.

Recomendaciones para la Protección del Consumidor contra el Phishing Para mejorar la aplicación de esta ley en la lucha contra el phishing, se recomienda: 1. Educación y Concienciación: o Campañas informativas sobre cómo identificar correos electrónicos y mensajes fraudulentos. o Advertencias oficiales de bancos y empresas sobre tácticas de phishing comunes. 2. Fortalecimiento de la Regulación de Comercio Electrónico:

o Implementar certificaciones electrónicas obligatorias para páginas de venta en línea. o

Mayor regulación a plataformas de pago para detectar transacciones fraudulentas en tiempo real. 3. Sanciones Más Severas para el Uso Fraudulento de Identidades Comerciales: o Si un delincuente usa el nombre de una empresa o institución pública para engañar a consumidores, la empresa afectada debería poder iniciar acciones legales inmediatas.

o Creación de un registro nacional de dominios comerciales verificados para prevenir la creación de sitios web fraudulentos. Facilidad de Denuncias en Línea: o Establecer un portal digital donde los consumidores puedan reportar intentos de phishing y fraudes electrónicos. o Implementar sanciones efectivas contra operadores de telecomunicaciones y bancos que no protejan a sus clientes contra fraudes electrónicos. (Ley de Protección al Consumidor, Decreto No. 24-2008.) Conclusión Ley de Protección al Consumidor de Honduras proporciona una base legal para proteger a los ciudadanos contra fraudes electrónicos y phishing. Los artículos 9, 48 y 58 permiten:

• Sancionar publicidad engañosa utilizada en phishing.

• Garantizar la cancelación de contratos electrónicos fraudulentos.

• Regulares transacciones electrónicas para evitar engaños en línea.

• Exigir compensaciones económicas por daños causados por el phishing. Sin embargo, se necesita una regulación más específica para abordar de manera directa los delitos cibernéticos y reforzar la seguridad digital en el país. (Ley de Protección al Consumidor, Decreto No. 24-2008.)

**Ley de Protección de Datos Personales (Decreto No. 25-2022)**

Protección de Datos en Honduras El Proyecto de Ley de Protección de Datos Personales representa una oportunidad para mejorar la seguridad digital en Honduras, pero su aprobación sigue pendiente. Es crucial que el país adopte medidas concretas para regular el uso de datos, sancionar el fraude cibernético y educar a la población sobre los riesgos del phishing. En la era de la información, proteger los datos personales no es solo una cuestión de privacidad, sino también una necesidad para garantizar la seguridad y confianza en el entorno digital. (Claribel & Humberto Medina, Ley de protección de datos, 2021) Contexto La protección de datos personales es un derecho fundamental que garantiza la privacidad e integridad de la información de los ciudadanos. En Honduras, este derecho se encuentra respaldado en la Constitución de la República y en iniciativas legislativas que buscan su regulación y protección efectiva. A lo largo de los años, el

país ha reconocido la necesidad de establecer mecanismos legales para resguardar la información personal de sus ciudadanos ante los avances tecnológicos y el uso masivo de datos en plataformas digitales. (Claribel & Humberto Medina, Ley de protección de datos, 2021) Marco Constitucional de la Protección de Datos en Honduras La Constitución de la República de Honduras establece las bases fundamentales para la protección de datos personales en varios de sus artículos.

• Artículo 76: Reconoce el "derecho al honor, a la intimidad personal, familiar y a la propia imagen", sentando un precedente para la protección de información personal y estableciendo un límite a la divulgación o manipulación indebida de datos.

• Artículo 100: Garantiza la inviolabilidad y el secreto de las comunicaciones, permitiendo su acceso solo mediante resolución judicial. Esto implica que los documentos personales solo pueden ser revisados por autoridades competentes, protegiendo la información de cualquier tipo de intervención arbitraria.

• Artículo 182, numeral 2: Introduce la Garantía Constitucional del Habeas Data, la cual otorga a los ciudadanos el derecho de acceder, rectificar y controlar el uso de su información personal en bases de datos públicas y privadas. Esta figura no solo reconoce el derecho de protección de datos, sino que también habilita una acción legal para su exigencia en caso de vulneración. Si bien estos artículos establecen principios generales para la protección de datos en Honduras, la falta de un marco legal específico ha generado dificultades en la aplicación práctica de estos derechos. (Claribel & Humberto Medina, Ley de protección de datos, 2021) Desafíos en la Protección de Datos en Honduras A pesar de que la Constitución hondureña reconoce y protege los derechos relacionados con la privacidad y el manejo de datos personales, la realidad demuestra que estos derechos aún no cuentan con un mecanismo de aplicación efectivo. Existen varios desafíos en este campo:

1. Ausencia de una legislación específica: Aunque el derecho a la protección de datos está reconocido, no hay una ley integral que regule su aplicación en el sector público y privado.

2. Falta de cultura en protección de datos: No solo es necesario contar con regulaciones, sino también con una sociedad educada sobre la importancia del manejo seguro de la información.

3. Limitada capacidad institucional: No existe una entidad autónoma y especializada que supervise y sancione el mal uso de datos personales. (Claribel & Humberto Medina, Ley de

protección de datos, 2021)

**Proyecto de Ley de Protección de Datos Personales**

Ante la necesidad de una legislación que garantice una regulación clara y efectiva en la protección de datos personales, en abril de 2018 se presentó ante el Congreso Nacional de Honduras el Proyecto de Ley de Protección de Datos Personales. Este aún no se ha aprobado totalmente, quedando en suspenso en su tercer y último debate.

Este proyecto de ley busca establecer los principios, derechos y mecanismos para la recolección, almacenamiento y uso de datos personales en Honduras. Entre sus disposiciones relevantes están: Definiciones y Principios del Proyecto de Ley. El proyecto propone definiciones amplias para asegurar que cualquier dato personal pueda protegerse dentro del marco legal. Dentro de sus principios destacan:

1. Principio de Finalidad de Propósitos: Los datos solo pueden ser recopilados y tratados con un propósito específico y legítimo, evitando su uso para finalidades distintas a las originalmente establecidas.

2. Principio de Acceso a la Información: Toda persona tiene derecho a conocer qué información personal se encuentra en poder de terceros y el uso que se le está dando.

3. Principio de Seguridad: Se establece la obligación de implementar medidas de seguridad para evitar el acceso, uso o alteración no autorizada de datos personales.

4. Principio de Confidencialidad: Las personas o entidades que manejen datos personales deben garantizar su reserva y no divulgarlos sin el consentimiento del titular. (Claribel & Humberto Medina, Ley de protección de datos, 2021) Derechos ARCO y Mecanismos de Acción El proyecto de ley introduce los Derechos ARCO (Acceso, Rectificación, Cancelación y Oposición), que garantizan el control de los ciudadanos sobre su información personal.

• Derecho de Acceso: Permite a los ciudadanos solicitar información sobre los datos personales que se tienen sobre ellos.

• Derecho de Rectificación: Otorga la posibilidad de corregir información incorrecta o desactualizada.

• Derecho de Cancelación: Permite eliminar datos personales cuando ya no sean necesarios

o se hayan recolectado sin consentimiento.

• Derecho de Oposición: El titular puede negarse al tratamiento de sus datos cuando considere que pueden ser utilizados de forma incorrecta o perjudicial. Para hacer valer estos derechos, el proyecto establece mecanismos de acción, entre ellos:

• Solicitudes formales para ejercer los derechos ARCO. • Acceso a información sobre el manejo de datos personales.

• Regulación del consentimiento en la cesión de datos a terceros. (Claribel & Humberto Medina, Ley de protección de datos, 2021) Contradicciones y Problemas en el Proyecto de Ley A pesar de que el proyecto de ley representa un avance significativo en la regulación de la protección de datos en Honduras, algunos artículos presentan contradicciones o pueden prestarse a abusos. (Claribel & Humberto Medina, Ley de protección de datos, 2021)

• Artículo 5: Excepciones a la Protección de Datos: Si bien es normal que las leyes contemplen excepciones, la redacción amplia de este artículo deja espacio para interpretaciones arbitrarias. No se establece con claridad bajo qué criterios se pueden ignorar las garantías de protección de datos.

• Artículo 46, Literal A: Cesión de Datos por Autorización Legal: Este artículo establece que los datos pueden ser compartidos si una ley lo permite, lo que podría usarse como excusa para vulnerar la privacidad de los ciudadanos. Estos puntos generan preocupación debido a antecedentes de abusos en legislaciones previas, como la Ley de Intervención de las Comunicaciones, la cual permitió que el Estado accediera a datos privados bajo el argumento de "seguridad nacional". (Claribel & Humberto Medina, Ley de protección de datos, 2021) Regulación y Aplicación en el Sector Privado y Público Uno de los aspectos importantes del proyecto de ley es que impone la obligación de implementar políticas de protección de datos en el sector privado, especialmente en el ámbito bancario.

Sin embargo, en el sector público se debe trabajar en fortalecer la transparencia institucional y la capacitación de los funcionarios en el manejo adecuado de la información personal. El éxito de una legislación de protección de datos no solo depende de su contenido, sino también de su correcta implementación y cumplimiento. En este sentido, la creación de una Institución Garante con capacidad real de supervisión y sanción es crucial para evitar la impunidad

en el uso indebido de la información personal. (Claribel & Humberto Medina, Ley de protección de datos, 2021).

**Importancia de la Protección de Datos en la Era Digital**

Hoy en día la información personal es uno de los recursos más valiosos, su manejo inadecuado puede derivar en fraudes, robos de identidad y violaciones a la privacidad. La mayoría de los países han comprendido la importancia de regular los datos personales, implementando leyes como el Reglamento General de Protección de Datos (GDPR) en Europa, que establece estrictas normas para recopilar y tratar datos.

En el caso de Honduras, la falta de regulación efectiva coloca a los ciudadanos en una situación de vulnerabilidad. A medida que el país avanza en el ámbito digital, es fundamental que el marco legal evolucione en la misma dirección para garantizar el respeto a la privacidad y la seguridad de los datos personales.

Conclusión La protección de datos en Honduras es un derecho reconocido constitucionalmente, pero con serias deficiencias en su aplicación. El Proyecto de Ley de Protección de Datos Personales representa un intento de modernizar la regulación en este campo, pero aún quedan retos importantes, como la definición clara de sus excepciones, la creación de un ente regulador con capacidad real de fiscalización y la educación de la sociedad sobre la importancia del resguardo de su información personal. En un mundo donde la información es poder, la protección de datos no es solo una cuestión legal, sino una necesidad fundamental para garantizar la privacidad y seguridad de los ciudadanos en la era digital. (Claribel & Humberto Medina, Ley de protección de datos, 2021).

**Convenio Internacionales**

Convenio de Budapest Existen tesis en el ámbito del derecho que abordan soluciones para combatir las estafas cibernéticas en países con legislaciones penales establecidas. Un ejemplo es la tesis titulada "Los delitos informáticos en el Código Penal Argentino: Análisis de la Ley 26.388 y su adecuación al Convenio de Budapest", la cual analiza cómo la Ley 26.388 incorporó diversos delitos informáticos en el Código Penal de Argentina, adecuando la legislación nacional a las normas previstas en el Convenio sobre Ciberdelincuencia de Budapest.

Esta reforma actualizó la legislación penal argentina, también cambió la concepción en

conceptos legales que el avance tecnológico había quedado obsoletos, así como la incorporación de nuevos tipos penales y la actualización de algunos ya existentes. (Tesis los delitos informáticos en argentina a partir de la adhesión al convenio de Budapest, Carla Cruzado, 1 de marzo 2021) Honduras no ha formalizado su adhesión al Convenio de Budapest sobre ciberdelincuencia.

Sin embargo, ha mostrado interés en alinearse con sus directrices. En 2019, congresistas de la comisión especial multipartidaria del Congreso Nacional recomendaron la adhesión al Convenio, tras reuniones con miembros del programa GLACY+ en el Foro de presidentes de Poderes Legislativos de Centroamérica y la Cuenca del Caribe (FOPREL) en San Salvador. (IPANDETEC Centroamérica, 2020) Además, en una intervención ante las Naciones Unidas en 2020, Honduras expresó su preocupación por el incremento de delitos en el ámbito digital y destacó la necesidad de mejorar la cooperación internacional para combatir eficazmente estos crímenes, Con respecto a la estructura y considerando como punto de referencia las Convenciones de Palermo, el Convenio de Budapest y la Convención de Naciones Unidas contra la Corrupción, Honduras considera que la Convención debe de estructurarse con un preámbulo que describa su alcance y objetivos.

Un capítulo sobre criminalización y la persecución de la conducta delictiva en el ciberespacio. Un segundo apartado que contenga reglas de procedimiento, que reafirmen el debido proceso con herramientas jurídicas modernas, el respeto a los derechos humanos, incluyendo el derecho a la privacidad, a la protección de datos personales, a la protección de las víctimas; así como, los principios de necesidad y proporcionalidad.

Un capítulo relativo a la cooperación internacional, incluyendo la asistencia legal mutua. Un capítulo sobre asistencia técnica y fomento de capacidades, incluyendo el rol de la Oficina de las Naciones Unidas contra la Droga y el Delito y finalmente un mecanismo de implementación. (Intervención de Honduras Primer período de sesiones del Comité Ad Hoc encargado de elaborar una Convención Internacional sobre Ciberdelito 1 de marzo de 2022) La tesis titulada "Los delitos informáticos en el Código Penal Argentino: Análisis de la Ley 26.388 y su adecuación al Convenio de Budapest" examina cómo la Ley 26.388 incorporó diversos delitos informáticos en el Código Penal de Argentina, alineándose con las normas establecidas en el Convenio sobre Ciberdelincuencia de Budapest. Esta reforma no solo actualizó la legislación penal argentina, sino que también implicó un cambio en muchos conceptos legales que el avance tecnológico había

dejado obsoletos, así como la incorporación de nuevos tipos penales y la actualización de algunos ya existentes. (Linares, María Belén, 2020) La Ley 26.388, sancionada en 2008, introdujo modificaciones significativas en el Código Penal argentino para abordar la criminalidad informática. Entre las principales incorporaciones se encuentran: Delitos contra la integridad sexual: Se amplió la tipificación de la producción, distribución y tenencia de material de abuso sexual infantil, adaptando la legislación a los estándares internacionales. Violación de secretos y de la privacidad: Se incorporó el artículo 153 bis, que penaliza el acceso indebido a sistemas o datos informáticos de acceso restringido. Estafas informáticas: Se añadió el inciso 16 al artículo 173, que sanciona al que defraudare a otro mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema o la transmisión de datos. Daños informáticos: Se modificaron los artículos 183 y 184 para incluir daños a sistemas y datos informáticos, penalizando la destrucción, inutilización o alteración de datos, programas o sistemas informáticos. (Linares, María Belén, 2020) El propósito de estas reformas es adecuar la legislación argentina a los desafíos que plantea la ciberdelincuencia, proporcionando herramientas legales para la prevención, investigación y sanción de estos delitos.

La adecuación al Convenio de Budapest refuerza la cooperación internacional y establece estándares comunes para enfrentar la criminalidad informática. (Linares, María Belén, 2020) Para que Honduras se convierta en un país más seguro frente a los hackers y pueda detectar inmediatamente a los agresores cuando cometan un robo o hackeo de información, es necesario un enfoque integral que combine legislación, tecnología y cooperación internacional a través de un plan estructurado con medidas concretas:

1. Fortalecimiento del Marco Legal Honduras debería actualizar su legislación penal siguiendo modelos internacionales como el Convenio de Budapest (Tratado Internacional sobre Ciberdelincuencia). Para esto, se pueden implementar:

   • Reformas al Código Penal: Tipificar con mayor claridad delitos como el phishing, ransomware, espionaje digital y fraude cibernético. • Obligatoriedad de Reporte de Incidentes: Exigir a bancos, empresas de telecomunicaciones y entidades estatales informar inmediatamente sobre hackeos o fraudes. • Endurecimiento de Penas: Aumentar las sanciones para ciberdelincuentes, incluyendo penas de prisión más severas y sanciones económicas.

2. Creación de una Agencia Nacional de Ciberseguridad Esta entidad se encargaría de: • Monitoreo en tiempo real de amenazas: Analizar patrones de ataques y detectar actividad sospechosa en redes públicas y privadas. • Coordinación con Interpol y otras agencias: Compartir información sobre ciberdelincuentes con organismos internacionales. • Protección de Infraestructura Crítica: Defender instituciones gubernamentales, bancos y telecomunicaciones de ciberataques.

3. Implementación de Tecnologías de Detección en Tiempo Real

• Sistema de Inteligencia Artificial: Desarrollar software que analice el tráfico de datos y detecte accesos sospechosos en tiempo real.

• Autenticación Reforzada: Obligar a todas las instituciones a usar autenticación multifactor (MFA) y cifrado de datos avanzado.

• Monitoreo en Blockchain: Usar tecnología de cadena de bloques para rastrear transacciones financieras fraudulentas.

4. Creación de una Unidad Especializada en Ciberdelitos • Investigadores con formación en ciberseguridad: Expertos en rastreo digital y técnicas de hacking ético. • Colaboración con bancos y empresas tecnológicas: Implementar sistemas de alerta en transacciones sospechosas. • Infiltración en redes criminales: Uso de agentes encubiertos en la Dark Web para desmantelar redes de ciberdelincuentes.

5. Educación y Concienciación Pública • Campañas nacionales sobre ciberseguridad: Educar a la población sobre cómo evitar fraudes en línea. • Instrucción obligatoria en universidades y colegios: Enseñar seguridad digital como parte del currículo académico. • Simulacros de ciberataques: Entrenar a empleados públicos y privados en cómo reaccionar ante un ataque informático.

6. Implementación de un Sistema Nacional de Alertas Digitales • Alertas en tiempo real: Si se detecta una estafa o hackeo, enviar notificaciones inmediatas a bancos, empresas y usuarios afectados.

• Lista negra de estafadores: Crear una base de datos accesible para ciudadanos y empresas con números y correos electrónicos vinculados a fraudes (Plan nacional de gobierno digital 2023-2026) (Paso a paso para una política de ciberseguridad integral, IPANDEC) Diseñan ley para

proteger datos ante ciberdelincuentes.

El Diario La Prensa Hondureño, informó en 2023, que bases de datos privadas y públicas que contienen información personal de los hondureños, entre ellas el censo electoral de 2021, son vendidas en bitcoin en la internet oscura, lo cual vulnera aún más la seguridad de los ciudadanos, que ya son objeto de estafas y extorsiones cibernéticas. (LA PRENSA, Diseñan ley para proteger datos ante ciberdelincuentes, 2023).

El artículo de La Prensa titulado "Diseñan ley para proteger datos ante ciberdelincuentes" aborda los esfuerzos del Congreso Nacional de Honduras para fortalecer el marco legal en respuesta al incremento de delitos informáticos, como estafas, extorsiones y vaciado de cuentas bancarias.

El diputado Rafael Sarmiento destaca la elaboración de propuestas legislativas, una ley de firma electrónica, una ley de ciberseguridad y una ley de protección de datos personales, para salvaguardar la información de los ciudadanos en la era digital. El artículo también señala la preocupación por la recopilación indiscriminada de datos personales por parte de empresas como farmacias, supermercados y gasolineras, sin una regulación adecuada.

Esta falta de control facilita que dicha información sea vendida, tanto legal como ilegalmente, convirtiéndose en una herramienta para la comisión de delitos como estafas y extorsiones. Expertos en informática enfatizan la necesidad de que, además de la aprobación de nuevas leyes, se implemente una capacitación adecuada para jueces, fiscales y abogados en el manejo de tecnologías digitales y evidencia electrónica. Reivyn Cálix, hacker ético e investigador forense digital, subraya la importancia de formar a los operadores de justicia para garantizar la efectividad del nuevo marco legal y asegurar una correcta admisión y evaluación de las evidencias digitales en los procesos judiciales.

En resumen, el artículo destaca la iniciativa legislativa del Congreso Nacional para crear un conjunto de leyes destinadas a proteger los datos personales de los hondureños frente a la creciente amenaza de los ciberdelincuentes, así como la importancia de la capacitación del personal judicial para enfrentar eficazmente estos nuevos desafíos en el ámbito digital. (LA PRENSA, Diseñan ley para proteger datos ante ciberdelincuentes, 2023).

**Definiciones Conceptuales**

A continuación, se presentan las definiciones de los términos clave relacionados con tu investigación sobre phishing y ciberdelitos en Honduras:

1. 2.5.1 Phishing: Es una técnica de ingeniería social en la que los ciberdelincuentes se hacen pasar por entidades legítimas, como bancos o instituciones, para engañar a las personas y obtener información confidencial, como contraseñas o datos bancarios. (Gallego, D., & Norela, D. (2025).

2. 2.5.2 Spear Phishing: Variante del phishing que se dirige a individuos o empresas específicas. Los atacantes personalizan sus mensajes utilizando información detallada sobre la víctima para aumentar la probabilidad de éxito en el engaño. (KAPERSKY, Spear Phishing)

3. 2.5.3 Ransomware: Tipo de software malicioso que cifra los archivos

de una víctima, bloqueando su acceso. Los atacantes exigen un pago (rescate) para proporcionar la clave de descifrado y restaurar el acceso a los datos. (Ruiz Muñoz, Jorge Antonio, 2017)

4. 2.5.4 Ciberdelito: Actividad ilícita que se lleva a cabo a través de medios digitales o en el ciberespacio, incluyendo fraudes electrónicos, robo de identidad, ataques a sistemas informáticos y distribución de malware. (Blázquez, R., & Luis, J. (2014).

5. 2.5.5 Evidencia Digital: Información o datos almacenados o transmitidos en formato digital que pueden ser utilizados en procedimientos legales para demostrar hechos o acciones, como correos electrónicos, registros de chat, archivos y registros de acceso. (López, D. del V. (2018).

6. 2.5.6 Ciberseguridad: Conjunto de prácticas, medidas y tecnologías diseñadas para proteger sistemas informáticos, redes y datos contra accesos no autorizados, ataques o daños. (Estévez Herrera, J. (2025).

7. 2.5.7 Protección de Datos: Disciplina que se enfoca en salvaguardar la privacidad y los datos personales de individuos, asegurando que la recopilación, almacenamiento y procesamiento de dicha información se realice de manera segura

y conforme a la legislación vigente. (Pérez Rojas, D. R. O. (2023).

8. 2.5.8 Firma Electrónica: Conjunto de datos electrónicos que acompañan o están

asociados a un documento electrónico, y que permiten identificar al firmante, verificar la integridad del documento y garantizar el no repudio en el origen.

(Cristian, M. C., & Erick, R. C. (2021)

## 2.4 FORMULACION DE HIPOTESIS

### 2.4.1 Hipótesis General

Percepción de vulnerabilidad y desprotección ante el phishing de datos en Honduras

Se espera que los hondureños, naturales y jurídicas, desconozcan qué es el phishing de datos, cómo identificarlo y cómo protegerse, por la falta de educación digital y la falta de un marco legal específico. Además, se prevé que la población perciba al sistema de justicia penal como ineficaz para prevenir y sancionar estos delitos, lo que aumenta la sensación de vulnerabilidad e impunidad.

### 2.4.2 Hipótesis Especificas

-Familiaridad con el phishing, pero desconocimiento de sus riesgos reales Se prevé que la mayoría de los encuestados reconozca haber recibido correos electrónicos o mensajes sospechosos relacionados con phishing, pero pocos sabrán identificar estos intentos como ciberdelitos, demostrando un bajo nivel de conocimiento sobre la seguridad digital.

-Baja tasa de denuncias y desconfianza en las autoridades

Se espera que la mayoría de los encuestados no haya reportado intentos de phishing a las autoridades, ya sea por desconocimiento de cómo hacerlo, por falta de confianza en el sistema judicial o porque consideran que no se obtendría una solución efectiva.

-Deficiencias del marco legal hondureño ante el phishing

Se anticipa que los entrevistados, especialmente expertos en la materia, coincidan en que el marco legal hondureño es insuficiente para regular y sancionar el phishing, y que existe una necesidad urgente de reformarlo e incluir mecanismos más modernos de prevención y persecución.

-Necesidad de cooperación internacional y modernización tecnológica

Se estima que tanto la población como los expertos considerarán que la adopción de convenios internacionales, la implementación de tecnología avanzada y la creación de una

unidad especializada en ciberdelitos mejorarían significativamente la lucha contra el phishing en Honduras, pero también que dichas medidas aún están lejos de materializarse por falta de voluntad política y recursos.

# CAPÍTULO III. METODOLOGÍA

## 3.1 DISEÑO METODOLOGICO

La presente investigación empleara una metodología jurídica no experimental, Siendo el derecho una ciencia, cuenta con sus propias metodologías de la investigación, con un enfoque mixto, basada en el análisis empírico y comparativo, con el objetivo de evaluar la eficacia del sistema de justicia penal en Honduras frente a las estafas cibernéticas y el robo de identidad.

El análisis empírico permitirá estudiar casos concretos de cibercrímenes en el país, recopilando datos sobre la frecuencia de los delitos, las estrategias utilizadas por los ciberdelincuentes y la respuesta de las autoridades. Se examinarán informes oficiales, estadísticas judiciales y testimonios de afectados para obtener una visión realista del problema y determinar el nivel de vulnerabilidad de los usuarios hondureños.

Por otro lado, el análisis comparativo se enfocará en contrastar el marco legal hondureño con legislaciones más avanzadas en materia de ciberdelitos, con el fin de identificar vacíos normativos y estrategias exitosas que puedan adaptarse al contexto nacional. Se estudiarán experiencias de otros países con mecanismos más eficientes para la prevención, detección y sanción de estos delitos.

Esta metodología permitirá evaluar tanto la dimensión práctica como la normativa del problema, ofreciendo un enfoque integral para la formulación de estrategias legislativas, tecnológicas y de cooperación interinstitucional que contribuyan a la reducción del phishing y otros delitos cibernéticos en Honduras

La matriz de congruencia se define como: Una herramienta que brinda la oportunidad de abreviar el tiempo dedicado a la investigación, su utilidad permite organizar las etapas del proceso de investigación de manera que desde el principio exista una congruencia entre cada una de las partes involucradas en dicho procedimiento (Pedraza, 2001, p. 313).

La matriz de congruencia metodológica muestra un resumen de la investigación y permite comprobar la secuencia lógica. La siguiente tabla muestra la matriz de congruencia metodológica de esta investigación y señala la relación entre variables:

## 3.1 Tabla 1. Matriz Metodológica

| Título de Investigación | Objetivos de Investigación | | Variables | |
|---|---|---|---|---|
| | General | Específicos | Dependiente | Indepe |
| Estafas cibernéticas y robo de identidad en Honduras: un análisis de la eficacia de la respuesta del sistema de justicia penal. | Analizar la problemática del phishing de datos en Honduras, identificando sus tipos más frecuentes, las estrategias utilizadas por los cibercriminales, las deficiencias del marco legal vigente y las oportunidades de mejora, con el propósito de proponer estrategias legislativas, tecnológicas y de cooperación interinstitucional que contribuyan brindando una respuesta eficiente a la reducción de este delito en el país. | A. Identificar y analizar los tipos de cibercrímenes más frecuentes en Honduras, determinando su impacto en la seguridad digital y evaluando los factores que contribuyen a su proliferación, con Proponer estrategias de prevención y mitigación. | Eficacia del sistema de justicia penal en Honduras frente a las estafas cibernéticas y el robo de identidad. | Tipos de cib más frecuente Honduras. |
| | | Examinar las estrategias y métodos utilizados por los cibercriminales para ejecutar ataques de phishing en el mundo, y como Honduras se ve afectada ante esta realidad en la actualidad, identificando sus principales técnicas, plataformas de ataque y el nivel de vulnerabilidad de los usuarios, con el propósito de proponer medidas de prevención y concienciación. | | Estrategias y utilizados en los ataques phishing. |
| | | C. Analizar las principales deficiencias del marco legal hondureño en la lucha contra el phishing de datos, comparándolo con legislaciones más avanzadas a nivel internacional, con el fin de identificar vacíos normativos y proponer mejoras para una regulación más efectiva. | | Deficiencias legales honduras en la lucha c phishing. |
| | | D. Proponer estrategias legislativas, tecnológicas y de cooperación interinstitucional que puedan implementarse en Honduras para reducir la incidencia del phishing de datos en los próximos años, tomando como referencia modelos exitosos a nivel internacional y adaptándolos al contexto nacional. | | Propuestas d estrategias le tecnológicas cooperaciones interinstitucional |

Fuente: Propia

## 3.2 OPERACIONALIZACIÓN DE LAS VARIABLES

### Tabla 2. Matriz de la operacionalización de las variables

| Variable | Definicion conceptual | Definicion operacional | Dimensiones | Item |
|---|---|---|---|---|
| Tipos de cibercrímenes más frecuentes en Honduras. | Conjunto de delitos informáticos que afectan a personas y entidades en Honduras, incluyendo fraude, robo de identidad y ataques cibernéticos. | Identificación y clasificación de los principales cibercrímenes reportados en Honduras mediante análisis de casos y estadísticas oficiales. | - Phishing de Datos<br>- Fraude en línea<br>- Robo de identidad<br>- Acceso ilegal a sistemas<br>- Extorsión digital | ¿Alguna vez ha sido víctima de un cibercrimen en Honduras?<br>-¿Qué tipo de cibercrimen ha experimentado?<br>-¿Considera que los cibercrímenes han aumentado en Honduras en los últimos años?<br>-¿Reportó el incidente a las autoridades? |
| Estrategias y métodos utilizados en los ataques de phishing. | Técnicas empleadas por ciberdelincuentes para obtener información personal y financiera mediante engaños digitales. | Análisis de casos documentados de phishing en Honduras y comparación con estrategias utilizadas en otros países. | - Ingeniería social<br>- Suplantación de identidad<br>- Uso de malware<br>- Correos electrónicos fraudulentos | -¿Ha recibido correos electrónicos o mensajes sospechosos solicitando información personal?<br>-¿Qué estrategias de phishing ha identificado con mayor frecuencia?<br>-¿Cuál cree que es la forma más efectiva de prevenir un ataque de phishing? |
| Deficiencias del marco legal hondureño en la lucha contra el phishing. | Limitaciones normativas que dificultan la prevención, investigación y sanción de delitos de phishing en Honduras. | Evaluación de la legislación vigente en Honduras en comparación con leyes internacionales más avanzadas. | - Ambigüedad normativa<br>- Falta de mecanismos de supervisión<br>- Baja tasa de denuncias y sanciones<br>- Cooperación internacional insuficiente | -¿Cree que las leyes actuales en Honduras son efectivas para combatir el phishing?<br>-¿Cuáles considera que son las principales deficiencias del marco legal en la lucha contra el phishing?<br>-¿Confía en que las autoridades hondureñas pueden manejar adecuadamente los casos de phishing? |
| Propuestas de estrategias legislativas, tecnológicas y de cooperación interinstitucional. | Medidas destinadas a fortalecer la lucha contra el phishing mediante mejoras legales, uso de tecnología avanzada y trabajo conjunto entre instituciones. | Elaboración de un conjunto de recomendaciones basado en el análisis de buenas prácticas internacionales y necesidades del país. | - Reformas legales<br>- Implementación de tecnologías de ciberseguridad<br>- Capacitación institucional<br>- Alianzas público-privadas | -¿Qué medidas considera más importantes para combatir el phishing en Honduras?<br>-¿Cree que la cooperación internacional ayudaría a reducir los ataques de phishing en Honduras?<br>-¿Está dispuesto a recibir capacitación sobre cómo evitar ataques de phishing? |

Fuente: Propia

## 3.2 TIPO DE INVESTIGACION

La investigación exploratoria es un enfoque de estudio que se emplea cuando se busca obtener una comprensión inicial de un fenómeno poco estudiado o novedoso. Su objetivo es dar una visión general que permita identificar patrones, ideas o hipótesis que puedan investigarse con mayor profundidad en estudios posteriores. Este tipo de investigación se caracteriza por su flexibilidad y apertura, adaptándose a medida que se recopila nueva información. Es especialmente útil para familiarizarse con temas desconocidos y establecer las bases para futuras investigaciones más detalladas. (Teressa Kiss, 2024).

## 3.3 ENFOQUE DE LA INVESTIGACION

El enfoque de la investigación hace referencia a la perspectiva asumida o rutas para

aproximarse al conocimiento. En la teoría generalmente se mencionan tres enfoques: cuantitativo, cualitativo y mixto (combinación de los dos anteriores). El enfoque cuantitativo se basa en la recolección y análisis de datos numéricos para medir variables, establecer relaciones y realizar generalizaciones estadísticas.

Se utilizan mediciones estandarizadas c para obtener resultados comparables. Se emplean muestras grandes y representativas para garantizar precisión y validez en sus conclusiones.

Su análisis conlleva la aplicación de técnicas como pruebas de hipótesis y correlaciones para identificar patrones y relaciones significativas entre variables. Su enfoque es deductivo, formulando hipótesis que se prueban mediante evidencia empírica, lo que lo hace ampliamente utilizado en estudios científicos y sociales. (Miguel Ángel Medina Romero, Libro Método Mixto, 2023 Pag 16.)

El enfoque cualitativo busca comprender fenómenos complejos a través del análisis de datos no numéricos, como entrevistas y observaciones. Se enfoca en la interpretación de significados, se utilizan muestras pequeñas y selectivas para obtener una visión detallada del contexto estudiado. Su análisis es interpretativo e inductivo, permitiendo la generación de teorías a partir de los datos recopilados. (Miguel Ángel Medina Romero, Libro Método Mixto, 2023 Pag 17 -18.)

Por otro lado, el mixto combina enfoques cuantitativos y cualitativos para obtener una visión más completa de los fenómenos estudiados. Se basa en la integración de datos, recopilados de forma simultánea o secuencial, y en la triangulación, que permite contrastar y validar los resultados desde diferentes perspectivas. (Miguel Ángel Medina Romero, Libro Método Mixto, 2023 Pag 17 -18.)

La presente investigación tiene un enfoque cualitativo ya que busca conocer y describir la realidad hondureña respecto a la protección de datos personales para evitar la comercialización ilegal de bases de datos.

### 3.4 ALCANCE DE LA INVESTIGACIÓN

Resulta obligatorio conocer el alcance del estudio para poder definir una estrategia de investigación, estableciendo sus límites conceptuales y metodológicos. La teoría determina cuatro tipos de alcances: exploratorio, descriptivo, correlacional y explicativo.

En el alcance exploratorio, la investigación se enfoca en el estudio de fenómenos poco examinados, permitiendo identificar sus características principales y generar una comprensión inicial del tema.

El fenómeno de estudio ya se ha identificado previamente, por lo que el objetivo principal es analizar su presencia en un grupo específico, detallando sus atributos y comportamientos.

En el alcance correlacional, la investigación plantea una hipótesis que establece la relación entre dos o más variables, con el propósito de determinar cómo una afecta a la otra. En el alcance explicativo, el propósito es profundizar en la comprensión de los fenómenos estudiados, identificando sus causas y factores determinantes para ofrecer una explicación fundamentada sobre su origen y comportamiento. (Carlos Ramos Galarza, Los Alcances de la Investigación, 2020) La presente investigación tiene un alcance: Descriptivo

## 3.5 METODOS DE LA INVESTIGACIÓN

Los métodos de investigación se definen como los procedimientos utilizados para generar nuevos conocimientos, establecer reglas específicas para el análisis de fenómenos y desarrollar estrategias de estudio que permitan avanzar en la comprensión de un tema (Mejía, 2006, p. 166). En el ámbito jurídico, estos métodos se relacionan con la interpretación y la aplicación de normas metodológicas que facilitan el análisis del derecho desde distintas perspectivas (Mejía, 2006, p. 166). A continuación, se presentan los principales métodos empleados en la investigación jurídica, destacando que, para el desarrollo del presente estudio, se han seleccionado el método inductivo, el intuitivo, el comparado y el sistémico.

### Método Inductivo

El método inductivo sigue un proceso en el que se parte de casos específicos para extraer conclusiones generales. Se basa en el análisis de situaciones particulares para identificar patrones o regularidades que puedan aplicarse a contextos similares. Este enfoque es especialmente útil en estudios cualitativos, ya que permite generar hipótesis y establecer tendencias a partir de la observación de casos concretos (Villabella Armengo, 2015, p. 938). Según Villabella (2015), en el ámbito jurídico, la inducción posibilita la construcción de teorías mediante el estudio de hechos particulares, permitiendo establecer principios generales y formular conclusiones fundamentadas

(p. 983). Por su parte, Ponce (1996) señala que este método facilita la identificación de tendencias al examinar diversos casos jurídicos, lo que lleva a conclusiones generales aplicables a otros contextos (p. 69).

**Método Histórico**

El método histórico permite analizar la evolución de un fenómeno a lo largo del tiempo, destacando las principales etapas de su desarrollo, las tendencias que han marcado su transformación y las causas que han influido en su progreso.

En el ámbito del derecho, este método es útil para comprender cómo ciertas normativas han cambiado con el tiempo y cómo han influido en la regulación actual (Villabella, 2015, pp. 936- 937). Su aplicación facilita el estudio de antecedentes jurídicos y la valoración de normas pasadas para entender su impacto en la legislación vigente.

Además, permite analizar la evolución de instituciones jurídicas, estableciendo una conexión entre su origen y su estado actual (Villabella, 2015, p. 937).

**Método de Derecho Comparado**

Este método es característico de la investigación jurídica y consiste en contrastar diferentes sistemas normativos o instituciones legales con el propósito de identificar similitudes, diferencias y tendencias.

Su aplicación permite establecer modelos exitosos, clasificar conceptos jurídicos y evaluar el impacto de ciertas regulaciones en distintos contextos (Villabella, 2015, p. 940). Según la doctrina (Villabella Armengo, 2015), la comparación jurídica puede realizarse desde diferentes perspectivas:

• Comparación interna: Cuando se analizan elementos dentro de un mismo sistema jurídico.

• Comparación externa: Cuando se estudian regulaciones pertenecientes a sistemas jurídicos distintos.

• Comparación técnica: Cuando el análisis se enfoca en el lenguaje jurídico y su aplicación textual.

• Comparación sociológica-jurídica: Cuando se consideran factores históricos, culturales y sociales en la comparación de normas.

**Método Dialectico**

El método dialéctico se basa en la confrontación de ideas mediante la exposición de una tesis y su contraposición con una antítesis, con el fin de alcanzar una síntesis que permita una mejor comprensión del fenómeno analizado. En el campo jurídico, este método se utiliza para evaluar diferentes interpretaciones de una norma y llegar a un consenso fundamentado (Ponce, 1996, p. 70).

**Método Sistémico**

También conocido como método estructural-funcional, este enfoque permite analizar un objeto dentro de un sistema más amplio, compuesto por diversos elementos interconectados. Su aplicación en el ámbito jurídico facilita la organización del conocimiento al agrupar conceptos en estructuras coherentes, identificando cómo interactúan y se influyen entre sí (Villabella, 2015, p. 939). A través de este método, se examina cada parte de un sistema legal para comprender su función, su jerarquía dentro del conjunto normativo y su interacción con otras normas. Es especialmente útil cuando se estudian regulaciones complejas que requieren una visión integral de su funcionamiento (Villabella, 2015, p. 939).

**Método Hermenéutico**

El método hermenéutico se centra en la interpretación de textos jurídicos a partir de su contexto lingüístico y cultural. Su nombre proviene del vocablo griego hermeneutiké, asociado a la figura de Hermes, quien en la mitología griega era el mensajero de los dioses. En el ámbito jurídico, este método permite analizar el significado de normas legales, considerando factores históricos, lingüísticos y psicológicos para comprender la intención del legislador (Villabella, 2015, p. 944).

## 3.6 DISEÑO DE LA INVESTIGACION

El propósito principal de un diseño experimental es identificar si existen diferencias en los resultados al aplicar distintos tratamientos dentro de un experimento y, en caso afirmativo, medir dichas diferencias. Este diseño se basa en un proceso estructurado que permite evaluar cuantitativamente cómo una variable influye sobre otra, lo que implica la manipulación o regulación de la variable independiente. Para ello, se requiere un esquema de acción que puede desarrollarse en distintas fases, como la implementación de un programa de intervención o

mediante un enfoque escalonado que establezca parámetros dentro de ciertos rangos. (José Arias Gonzales, 2021).

En este tipo de diseño no se aplican estímulos ni se modifican las condiciones experimentales de las variables de estudio ya que todo sucedió. Los participantes son observados dentro de su entorno natural sin alterar las circunstancias, y no se realiza manipulación alguna de las variables analizadas. En este enfoque existen dos categorías principales: transversal y longitudinal, cuya diferencia radica en el período de tiempo en que se realizan. (José Arias Gonzales, 2021. Pag 73-74)

**Diseño Transversal**

Este diseño se basa en la recolección de datos en un solo momento, sin seguimiento posterior. Se asemeja a tomar una imagen instantánea de la realidad para su posterior análisis en la investigación. Puede emplearse con fines exploratorios, descriptivos o correlacionales. De acuerdo con Manterola, Quiroz, Salazar y García (2019), su característica fundamental es que se realiza en una única instancia, por lo que no permite observar cambios en el tiempo. (José Arias Gonzales, 2021. Pag 78)

**Diseño Longitudinal**

A diferencia del diseño transversal, este enfoque estudia la evolución de las variables en el tiempo, sin intervención directa en su desarrollo. No se alteran las condiciones del fenómeno, sino que se registra su transformación a lo largo de diferentes periodos. Un estudio longitudinal requiere más de dos mediciones para poder comparar los resultados y analizar tendencias en procesos de cambio. Es útil en investigaciones sobre fenómenos sociales, patrones de comportamiento o análisis de tendencias. (José Arias Gonzales, 2021. Pag 79)

Esta Investigación tendrá un diseño no experimental cualitativo donde se buscará comprender, analizar e interpretar el fenómeno del phishing de datos en Honduras sin manipular variables, enfocándose en la recolección de información a través de fuentes documentales, entrevistas y análisis normativo.

Dado que no se aplicarán estímulos ni se alterarán las condiciones del fenómeno, el estudio se centrará en observar y describir cómo ocurre el phishing, qué impacto tiene en los usuarios y qué deficiencias existen en el marco legal hondureño para enfrentarlo.

## 3.7 POBLACION

La población o universo se define como el conjunto de elementos que comparten ciertas características específicas dentro de una investigación (Hernández et al., 2014, p. 174). En el caso de este estudio, la población está compuesta por instituciones y organismos en Honduras encargados de la protección de datos personales, así como por usuarios que han sido víctimas de phishing y robo de información digital, con el objetivo de analizar su nivel de vulnerabilidad y las estrategias disponibles para su protección.

### MUESTRA

La muestra se refiere a un segmento de entre todo el universo de observación (población) sobre el cual se realizará el estudio. Es un grupo representativo de la población al que se le aplicarán entrevistas, encuestas, cuestionarios, pruebas, etc., para obtener los datos requeridos por la investigación (Olvera, 2015, p. 64 y 127). Dado que el enfoque de esta investigación es mixto (cualitativo y cuantitativo), el estudio requerirá una muestra que combine criterios de representatividad estadística (para la parte cuantitativa) y criterios de selección intencional o por conveniencia (para la parte cualitativa).

Tipo de Muestra para realizar en el Proyecto • Para el enfoque cuantitativo: Se utilizará una muestra probabilística o aleatoria dentro de una población definida, permitiendo generalizar los resultados obtenidos en encuestas sobre phishing y protección de datos en Honduras.

Para el enfoque cualitativo: Se empleará una muestra intencional o por conveniencia, seleccionando expertos y víctimas de phishing que puedan aportar información relevante a través de entrevistas en profundidad.

¿A quiénes se dirigirán las encuestas y entrevistas?

1. Usuarios afectados por phishing: Personas que han sido víctimas de fraudes electrónicos, robo de identidad o estafas digitales en Honduras.

2. Empresas y comercios electrónicos: Negocios que manejan datos personales de sus clientes y enfrentan riesgos de ciberataques.

3. Expertos en ciberseguridad y derecho digital: Profesionales en el ámbito tecnológico y jurídico que puedan aportar información sobre el estado de la legislación y las estrategias de protección.

4. Instituciones gubernamentales y organismos de regulación: Entidades como la Comisión Nacional de Bancos y Seguros (CNBS), el Ministerio Público y la Policía Cibernética de Honduras, que trabajan en la prevención y sanción de delitos cibernéticos. Este tipo de muestreo garantizará una visión integral del problema, combinando datos estadísticos con análisis en profundidad sobre las causas y posibles soluciones del phishing en Honduras.

## 3.8 FUENTES DE INFORMACION

### Fuentes Primarias

Las fuentes primarias proporcionan datos de primera mano, documentos con resultados de los estudios correspondientes. Algunos ejemplos de fuentes primarias son libros, artículos de publicaciones periódicas, monografías, tesis, disertaciones, documentos oficiales, reportes de asociaciones, testimonios de expertos, documentales, foros, páginas de internet, entre otras (Hernández et al., 2014, p. 72).

En la presente investigación, las fuentes primarias son las encuestas y entrevistas realizadas a la muestra seleccionada, la Constitución de la República de Honduras, El Código Penal de Honduras, Ley de Firmas Electrónicas, La Ley de Comercio electrónico, Derechos de los Consumidores, Proyecto de Ley de Protección de Datos Personales, Convenios Internacionales (Budapest) o legislación comparada internacional, libros, tesis, revistas académicas, noticias y reportes de asociaciones.

### Fuentes Secundarias

Las fuentes secundarias tienen información primaria, sintetizada y/o reorganizada. En esta investigación las fuentes secundarias son foros de internet, diccionarios, enciclopedias jurídicas, videos, comentarios de expertos, entre otros.

### Técnicas de recolección de Datos

Para llevar a cabo esta investigación, es fundamental definir las técnicas e instrumentos que se emplearán para medir las variables y responder a la pregunta principal del estudio. La mayoría de estos instrumentos deben construirse en función de las variables específicas que se desean evaluar.

Una vez diseñados, se aplican a la muestra seleccionada para recopilar los datos que luego se presentarán y analizarán.

Los instrumentos que se utilizarán en esta investigación son: Encuestas: Una encuesta se define como la "búsqueda sistemática de información en la que el investigador pregunta a los sujetos sobre los datos que desea obtener para luego acumular esos datos individuales y realizar con ellos una evaluación".

En este estudio, se usará un cuestionario diseñado por el investigador para conocer la opinión de la muestra de la población sobre la situación de los ataques de phishing de datos en Honduras Entrevistas no estructuradas: Una entrevista es una conversación entre dos o más personas sobre un tema que sigue ciertos esquemas o pautas.

Las entrevistas no estructuradas son flexibles y permiten incorporar temas de interés que surjan a partir de las respuestas de los entrevistados. Para esta investigación, se entrevistarán a expertos en materia de ciberdelitos y phishing de datos, como abogados e ingenieros en sistemas e informáticos, quienes ofrecerán su opinión sobre los aciertos y vacíos en la aplicación del anteproyecto de ley con el convenio de Budapest como propuesta de solución.

**Limitaciones de la investigación**

Dentro de las limitaciones de esta investigación, hubo dificultades para encontrar el personal correcto y con conocimiento sobre el phishing de datos. Se tenía una fecha prevista para la realización de las entrevistas en la CNBS, Conatel y el Ministerio Público, pero por falta de contactos personales, accesos a las diferentes instituciones, el no trabajar en ninguna de estas instituciones y dificultades de horarios por parte de las personas a entrevistar, Las entrevistas no se realizaron en el tiempo objetivo, se tardaron de 1 a 2 semanas más de lo previsto en llevarse a cabo.

Limitaciones conceptuales por parte de algunos miembros entrevistados, es decir, poco vocabulario técnico sobre definiciones conceptuales de ciberdelitos y ciberseguridad, por parte del abogado morales de Fe Prosi y del Ingeniero de Conatel (Esto no interfirió con la información esencial, ni la comparativa de respuestas recibidas en las 3 instituciones, ya que fueron resultados muy semejantes)

# CAPÍTULO IV. RESULTADOS Y ANÁLISIS

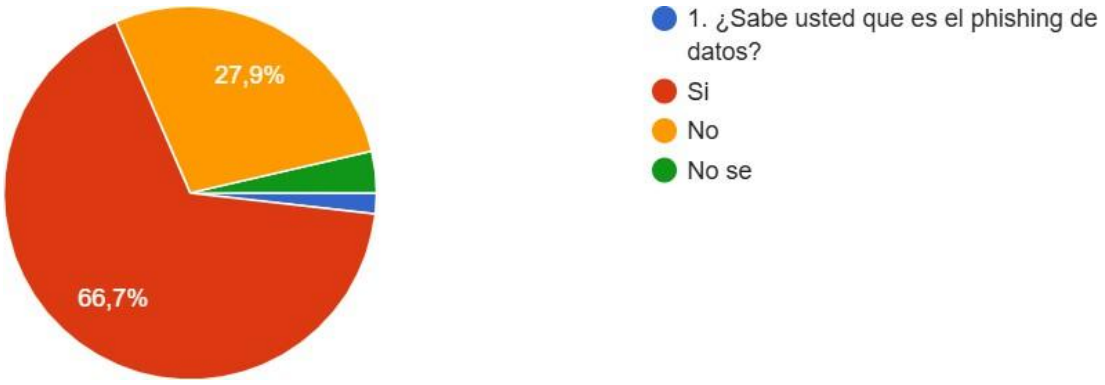
## 4.1Resultados

Este instrumento fue aplicado de forma aleatoria y digital a través de la Modalidad de Google Forms donde se obtuvieron 111 respuestas en total. El objetivo de la encuesta era recopilar diferentes criterios generales de diferentes hondureños y poder evaluar el conocimiento actual, la concientización actual, la orientación general que tiene el hondureño sobre el tema y la opinión jurídica del ciudadano hondureño sobre el phishing de datos como ciberdelito en el País.

Esta encuesta proporciono resultados que formaron una base critica en real y refleja desde una perspectiva general y no técnica, que puntos podrían considerarse para comenzar a poner mayor atención y enfoque, que permitirán como resultado, brindar las correctas propuestas resolutivas para familiarizar y proteger al ciudadano hondureño ante este ciberdelito.

### 4.1.1 Análisis individual de las respuestas de la encuesta aplicada

**Figura 12. Sobre el concepto de phishing**



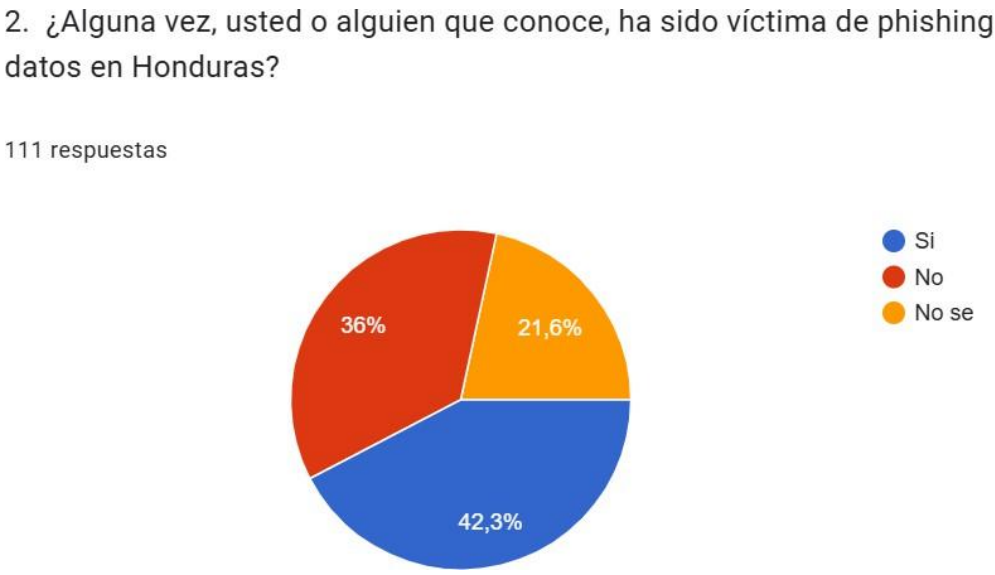

Fuente: Propia.

En la primera pregunta de la encuesta, los resultados obtenidos respaldan la hipótesis formulada. De 111 encuestados, el 66.7 % conocía el concepto de "phishing de datos". Este dato evidencia un nivel considerable de familiarización con este tipo de ciberdelito dentro de la población encuestada, lo cual es un indicativo positivo respecto a la concienciación ciudadana en materia de seguridad digital. El 27.9% de los participantes manifestó desconocer el término, lo que

muestra una oportunidad significativa para diseñar e implementar estrategias educativas y de sensibilización orientadas a fortalecer la cultura de ciberseguridad en el país.

Estos hallazgos permiten identificar no solo el grado de conocimiento existente, sino también áreas críticas donde se requiere un enfoque proactivo para mitigar riesgos asociados al phishing, contribuyendo así a la construcción de un entorno digital más seguro y resiliente para la sociedad hondureña.

**Figura 13. Víctimas del Ciberdelito en Investigación**



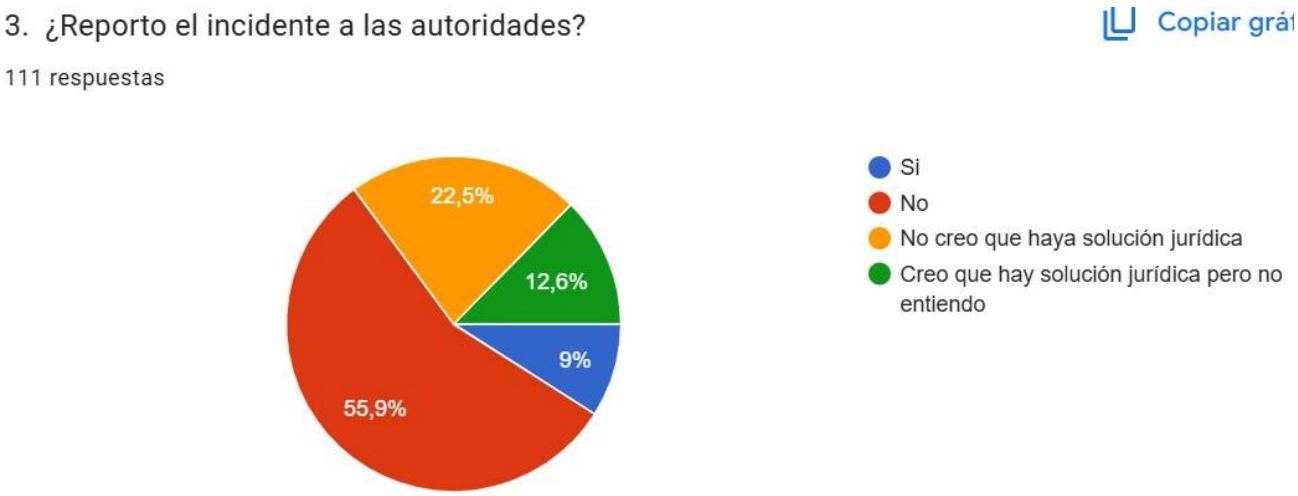

Fuente: Propia

En la segunda pregunta de la encuesta, los resultados obtenidos corroboran nuevamente la hipótesis planteada. De los 111 participantes, el 42.3% indicó que ellos mismos o alguien que conocen ha sido víctima de phishing de datos en Honduras. Este hallazgo revela un alto grado de exposición de la población a este tipo de ciberdelito, evidenciando la prevalencia del phishing en el entorno digital hondureño.

Por otro lado, el 36% de los encuestados respondió negativamente, lo cual, si bien es un dato alentador, no debe interpretarse como una ausencia de riesgo, sino más bien como una oportunidad para reforzar las medidas preventivas y educativas. Adicionalmente, el 21.6% de los participantes expresó no saber si han sido víctimas o si conocen a alguien que lo haya sido. Este porcentaje resalta un área crítica de desconocimiento y potencial vulnerabilidad, alineándose con los resultados de la primera pregunta respecto a la falta de familiarización con el concepto de phishing.

Fuente: Propia

**Figura 14. Reportes de las Victimas a las autoridades de Honduras**




Los resultados de la tercera pregunta revelan un panorama preocupante respecto al reporte de incidentes de phishing de datos a las autoridades en Honduras. Solo el 9 % de los encuestados afirmó haber denunciado el incidente, lo que evidencia una baja participación ciudadana en la notificación formal de estos ciberdelitos.

Un 55,9 % de los participantes manifestó no haber reportado el incidente, lo que sugiere barreras significativas, ya sea por desconocer los canales de denuncia, desconfianza en las instituciones o falta de seguimiento efectivo a los casos reportados.

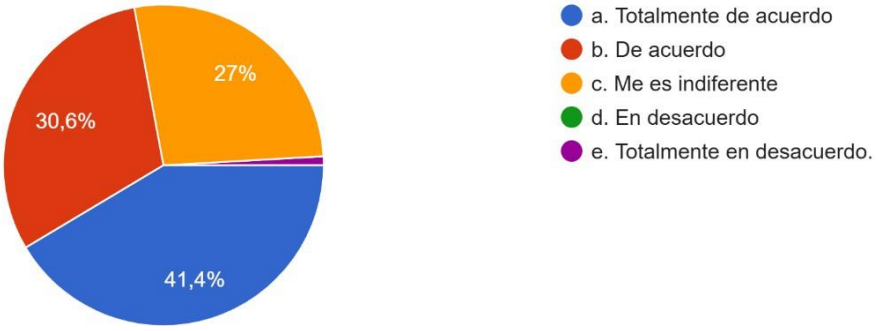
Además, el 22.5% de los encuestados expresó no creer que exista una solución jurídica para el phishing, mientras que el 12.6% indicó que, aunque perciben la posibilidad de una solución legal, no comprenden del todo el proceso. Estos datos reflejan una brecha crítica en la educación y sensibilización legal de la población, que podría estar limitando la efectividad de las acciones gubernamentales contra el ciberdelito.

Fuente: Propia

**Figura 15. Aumento del Phishing de Datos en los últimos 5 anos**

4. ¿Considera que el phishing de datos ha aumentado en Honduras en los últimos 5 años?

111 respuestas




En la cuarta pregunta de la encuesta, los resultados obtenidos reafirman la hipótesis planteada. Ante la consulta sobre si consideran que el phishing de datos ha aumentado en Honduras en los últimos 5 años, se observó una tendencia clara hacia la percepción de un incremento en este tipo de ciberdelito.

El 41.4% de los encuestados se mostró "totalmente de acuerdo", lo cual evidencia una alta sensibilización y posiblemente una mayor exposición a información relacionada con la ciberseguridad. Este dato es relevante, ya que sugiere que una parte considerable de la población ha notado cambios en la frecuencia o gravedad de los incidentes de phishing.

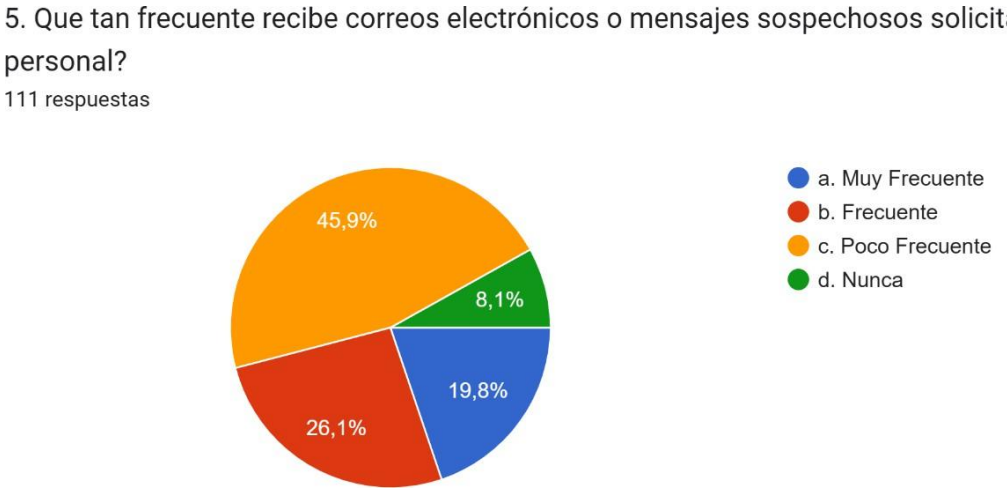
Además, un 30.6% se declaró "de acuerdo", elevando al 72% el porcentaje total de personas que perciben un aumento del phishing de datos. Esta cifra corrobora la hipótesis inicial y destaca la visibilidad de las amenazas digitales en el país.

Por otro lado, el 27% de los participantes indicó que el tema "les es indiferente". Aunque a primera vista podría interpretarse como falta de interés, este resultado podría reflejar un bajo nivel de educación digital o una ausencia de experiencias directas con el phishing. Esto representa una oportunidad valiosa para desarrollar campañas de sensibilización orientadas a transformar la indiferencia en conciencia activa, especialmente en aquellos que podrían no percibir el riesgo hasta enfrentarlo de manera directa.

Estos hallazgos permiten no solo validar la hipótesis, sino también identificar áreas críticas donde es necesario implementar estrategias educativas y preventivas, con el fin de promover un

entorno digital más seguro y resiliente para la población hondureña

**Figura 16**




Los resultados de la quinta pregunta de la encuesta también muestran estadísticas ampliamente coherentes y evidentes, continuando, reafirmando la hipótesis planteada. Al consultar la frecuencia con la que los encuestados reciben correos electrónicos o mensajes sospechosos solicitando información personal, se observa un alto nivel de exposición al phishing de datos.

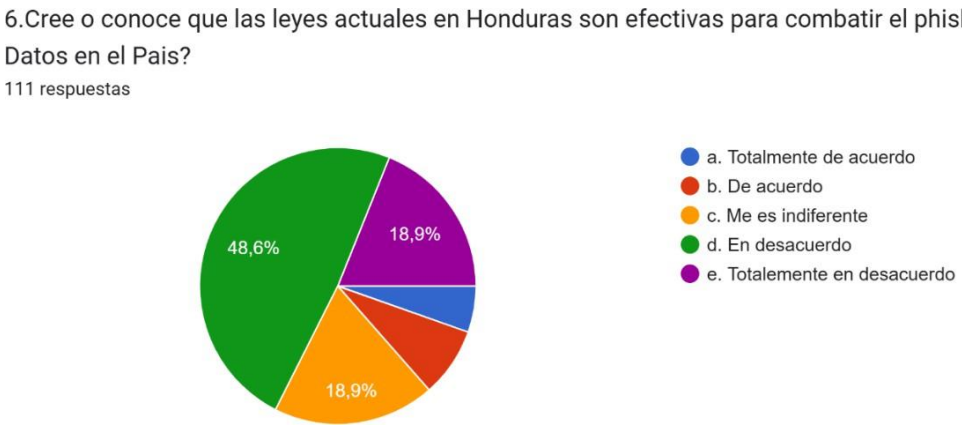
El 45.9% de los participantes indicó que esto ocurre de manera "Poco Frecuente", lo cual, aunque sugiere una exposición moderada, no deja de ser preocupante, ya que demuestra que casi la mitad de los encuestados ha recibido al menos algunos intentos de phishing.

El 26.1% respondió Frecuente", y el 19.8% señaló Muy Frecuente, lo que en conjunto representa un 45.9% adicional de personas con una exposición regular o constante a este tipo de amenazas. Este dato es clave, ya que refleja que una cantidad considerable de la población está en riesgo de ser víctima de ciberataques, subrayando la urgencia de fortalecer las medidas de prevención y la educación en ciberseguridad.

Por otro lado, solo un 8.1% mencionó "Nunca" haber recibido correos o mensajes sospechosos. Aunque esta cifra podría parecer tranquilizadora, es importante no subestimar la amenaza, ya que la baja percepción de riesgo podría derivarse de la falta de habilidades para identificar correctamente los intentos de phishing.

**Figura 17. Conocimiento de la población hondureña sobre las leyes y efectividad de**

**estas contra el phishing**




Los resultados de la sexta pregunta de la encuesta continúan reafirmando la hipótesis planteada.

Al consultar si las leyes actuales en Honduras son efectivas para combatir el phishing de datos en el país, se percibe una clara falta de confianza en el marco legal vigente.

El 48.6% de los encuestados respondió "En desacuerdo", lo cual evidencia que casi la mitad de la población no percibe las leyes como herramientas efectivas contra este tipo de ciberdelito. Este dato subraya una posible deficiencia en la aplicación de las leyes, en la comunicación de su efectividad o en la falta de resultados visibles en la protección de los ciudadanos frente al phishing.

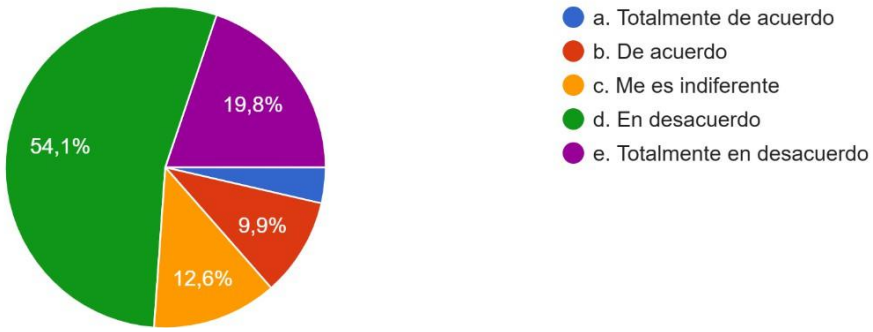
Además, se registró un empate del 18.9% entre quienes indicaron "Me es indiferente" y "Totalmente en desacuerdo". Este empate refleja tanto una posible apatía o desconocimiento sobre el tema, como una crítica directa a la incapacidad del sistema legal para abordar de manera efectiva los casos de phishing. La indiferencia podría ser una señal de desinformación o de desconfianza hacia las instituciones, mientras que la percepción negativa más radical indica una insatisfacción profunda con el estado actual de la ciberseguridad en el país.

El resto de los encuestados distribuyó sus respuestas entre "Totalmente de acuerdo" y "De acuerdo", lo cual sugiere que solo una minoría percibe que el marco legal cumple su función de manera adecuada.

Figura 18

7. Confía en que las autoridades hondureñas puedan manejar adecuadamente los casos de phishing de datos?

111 respuestas

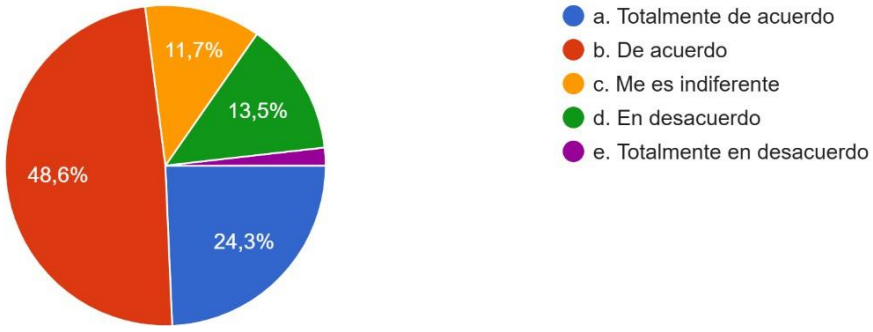



Los resultados de la pregunta número 7, también reafirman la hipótesis planteada. El 54.1% de los 111 encuestados expresa su desacuerdo en que las autoridades hondureñas puedan manejar adecuadamente los casos de phishing de datos. Este dato refleja una clara desconfianza hacia el sistema de justicia del país en relación con la capacidad de las autoridades para gestionar este tipo de delitos cibernéticos. Aunque un 19.8% confía en que las autoridades pueden manejar la situación, el porcentaje de desconfianza es considerablemente mayor, lo que pone de relieve la necesidad urgente de fortalecer la capacidad institucional y la confianza pública en el manejo de delitos de esta naturaleza.

Figura 19

8. Bajo un contexto jurídico, cree que la cooperación internacional con convenios internacionales, como una estrategia legislativa, ¿ayudaría a reducir los ataques de phishing de datos en Honduras?

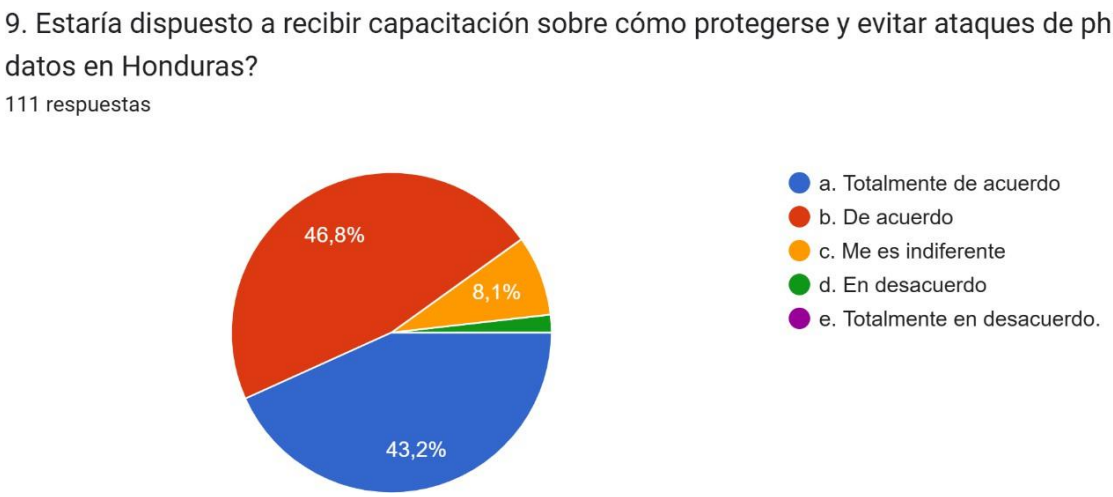
111 respuestas




Los resultados de la pregunta número 8 siguen respaldando la hipótesis planteada, ya que la mayoría de los encuestados (48.6%) están de acuerdo con la cooperación internacional mediante convenios internacionales como estrategia legislativa para reducir los ataques de phishing en

Honduras. Además, el 24.3% está totalmente de acuerdo, lo que sugiere un fuerte apoyo a la idea de que la cooperación internacional podría ser efectiva en la lucha contra este tipo de delitos. Aunque un 13.5 % se mostró en desacuerdo y un 11.7 % indiferente, la tendencia favorece aplicar estas estrategias como medida relevante en el contexto legal del país.

Figura 20




Los resultados de la pregunta número 9 muestran una alta disposición entre los encuestados para recibir capacitación sobre cómo protegerse y evitar ataques de phishing de datos en Honduras. Un 46.8% está de acuerdo y un 43.2% está totalmente de acuerdo, lo que indica un interés significativo en mejorar la protección contra este tipo de amenazas. Solo un 8.1% expresó indiferencia, lo que sugiere que la mayoría de las personas están conscientes de la importancia de estar preparados para enfrentar los riesgos de phishing. Estos resultados destacan la relevancia de ofrecer programas educativos y capacitaciones para fortalecer la seguridad digital en el país.

### 4.1.2 Síntesis General de los Resultados de la Encuesta sobre el Phishing de Datos en Honduras

La encuesta aplicada a 111 hondureños de manera digital y aleatoria reveló importantes hallazgos respecto al conocimiento, percepción y postura jurídica de la población sobre el phishing de datos como ciberdelito en el país. 1. Conocimiento sobre el Phishing: El 66.7% de los encuestados indicó conocer el concepto de phishing, lo cual es un indicativo positivo respecto a la concienciación en ciberseguridad. Sin embargo, el 27.9% no conocía el término, lo que evidencia la necesidad de más educación en esta área.

2. Exposición al Phishing: El 42.3% de los encuestados o alguien cercano ha sido víctima

de este ciberdelito, lo que refleja una alta exposición al riesgo. Además, un 45.9% afirmó recibir mensajes sospechosos con poca frecuencia, mientras que un 45.9% adicional reportó recibirlos con frecuencia o muy frecuentemente.

3. Reporte a las Autoridades: Solo el 9% de las víctimas de phishing reportaron el incidente a las autoridades, lo que sugiere barreras significativas para la denuncia, ya sea por desconfianza, desconocimiento o falta de seguimiento de los casos.

4. Percepción del Aumento del Phishing: El 72% de los encuestados percibe que los ataques de phishing han aumentado en los últimos 5 años, mostrando una alta sensibilización y necesidad de acciones preventivas.

5. Confianza en el Marco Legal: El 48.6% considera que las leyes actuales no son efectivas para combatir el phishing, y un 54.1% expresó desconfianza en la capacidad de las autoridades para gestionar estos casos. Estos datos reflejan una percepción negativa hacia el sistema de justicia y su capacidad de respuesta frente a los ciberdelitos.

6. Cooperación Internacional: La mayoría (48.6%) apoya la cooperación internacional mediante convenios como estrategia legislativa para reducir los ataques de phishing, lo cual indica un interés en soluciones más amplias y estructuradas.

7. Capacitación y Educación: Un 90% de los encuestados estaría dispuesto a recibir capacitación para protegerse del phishing, mostrando un fuerte interés en aprender cómo evitar este tipo de amenazas digitales. Conclusión: Los resultados de la encuesta destacan una significativa necesidad de mejorar la educación en ciberseguridad, reforzar el marco legal y las capacidades institucionales, y promover la cooperación internacional como medidas para mitigar el phishing de datos en Honduras.

### 4.2 Análisis de la Entrevista a la CNBS (Comisión Nacional de Bancas y Seguros) al Supervisor de Riesgos Tecnológicos

La siguiente entrevista fue realizada al Ingeniero Carlos Augusto Funez, Supervisor de Riesgo Tecnológico en la Comisión Nacional de Bancas y Seguros (CNBS). Su experiencia proporciona una visión técnica y estratégica sobre las modalidades de phishing más comunes en Honduras, las principales deficiencias del sistema de justicia penal para enfrentar estos delitos y las medidas que podrían implementarse para fortalecer la ciberseguridad en el país.

Preguntas Realizadas ¿Qué tipos de phishing o robo de datos personales, ha identificado con mayor frecuencia en Honduras en los últimos 5 años?

¿Qué principales deficiencias considera el sistema de justicia penal en Honduras para combatir el phishing de datos?

¿Cuál cree que es la forma de prevención más efectiva, que el marco legal en honduras podría implementar para prevenir más ataques de phishing de datos en el país?

¿Qué estrategia o estrategias tecnológicas considera que se deben implementar en Honduras, para comenzar a darle fin a los ataques de phishing de datos en el país?

¿Como considera que el sistema de justicia penal en Honduras podría responder eficazmente al delito de phishing de datos? 4.2.3

Respuestas:

Se describió la información proporcionada por el ingeniero Carlos Augusto Funez, quien desde su posición como Supervisor de Riesgos Tecnológicos en la Comisión Nacional de Bancas y Seguros (CNBS), expone una visión técnica y especializada sobre el panorama del phishing de datos en Honduras en los últimos 5 años. Tipos de Phishing más frecuentes en Honduras en los últimos 5 años.

El ingeniero Funez identifica una variedad de métodos empleados por los ciberdelincuentes para obtener datos personales y financieros. Entre los más recurrentes se destacan:

• Envío de correos masivos y dirigidos para robar credenciales.

• Creación de páginas web falsas que suplantan la identidad de bancos en buscadores como Google

• Llamadas telefónicas y mensajes de WhatsApp para engañar a las víctimas.

• Estafas mediante la venta de productos en plataformas como Marketplace. Este diagnóstico refleja la diversificación de las técnicas utilizadas, resaltando cómo los atacantes se adaptan a las plataformas y hábitos digitales de los hondureños. Deficiencias en el Sistema de Justicia Penal

• El experto menciono varios obstáculos que limitan la lucha contra el phishing en

Honduras:

• Ausencia de adhesión al Convenio de Budapest (tratado internacional sobre ciberdelincuencia), lo que dificulta la colaboración internacional.

• Falta de recursos humanos, tecnológicos y de capacitación en el Ministerio Público.

• Carencia de una estrategia nacional de ciberseguridad que coordine esfuerzos a nivel país.

• Inexistencia de una ley de Protección de Datos, dejando a los ciudadanos vulnerables ante el robo de su información. Estas deficiencias no solo complican la investigación de los casos, sino que también debilitan la capacidad del Estado para prevenir y sancionar estos delitos. Prevención desde el marco legal El ingeniero propone medidas clave para fortalecer la prevención:

• Campañas de concientización para educar a la población sobre los riesgos y buenas prácticas en el uso de la tecnología.

• Reformas educativas que incorporen la ciberseguridad en el pensum académico desde etapas tempranas.

• Implementación de buenas prácticas de seguridad de la información tanto en el sector público como privado.

Estas propuestas apuntan a una estrategia integral que combine educación, regulación y responsabilidad empresarial para crear una cultura nacional de ciberseguridad. Estrategias tecnológicas recomendadas El ingeniero Funez enfatizo que el phishing es una amenaza en constante evolución y, aunque erradicarlo es improbable, es posible reducir significativamente el riesgo.

Entre las estrategias tecnológicas sugeridas destacan:

• Autenticación multifactor (2FA), especialmente versiones resistentes al phishing.

• Autenticación sin contraseña (passwordless) y biometría.

• Sistemas de monitoreo basados en el comportamiento del usuario, diseñados para detectar actividades inusuales prevenir ataques en tiempo real. Estas herramientas tecnológicas, combinadas con una estrategia de educación y concientización, ofrecen una defensa más robusta contra el phishing. formación es crucial para que el sistema de justicia no solo persiga los delitos, sino que logre condenas efectivas.

Respuesta eficaz del sistema de justicia penal Finalmente, Funez subraya la importancia de capacitar a los jueces y fiscales en ciberdelitos para que comprendan las complejidades técnicas y puedan procesar los casos de manera más eficiente.

### 4.2.4 Conclusión de la primera entrevista

El análisis de la entrevista con el ingeniero Carlos Augusto Funez deja en evidencia que Honduras enfrenta desafíos tanto tecnológicos como legales en la lucha contra el phishing. La combinación de medidas preventivas, inversión en tecnologías avanzadas y fortalecimiento del marco legal y judicial resulta imprescindible para mitigar el impacto de este tipo de ciberdelincuencia en el país.

4.3 Análisis de la Entrevista a CONATEL (Comisión Nacional de Telecomunicaciones de Honduras)

Se entrevistó a dos expertos de la Comisión Nacional de Telecomunicaciones de Honduras (CONATEL), un ingeniero informático y una abogada, ambos con amplia experiencia en temas de ciberseguridad y el sistema de justicia penal. A través de cinco preguntas clave, se buscó obtener información detallada sobre el fenómeno del phishing de datos en Honduras, así como evaluar las deficiencias y oportunidades de mejora en el marco legal y en la respuesta institucional frente a estos delitos cibernéticos.

4.3.1 Preguntas Realizadas

¿Qué estrategias de phishing de datos o robo de datos personales, ha identificado con mayor frecuencia en Honduras en los últimos 5 años?

¿Qué principales deficiencias considera el sistema de justicia penal en Honduras para combatir el phishing de datos?

¿Cuál cree que es la forma de prevención más efectiva, que el marco legal en honduras podría implementar para prevenir más ataques de phishing de datos en el país?

¿Qué estrategia o estrategias tecnológicas considera que se deben implementar en Honduras, para comenzar a darle fin a los ataques de phishing de datos en el país?

¿Como considera que el sistema de justicia penal en Honduras podría responder eficazmente al delito de phishing de datos?

4.3.2 Respuestas

1. Principales Estrategias de Phishing Identificadas en Honduras en los últimos 5 años.

La Abogada Belkis Amaya destacó los ataques de phishing vía WhatsApp y correos electrónicos masivos como las estrategias más frecuentes en los últimos cinco años. Esto resalta la vulnerabilidad de los hondureños a técnicas de ingeniería social a través de plataformas de comunicación cotidianas.

El Ingeniero José Luis Espinoza amplió el panorama mencionando el "SIM swap" o clonación de chips, un método que involucra la colaboración de empleados dentro de las compañías telefónicas. Esta práctica expone una grave vulnerabilidad interna en las telecomunicaciones, donde la seguridad no solo depende de la tecnología sino también de la integridad del personal. Además, enfatizó la falta de autenticación multifactor (MFA) y el riesgo emergente de tecnologías como "Deep Fake" y ataques a los sistemas biométricos, lo cual subraya la necesidad de educación y adopción de mejores prácticas de seguridad.

2. Deficiencias del Sistema de Justicia Penal en la Lucha contra el Phishing

Ambos expertos coinciden en la falta de convenios internacionales, especialmente el Convenio de Budapest, como una gran debilidad. La abogada Belkis Amaya mencionó la falta de formación técnica y tecnológica en jueces y operadores de justicia. Esta deficiencia no solo retrasa los procesos legales, sino que también impide una correcta interpretación de los delitos cibernéticos.

El ingeniero Espinoza reforzó esta idea señalando la falta de importancia que se le da a los ciberdelitos, sumado a los vacíos legales en la Ley de Información Pública. Además, destacó que la conceptualización del phishing no está bien comprendida, lo cual complica el debido proceso judicial, dejando a las víctimas desprotegidas.

3. Prevención Efectiva Desde el Marco Legal

La firma del Convenio de Budapest se posiciona como una solución clave para estandarizar los ciberdelitos y facilitar la cooperación internacional en investigaciones. Además, la abogada Amaya sugirió la importancia de estandarizar las definiciones legales de estos delitos, lo cual podría cerrar brechas legales y mejorar la coordinación en casos transnacionales.

4. Estrategias Tecnológicas Recomendadas

El ingeniero Espinoza propuso implementar un "Phishing Quiz" obligatorio antes de iniciar actividades laborales en el ámbito digital, lo cual podría elevar la conciencia cibernética de los usuarios. Esta iniciativa es innovadora y práctica, ya que permitiría educar de manera constante a la población sobre cómo identificar ataques de phishing.

Otras propuestas incluyeron:

• Verificación en Dos Pasos (2FA/MFA): Especialmente en aplicaciones de uso masivo como WhatsApp, Facebook e Instagram.

• Cursos Obligatorios de Ciberseguridad: Para estudiantes universitarios, aprovechando plataformas como KnowBe4, Coursera, Cybrary y SANS Institute. Esto no solo prepararía a los futuros profesionales, sino que también podría crear una cultura de seguridad

5. Mejora de la Respuesta del Sistema de Justicia Penal

La abogada Belkis Amaya señaló la necesidad de leyes específicas y equipos capacitados en la Fiscalía de Delitos Informáticos. Además, destacó la importancia de la imparcialidad del sistema penal, asegurando que todos los ciudadanos, independientemente de su estatus social, tengan acceso a un proceso judicial justo en casos de phishing de datos.

El enfoque en la formación continua de abogados y jueces en terminología y procesos de ciberseguridad podría reducir las tasas de fracaso en juicios relacionados con delitos informáticos. Además, la creación de unidades especializadas y la implementación de procedimientos claros y estandarizados permitirían responder de manera más efectiva a estos delitos.

### 4.3.3 Conclusión del Análisis a la Segunda Entrevista

La entrevista a CONATEL proporciona una perspectiva integral sobre el estado actual del phishing de datos en Honduras. Las principales amenazas incluyen no solo técnicas avanzadas como el "SIM swap" y el "Deep Fake," sino también problemas estructurales como la falta de legislación adecuada y educación en ciberseguridad. Las recomendaciones tanto legales como tecnológicas apuntan a fortalecer el marco legal, educar a la población y crear una infraestructura de seguridad más robusta y efectiva.

Este análisis complementa los hallazgos previos obtenidos a través de encuestas y establece una base sólida para formular recomendaciones concretas para reducir el impacto del phishing de datos en Honduras.

**4.4 Análisis de la Entrevista a FE-PROSI** (Fiscalía Especial de Propiedad Intelectual y Seguridad Informática) realizada al Abogado Héctor Morales

En el marco de la investigación sobre el phishing de datos en Honduras, se llevó a cabo una entrevista con el abogado Héctor Morales, representante de la Fiscalía Especial de Propiedad Intelectual y Seguridad Informática (FE-PROSI). Sus respuestas brindaron información valiosa sobre las modalidades de phishing más frecuentes, las deficiencias del sistema de justicia penal y las posibles soluciones para abordar este creciente problema en el país.

4.4.1 ¿Qué tipos de phishing de datos o robo de datos personales, ha identificado con mayor frecuencia en Honduras en los últimos 5 años?

Respuesta del Abogado Héctor Morales: Entre los delitos que más se dan, son el robo de datos vía la aplicación de WhatsApp, que consiste en que le bloquean su WhatsApp a través de otro número de teléfono, le mandan un mensaje a su WhatsApp donde le dicen que sus datos quieren actualizarlos a través de un click. Con ese click le hackean, le roban toda su información y queda bloqueada su cuenta de WhatsApp. Una vez robada la cuenta de WhatsApp, usted queda bloqueado de WhatsApp, la persona que le extrajo la información, se lleva todos los contactos de la víctima y empieza a mandarle mensajes a cada uno de ellos para continuar con el robo, haciéndose pasar como titulares de esos números robados.

La finalidad de esta acción es que el delincuente se quede con toda la información obtenida en accesos no autorizados a sistemas informáticos y usurpación de identidad, expreso.

Otro tipo de phishing o delito informático es cuando hay acceso no autorizado a los sistemas informáticos mediante el acceso a las Inter bancas, que varía a nivel de los bancos.

El artículo 405 del Código Penal, habla sobre las definiciones legales, donde nos dice que entendemos por datos informáticos, que entendemos por un sistema informático, y que entendemos por un programa informático.

¨Este tipo de phishing no necesariamente se da siempre por una persona en el exterior, también se da y se ha dado, desde el interior de los empleados de los bancos, expreso. ¨

Otro tipo de phishing que se da en Honduras es a A través de correros electrónicos masivos donde mandan a los usuarios a actualizar sus datos,

La venta de dólares ilegal a través del robo de WhatsApp.

Las Estafas Financieras a través de las redes sociales, market place, Facebook, Instagram,

Menciono el artículo 365 del Código Penal #1, donde se marcan todos los tipos de estafas, donde dice que quien, con el propósito de obtener un provecho ilícito, consigue transferencias no consentidas mediante manipulación informática, lo que se entiende por acceso no autorizado.

La Comisión Nacional de Bancas y Seguros ha emitido una regulación de evaluación a este tipo de phishing. Estas son regulaciones por parte de la CNBS como ente regulador hacia el sistema financiero Nacional, con el propósito de que tomen medidas preventivas en relación con este tipo de delitos.

4.4.2 Análisis de la pregunta 1

1. Tipología de Delitos de Phishing de Datos en Honduras El abogado Héctor Morales identificó varias modalidades comunes de phishing de datos en Honduras durante los últimos cinco años, destacando:

• Robo de datos a través de WhatsApp: Los ciberdelincuentes envían mensajes falsos solicitando actualizar información mediante un enlace, lo cual permite el acceso no autorizado a la cuenta y el robo de contactos para continuar la cadena de estafas.

• Accesos no autorizados a sistemas informáticos bancarios: Estos ataques varían según el banco e incluyen manipulación interna por empleados con acceso privilegiado a las bases de datos.

• Phishing a través de correos electrónicos masivos: Se solicitan datos personales o bancarios bajo pretextos falsos.

• Estafas financieras en redes sociales: Plataformas como Facebook, Instagram y Marketplace se utilizan para engañar a las víctimas con ofertas fraudulentas.

• Venta ilegal de dólares mediante robo de cuentas de WhatsApp: Una práctica emergente que combina técnicas de suplantación de identidad y manipulación financiera. Estas conductas delictivas se enmarcan en el artículo 365 del Código Penal hondureño, que tipifica las estafas mediante manipulación informática y accesos no autorizados, así como en el artículo 405, que establece definiciones legales y clave sobre sistemas y datos informáticos.

4.4.3 ¿Cuáles considera que son las principales deficiencias del sistema de justicia penal en Honduras, en la lucha contra el phishing de datos? Respuesta del Abogado Héctor Morales:

Como Ministerio Publico tenemos deficiencias en investigación, por el hecho de que no tenemos en este momento la práctica, ni el conocimiento para decir por donde vamos a investigar un delito de phishing o un delito de acceso no autorizado a sistemas informáticos.

Damos respuesta a la sociedad en la presentación de requerimientos fiscales, pero sin capacitación externa o interna, ha sido con las buenas prácticas aprendidas como investigar ciberdelitos, por ejemplo, que vamos a buscar elementos de prueba para presentar las acciones ante la autoridad judicial. Por qué el ente investigativo como tal, llamado DPI, no realiza su trabajo como tal, entonces, las acciones que hemos presentado, es por las investigaciones que hemos hecho aquí en interno como Fiscalía Especial de Propiedad Intelectual y Seguridad Informática y ministerio público.

Desde la entrada en vigor del código penal en junio del 2023, en materia de delitos informáticos, solo hemos presentado como 3 casos, no hemos presentado muchos, de los que no es fácil investigar, los hemos presentado por acceso no autorizados a sistemas informáticos, usurpación de identidades, por lavado de activos, porque, como el dinero lo mueven, de cuenta en cuenta, lo transforman, lo ocultan, lo convierten en el departamento técnico científico de la ATI, expreso.

4.4.4 Análisis de la Pregunta 2 Deficiencias del Sistema de Justicia Penal en la Lucha contra el Phishing de Datos El Abogado Morales subrayó importantes deficiencias en la respuesta del sistema de justicia penal de Honduras frente al phishing de datos. Entre las principales debilidades se encuentran: • Falta de capacitación especializada: Los fiscales y equipos investigativos carecen de formación específica en la investigación de delitos informáticos, lo cual afecta la calidad de los requerimientos fiscales presentados. • Deficiencia en la investigación policial: La Dirección Policial de Investigaciones (DPI) no ha proporcionado informes concluyentes sobre los casos investigados, lo que ha obligado a la FE-PROSI a realizar sus propias investigaciones internas.

• Bajas penas establecidas en el Código Penal: Delitos como el acceso no autorizado a sistemas informáticos tienen penas de 6 a 18 meses, lo que no resulta disuasorio para los ciberdelincuentes.

• Limitación en la persecución de delitos de estafa: Cuando el phishing se tipifica como estafa, la acción penal es privada, lo cual limita la intervención del Ministerio Público. 4.4.5 ¿Cuál

cree que es la forma de prevención más efectiva, que el marco legal en honduras podría implementar para prevenir más ataques de phishing de datos en el país? Respuesta del Abogado Héctor Morales: El marco legal no le da una forma de prevención, una forma de prevenir es que cada uno de los ciudadanos pongamos de nuestra parte a través de la concienciación y tener conocimiento de en qué consiste el phishing de datos, en que consiste un delito informático, que la población sepa que es un delito informático, en que consiste una suplantación de identidad, expreso.

Que exista la cultura de la denuncia del altercado a la entidad competente Que el Sistema Financiero Nacional, imponga mayor control de seguridad a lo interno de sus empleados, sobre los sistemas informáticos, ya que los empleados son quienes manejan las claves o los accesos a los sistemas informáticos, también expreso.

Que la Comisión Nacional de Bancas y Seguros como ente regulador, exija controles para mayor seguridad a nivel de sistemas informáticos para que el Sistema Financiero Nacional los implemente como protocolo de seguridad, a lo interno sus Bases de Datos para que los ciberdelincuentes no puedan tener acceso al mismo. Cada banco debe tener un protocolo de seguridad bastante rígido en la protección de datos.

4.4.6 Análisis sobre la pregunta

3. Propuestas de Mejora para Prevenir el Phishing de Datos El abogado propuso varias estrategias para reforzar la prevención del phishing de datos en Honduras, entre las que destacan:

• Concienciación ciudadana: Educar a la población sobre cómo identificar intentos de phishing y sobre la importancia de no compartir información personal a través de enlaces sospechosos.

• Cultura de la denuncia: Fomentar que las víctimas reporten estos delitos a las autoridades competentes.

• Mayor control interno en instituciones financieras: Regular y monitorear el acceso de los empleados a sistemas informáticos críticos para reducir riesgos internos. • Exigencias regulatorias para la seguridad informática: La Comisión Nacional de Bancas y Seguros (CNBS) debe imponer protocolos de seguridad más estrictos a los bancos, garantizando la integridad de las bases de datos y sistemas informáticos.

4.4.7 ¿Como considera que el sistema de justicia penal en Honduras podría responder eficazmente al delito de phishing de datos? Respuesta del Abogado Héctor Morales: Que exista la voluntad de todos los agentes involucrados en la investigación, llámese bien DPI, de hacer bien su trabajo, para que el ministerio público pueda responder a entablar las acciones correspondientes ante los entes correspondientes del poder judicial, dándole respuesta jurídica y eficiente a la sociedad. Porque si usted le pregunta a la DPI, ellos le van a decir o le dijeron que están bien capacitados, que hacen bien su trabajo y que han mandado no sé cuántos informes, si yo le dijese cuantos informes han mandado. Aquí las acciones que hemos presentado en materia de Delitos informáticos, es porque el ministerio publico las ha investigado, pero no es porque la DPI ha pasado un informe. En este momento la DPI no ha pasado ningún informe definitivo que diga, okay, con este informe podemos concluir que fulano de tal, cometió el delito de phishing de datos, lo podemos rastrear, está ubicado en tal lugar, ya podemos ejercer acciones jurídicas. La DPI no hace bien su trabajo, expreso. Hay problemas que salen del alcance de uno, porque dicen, el ministerio publico presento una acción y el Juez lo dejo libre, ¿pero ¿qué pasa? Si usted mira en las penas posibles a imponer de esos delitos, son penas bien bajas, según el Artículo 445 del Código Procesal Penal, estas no se consideran penas legales, manifestó. Otro punto, es que cuando el phishing de datos se presenta como estafa, este se convierte en un delito perseguible a instancia de parte, manifestó. Artículo 26, Numeral 8, Código Procesal Penal. Acciones no autorizadas a sistemas informáticos Art. 398 Código, Procesal Penal, las penas son apenas de 6 a 18 meses de cárcel, no hay castigos más severos. Articulo 26 CPP. Hay accesos no autorizados a sistemas informáticos y este sistema informático es de un particular, como también, hay accesos no autorizados a sistemas informáticos de la administración pública, y cuando sucede este tipo de accesos y violaciones, se le reconoce como Ciber terrorismo o Terrorismo Electrónico, Articulo 592 del Código Procesal Penal, manifestó.

4.4.8 Análisis de la Pregunta 4 Respuesta Eficaz del Sistema de Justicia Penal El Abogado sugiere, que, para responder de manera más efectiva a los delitos de phishing, es esencial mejorar la coordinación entre las entidades investigativas y judiciales, así como:

• Capacitación continua de investigadores y fiscales: Para fortalecer sus competencias en delitos informáticos.

• Mayor rigor en la DPI: Exigir informes completos y detallados que permitan al Ministerio

Público tomar acciones judiciales sólidas.

• Reforma legislativa: Aumentar las penas para delitos de phishing y acceso no autorizado a sistemas informáticos, transformándolos en delitos públicos perseguibles de oficio.

# CAPÍTULO V. Propuesta de Mejora

## 5.2 CONCLUSIONES

Las siguientes propuestas de mejoras para contratacar y proteger jurídica y tecnológicamente a la Población Hondureña, es el resultado de la validación de la hipótesis plantada y el trabajo de campo realizado a través de la aplicación de los diferentes instrumentos para esta investigación.

Esta investigación resulto bastante beneficiosa con los resultados obtenidos, para confirmar la viabilidad de este proyecto de investigación, debido a diferentes antecedentes históricos recopilados sobre el phishing de datos a nivel mundial, así como noticias y diferentes opiniones y acontecimientos ocurridos dentro del territorio Nacional.

Se obtuvieron estadísticas que evidenciaron la predominante realidad en la que el ciudadano Hondureño, siendo este persona natural y jurídica, se encuentra altamente vulnerable, desorientado en los pasos a seguir para protegerse de este delito, sin conocimiento técnico ni teórico acerca de la naturaleza de este ciberdelito, pero al mismo tiempo, expectante y familiarizados, con el nombre del delito debido a noticias, el Marco Jurídico Hondureño a través de diferente leyes de Honduras, las cuales sustentan a este proyecto en su respectivo capítulo de Bases legales, pero, los resultados confirmaron contundentemente, que la población hondureña se encuentra sin fe en el sistema de justicia Penal de Honduras como medio de protección definitiva contra el phishing de datos. Conclusiones

El sustento legal de esta investigación para brindar las propuestas de mejora que se mencionaran a continuación es el siguiente: El Código Penal de Honduras (Decreto No. 130-2017) en sus artículos 398, 399, 400, 401, 402 403 & 404.

La Ley de Firma Electrónica (Decreto No. 149-2013) en su artículo 8. La Ley de Comercio Electrónico (Decreto No. 149-2013) Art.9, numeral 6, 11, Art.48, Art.58. La Ley de Protección al Consumidor, (Decreto No. 24-2008) El Anteproyecto de Ley de Protección de Datos Personales

(Decreto No. 25-2022).

Aunque es cierto, estas leyes no regulan directamente el delito de Phishing de Datos en Honduras, pero si establecen principios generales y definiciones conceptuales, para proteger datos y regulan otros delitos específicos similares y forman parte de este delito en investigación.

La falta de un marco legal específico ha generado dificultades en la aplicación práctica de estos derechos. Otro factor importante que las diferentes investigaciones realizadas destacaron es la falta de un convenio y alianzas internacionales con Honduras para combatir ciberdelitos.

La Población Hondureña entrevistada y sometida a las respectivas encuestas, respondió positivamente a que Honduras adopte convenios internacionales, para establecer estándares sobre la persecución y penalización de ciberdelitos La Constitución de la República, en sus artículos 76, 100 & 82. 5.1 Primera Propuesta de Mejora, Fortalecimiento del Marco Legal 5.1.2 Acción 1: Adhesión del Convenio de Budapest Los resultados de esta investigación, mostraron que es urgente que Honduras firme y ratifique el Convenio de Budapest, lo que permitirá una cooperación internacional efectiva en la persecución de los ciberdelincuentes y facilitará el intercambio de información entre países.

¿Qué es el Convenio de Budapest? Es el primer tratado internacional que aborda los ciberdelitos, estableciendo normas sobre cómo los países deben tipificar delitos informáticos, mejorar sus procesos de investigación y facilitar la cooperación entre naciones. ¿Cómo Honduras puede adherirse a este Convenio? Presentación de la propuesta ante el Congreso Nacional: • Un diputado o el Poder Ejecutivo debe presentar una iniciativa de ley para que Honduras se adhiera al Convenio de Budapest.

• Es clave acompañar esta propuesta con datos del incremento del phishing en el país y la falta de herramientas internacionales para perseguir a los ciberdelincuentes que operan desde el extranjero. Ratificación internacional:

• Tras la aprobación legislativa, Honduras debe firmar el convenio y ser aceptada por el Consejo de Europa, que administra el tratado desde el 2001. • La Secretaría de Relaciones Exteriores y Cooperación Internacional debe gestionar el proceso diplomático. Adecuación del marco jurídico nacional:

• La legislación hondureña debe ajustarse a las disposiciones del Convenio, tipificando

nuevos delitos y actualizando procedimientos penales para agilizar la cooperación internacional. Como resultado esperado, Honduras tendría acceso a la red internacional de cooperación contra el ciberdelito, permitiendo rastrear ataques de phishing, incluso si los criminales operan desde otros países. 5.1.3 Acción 2: Reformas Específicas al Código Penal El objetivo de esta reforma, seria modernizar los artículos relacionados con delitos cibernéticos, especialmente el phishing. Posibles pasos para lograrla: Redacción de una propuesta de reforma:

• Incluir definiciones claras de phishing, spear phishing, Whaling y otras modalidades. • Establecer sanciones proporcionales al daño causado (por ejemplo, penas mayores si el phishing afecta a empresas de servicios públicos o bancos). Incluir agravantes especiales:

• Aumentar las penas cuando los ataques involucren robo de datos sensibles (como cuentas bancarias o registros médicos).

• Incorporar penas más severas para ciberdelincuentes reincidentes o quienes operen en redes organizadas. Resultado esperado: Mayor claridad en la persecución penal, sanciones más duras y cierre de vacíos legales que hoy permiten que el phishing no sea castigado con contundencia. 4.1.2 Acción 3: Ley de Protección de Datos Personales Objetivo de esta Ley: Garantizar que las empresas que manejan datos personales sean responsables de su seguridad y que los ciudadanos tengan control sobre su información. Pasos para implementarla: Incluir principios esenciales:

• Consentimiento explícito del usuario para usar sus datos. • Derecho a acceder, corregir y eliminar los datos personales en las plataformas.

• Multas fuertes a empresas que filtren o vendan datos sin permiso.

Proponer Crear un organismo de supervisión:

• Una "Agencia Nacional de Protección de Datos" encargada de vigilar y sancionar a las empresas que manejen mal la información de sus clientes.

• Coordinar esta agencia con la unidad especializada en cibercrimen para investigar filtraciones de datos.

Protección específica contra phishing:

• Obligar a las empresas, sin excepción de ningún empleado, que recojan datos personales

a implementar sistemas de autenticación robustos (como la verificación en dos pasos).

Resultado esperado: Los ciudadanos tendrán mayor control sobre sus datos, y las empresas serán responsables de proteger la información que almacenan.

**4.2 Creación de una Unidad Especializada en Delitos de Phishing**

• Fiscalía de Ciberdelitos: Se propone Crear una unidad dentro del Ministerio Público capacitada exclusivamente para investigar phishing y otros ciberdelitos, con personal entrenado en ciberseguridad y análisis forense digital. Esto necesitaría mayor compromiso y capacitación por parte de la Dirección Policial de Investigaciones (DPI) para realizar su trabajo de manera más efectiva. El abogado Morales perteneciente a FE-PROSI, manifestó que todas las acciones presentadas por ellos en materia de Delitos informáticos, es porque el ministerio publico hizo sus propias investigaciones, pero no debido a que la DPI haya pasado informes o información definitiva. Si la DPI se compromete a realizar su trabajo de manera más comprometida, el ministerio público también podría ser más efectivo en la realización de estas investigaciones.

• Invertir en el adecuado Equipamiento tecnológico: Dotar a esta unidad de software especializado para rastrear correos maliciosos, analizar redes sociales e identificar cuentas bancarias falsas vinculadas a fraudes electrónicos. Esto facilitaría las investigaciones de forma digital y reforzaría las habilidades tecnológicas de los empleados dentro del Ministerio Publico y en la Dirección Policial de Investigaciones

• Protocolos claros de denuncia: Simplificación del proceso de denuncia para que las víctimas, o sea, los ciudadanos sin conocimientos de las leyes y los debidos procesos puedan reportar phishing de manera más accesible, incluso mediante aplicaciones móviles.

4.3 Educación Digital Masiva y Obligatoria

5.3.1 Acción 1. "Phishing Quiz" obligatorio (Este se encuentra en Google)

Implementar un programa anual de concienciación digital en empresas privadas y entidades públicas, donde los empleados realicen una evaluación obligatoria que los entrene para reconocer intentos de phishing.

Objetivo: Se podría realizar a través de simulacros de correos electrónicos y mensajes falsos dirigidos a los empleados de empresas públicas y privadas, para medir el conocimiento y la habilidad de los empleados en detectar una página falsa con intención de phishing.

• Ante estos Phishing Quiz de Google, los empleados que fallen el simulacro, que sean sometidos a recibir una formación obligatoria sobre cómo identificar ataques reales.

• Las Empresas financieras, de telecomunicaciones y gubernamentales deben estar en la primera línea de esta estrategia.

Capacitación continua en el sector público:

• Los funcionarios que manejan datos personales o sensibles (como registros civiles, bancos públicos o servicios sanitarios) reciban capacitaciones periódicas para reconocer intentos de phishing.

• Que se implementen pruebas periódicas para medir el nivel de preparación de cada institución.

Resultado esperado:

• Que se reduzca el riesgo de que los empleados, por error, comprometan información sensible.

• Que las instituciones públicas y privadas estén más preparadas para actuar frente a

ataques de ingeniería social.

5.3.2 Acción 2. Capacitación desde la educación básica:

Introducir módulos de seguridad digital en las escuelas secundarias y universidades, adaptando programas como los de Coursera, Cybrary o el SANS Institute para crear una cultura de prevención desde temprana edad.

¿Como se puede realizar?

Creación de módulos educativos adaptados a cada nivel escolar:

• Primaria: Conceptos básicos de seguridad digital (no compartir contraseñas, no hacer clic en enlaces sospechosos).

• Secundaria: Reconocimiento de estafas digitales y buenas prácticas para proteger cuentas en redes sociales y correos electrónicos.

• Universidades: Formación más avanzada sobre phishing, ingeniería social y cómo proteger la identidad digital, especialmente para estudiantes de carreras administrativas,

financieras y tecnológicas.

Capacitación docente:

• Es clave que los maestros comprendan el phishing y la seguridad digital para poder transmitirlo adecuadamente a sus estudiantes.

• Se pueden hacer alianzas con empresas especializadas en ciberseguridad para ofrecer talleres gratuitos a los docentes.

Resultado esperado:

• Los estudiantes aprenderán desde pequeños a identificar posibles ataques de phishing, reduciendo las víctimas futuras.

• Se forma una nueva generación más preparada tecnológicamente, creando una barrera social contra el phishing.

5.3.3 Acción 3. Campañas Nacionales masivas de concienciación: Colaboración entre el gobierno, bancos y proveedores de servicios digitales para lanzar campañas masivas en redes sociales, televisión y medios tradicionales, alertando a la población sobre las técnicas más comunes de phishing.

Propuesta:

Alianzas con empresas tecnológicas y medios de comunicación:

• Desarrollar campañas visuales, radiales y en redes sociales con mensajes directos y fáciles de entender sobre cómo identificar intentos de phishing.

Ejemplos: "Si te piden tus datos personales por mensaje, es una estafa", "Ningún banco te pedirá tu contraseña por correo", etc.

• Utilizar influencers locales y figuras públicas para que el mensaje llegue más rápido a la población joven y adulta.

Aplicaciones móviles educativas:

• Crear una aplicación nacional gratuita que enseñe a detectar intentos de phishing con simulaciones prácticas y recompensas digitales al completar los niveles.

Resultado esperado:

• La población general estará más informada y alerta ante posibles estafas.

• La campaña masiva reducirá el número de personas que caen en ataques básicos de phishing.

5.4 Implementación de Tecnología de Defensa en Tiempo Real

• .4.1 Acción 1. Verificación de identidad obligatoria: Implementar la autenticación multifactor (MFA) en servicios críticos como bancos, plataformas de compras en línea y servicios gubernamentales digitales.

• 5.4.2 Acción 2. Sistema Nacional de Alerta de Phishing: Crear una plataforma centralizada que alerte a los ciudadanos cuando se detecten campañas masivas de phishing dirigidas a Honduras, similar a las alertas de emergencia.

Crear una plataforma centralizada conectada con ISPs y bancos:

• Esta plataforma debe poder detectar campañas de phishing en correos, SMS y redes sociales mediante inteligencia artificial.

• Cuando detecte un intento masivo de phishing dirigido a Honduras, enviará alertas en tiempo real a ciudadanos y empresas.

Sistema de reporte ciudadano:

• Los usuarios podrían reportar mensajes sospechosos directamente desde WhatsApp, Telegram o una app dedicada, alimentando la base de datos nacional.

• Cada reporte debe analizarse específicamente, para clasificar la amenaza y ampliar la alerta si es necesario.

Resultado esperado:

• La población y las empresas reaccionarán más rápido ante campañas de phishing activas.

• Los ciberdelincuentes perderían efectividad, porque sus métodos serán detectados y bloqueados en horas o minutos.

• 5.4.3 Acción 3: Monitoreo con inteligencia artificial:

Desarrollar o adquirir sistemas basados en IA para detectar patrones de phishing en tiempo real y rastrear servidores utilizados por los ciberdelincuentes.

• El gobierno puede hacer una licitación para adquirir tecnología avanzada o trabajar con universidades nacionales para desarrollar un software propio.

• La IA debe ser utilizada para analizar grandes volúmenes de tráfico web, detectar patrones y bloquear enlaces maliciosos automáticamente.

Resultado Esperado:

Honduras contaría con una tecnología propia para identificar y detener ataques de phishing antes de que lleguen a la población.

5.5 Reformas en la Cooperación Internacional

5.5.1 Acción 1: Acuerdos bilaterales y regionales

Firmar tratados con países avanzados en ciberseguridad:

• Estados Unidos, Estonia, España e Israel son líderes en ciberseguridad. Honduras podría buscar acuerdos de cooperación tecnológica y asesoramiento legal para mejorar la persecución de ciberdelitos.

• Estos acuerdos deben incluir intercambio de tecnología, acceso a bases de datos de ciberdelincuentes y capacitaciones continuas a fiscales y policías.

Crear una red centroamericana de ciberseguridad:

• Honduras puede liderar la creación de una red de cooperación regional contra el phishing junto a Guatemala, El Salvador, Nicaragua y Costa Rica.

• La red permitirá compartir información en tiempo real sobre campañas de phishing

detectadas en cualquiera de los países miembros.

Resultado esperado:

• Los ciberdelincuentes no podrán trasladar sus operaciones entre países vecinos sin ser detectados.

• Honduras fortalecerá su presencia internacional en la lucha contra el cibercrimen.

5.5.2 Acción 2: Integración a redes globales de ciberdefensa Ingreso a la Anti-Phishing Working Group (APWG):

• Esta organización global coordina esfuerzos entre gobiernos y empresas privadas para rastrear redes de phishing.

• Honduras debe gestionar su integración para acceder a las bases de datos globales y recibir alertas tempranas de campañas internacionales que puedan llegar al país.

Alianza con Interpol Cybercrime Division:

• Interpol cuenta con una división especializada en cibercrimen. Honduras puede firmar un convenio para trabajar de la mano con esta entidad y solicitar asistencia en investigaciones internacionales de phishing.

Resultado esperado:

• Honduras pasará de ser un país vulnerable a un aliado regional e internacional en la lucha contra el phishing.

# CAPÍTULO VI. Discusión, Conclusiones y Recomendaciones

". La creciente expansión del uso de las tecnologías digitales ha traído consigo grandes avances para la sociedad hondureña, pero también ha abierto la puerta a amenazas cibernéticas más sofisticadas, entre las que destaca el phishing de datos. Este delito, caracterizado por la manipulación psicológica de las víctimas para obtener información confidencial, ha evolucionado rápidamente, dejando en evidencia las vulnerabilidades del sistema de protección digital en Honduras.

A través de esta investigación, se analizaron las diversas modalidades de phishing que afectan tanto a individuos como a empresas, revelando la falta de preparación tecnológica, educativa y jurídica que enfrenta el país. Los resultados obtenidos a partir del trabajo de campo, encuestas y análisis documental confirmaron la urgencia de implementar cambios estructurales en las leyes, la tecnología y la cultura digital nacional.

La validación de la hipótesis planteada destacó que, si bien existen leyes generales relacionadas con la protección de datos personales y el comercio electrónico, estas resultan insuficientes y desactualizadas para enfrentar específicamente el phishing. Además, se evidenció

que la falta de cooperación internacional y de una unidad especializada en ciberdelitos deja a Honduras aislada y vulnerable frente a los cibercriminales, quienes operan desde cualquier parte del mundo con total impunidad.

En este contexto, las siguientes conclusiones recogen los hallazgos clave de la investigación y proponen acciones estratégicas dirigidas a fortalecer el marco legal, mejorar las capacidades tecnológicas, promover la educación digital y establecer alianzas internacionales. Estas medidas buscan no solo reducir la incidencia del phishing, sino también proteger jurídicamente a la población hondureña y devolverle la confianza en el sistema de justicia penal del país.

### 6.1.1 Conclusión A: Identificación y análisis de los tipos de phishing más frecuentes en Honduras

La investigación reveló que el phishing de datos es uno de los cibercrímenes más recurrentes en Honduras, afectando tanto a personas naturales como jurídicas y de diferentes tipos, como lo son:

- Envió de correos masivos para robo de credenciales.
- Envió de correos dirigidos para robo de credenciales.
- Patrocinio de páginas web suplantando a los bancos en los buscadores como Google.
- Llamadas telefónicas o WhatsApp.
- Venta de productos en Marketplace.

La población, aunque familiarizada con el término por medios de comunicación, carece de conocimientos prácticos sobre cómo protegerse. Los resultados del trabajo de campo confirmaron que la falta de educación digital, junto con la ausencia de medidas tecnológicas preventivas y un marco legal desactualizado, contribuyen directamente a la proliferación de estos delitos. La propuesta de implementar autenticación multifactorial (MFA) y el Sistema Nacional de Alerta de Phishing busca reducir esta vulnerabilidad. Además, el monitoreo con inteligencia artificial permitirá identificar y frenar campañas de phishing antes de que lleguen a los ciudadanos, lo que representa un cambio estructural en la protección digital del país.

### 6.1.2 Conclusión B: Estrategias y métodos utilizados por los cibercriminales para ejecutar

ataques de phishing

El estudio evidenció que Honduras es un blanco fácil para los ciberdelincuentes, quienes emplean técnicas sofisticadas como spear phishing, Whaling y suplantación de identidad corporativa. Se confirmó que los usuarios caen fácilmente en estos fraudes debido a la falta de formación sobre cómo reconocerlos. Para contrarrestar esto, la propuesta de "Phishing Quiz" obligatorio y campañas nacionales masivas de concienciación permitirá entrenar a los empleados y ciudadanos en la detección temprana de estos ataques. La inclusión de módulos de seguridad digital en las escuelas garantiza que las futuras generaciones tengan desde temprana edad las herramientas necesarias para proteger su identidad digital, cortando así el ciclo de vulnerabilidad social a largo plazo.

### 6.1.3 Conclusión C: Análisis de las deficiencias del marco legal hondureño frente al phishing

La evaluación del marco legal hondureño demostró que, aunque existen leyes relacionadas con la protección de datos personales (Constitución, Código Penal, Ley de Comercio Electrónico y la Ley de Protección al Consumidor), estas no tipifican directamente el phishing. Esta falta de precisión genera obstáculos para la persecución efectiva del delito, dejando a los ciudadanos en una situación de desprotección. Por ello, la reforma al Código Penal es una propuesta clave, con la incorporación de definiciones claras de phishing, spear phishing y Whaling, así como sanciones proporcionales al daño causado y agravantes especiales para ciberdelincuentes reincidentes. Además, la creación de la Ley de Protección de Datos Personales permitirá responsabilizar a las empresas que manejen información sensible, cerrando los vacíos legales que actualmente permiten que los datos sean explotados sin consecuencias jurídicas contundentes.

### 6.1.4 Conclusión D: Propuestas estratégicas para reducir el phishing en Honduras

Honduras enfrenta una alarmante falta de herramientas legales y tecnológicas para combatir el phishing. La adhesión al Convenio de Budapest surge como una estrategia crucial para integrar al país a una red internacional de cooperación, facilitando la persecución de ciberdelincuentes, incluso si operan desde el extranjero. La creación de una Unidad Especializada en Delitos de Phishing, con personal capacitado en ciberseguridad y análisis forense digital, junto con el fortalecimiento de la Dirección Policial de Investigaciones (DPI) y la mejora del Ministerio Público, permitirá una persecución más rápida y efectiva de los delitos informáticos. A nivel

internacional, la integración de Honduras a redes globales como Interpol Cybercrime Division y la Anti-Phishing Working Group (APWG) permitirá acceder a bases de datos de ciberdelincuentes globales, recibir alertas tempranas y colaborar en la investigación de redes criminales transnacionales.

La investigación demuestra que Honduras necesita una transformación estructural en su lucha contra el phishing, combinando reformas legales, tecnología avanzada y educación digital masiva. Las propuestas de mejora planteadas no solo cierran los vacíos normativos actuales, sino que también posicionan a Honduras como un país más seguro digitalmente, capaz de proteger a sus ciudadanos y cooperar a nivel internacional en la persecución del cibercrimen. La validación de la hipótesis confirmó que la población hondureña no confía en el sistema de justicia penal actual como defensa ante estos delitos, por lo que estas reformas son vitales para restaurar esa confianza y garantizar la seguridad digital del país.

### 6.2 Recomendaciones

A partir de los resultados obtenidos y las conclusiones formuladas, se plantean las siguientes recomendaciones estratégicas para fortalecer la capacidad de Honduras en la prevención, persecución y mitigación de los delitos de phishing de datos:

6.2.1 1. Reforma legislativa integral para enfrentar el phishing

• Tipificación directa del phishing y sus variantes (spear phishing, Whaling, etc.) dentro del Código Penal, con sanciones proporcionales al daño causado y agravantes según la magnitud del perjuicio.

• Aprobación acelerada de la Ley de Protección de Datos Personales (Decreto No.

25-2022), incorporando mecanismos claros para responsabilizar a las empresas que manejen información confidencial y regulando el uso de la autenticación multifactor (MFA) para proteger datos sensibles.

• Ratificación urgente del Convenio de Budapest, que permitirá a Honduras integrarse a la red internacional de persecución de ciberdelitos y mejorar la cooperación internacional.

6.2.2 2. Creación de una Fiscalía Especializada en Phishing y Delitos Informáticos

• Formación de una unidad exclusiva dentro del Ministerio Público para atender delitos de

phishing y otros cibercrímenes, dotada de especialistas en análisis forense digital y ciberseguridad.

• Capacitación técnica intensiva a la Dirección Policial de Investigaciones (DPI) para mejorar la coordinación con el Ministerio Público, agilizando la recopilación de pruebas digitales y reduciendo el tiempo de respuesta ante las denuncias.

• Implementación de herramientas tecnológicas avanzadas para rastrear direcciones IP, servidores y redes asociadas a campañas de phishing.

6.2.3 3. Fortalecimiento de la educación digital en la población hondureña

• Incorporación de módulos educativos obligatorios sobre seguridad digital y cibercrimen en la educación básica, media y superior, fomentando la cultura de la prevención desde temprana edad.

• Capacitación continua en empresas públicas y privadas a través de simulacros de phishing ("Phishing Quiz"), con formación obligatoria para empleados que no superen las pruebas.

• Campañas nacionales masivas de concienciación usando medios tradicionales y digitales para educar a la población sobre las modalidades de phishing más comunes y cómo evitarlas.

6.2.4 4. Implementación de tecnología de defensa cibernética en tiempo real

• Creación de un Sistema Nacional de Alerta de Phishing, conectado con bancos, ISP y servicios digitales esenciales, que emita alertas en tiempo real cuando se detecten campañas masivas de phishing dirigidas a Honduras.

• Monitoreo de tráfico digital con inteligencia artificial para detectar patrones de phishing, bloquear enlaces maliciosos automáticamente y rastrear servidores asociados a los ataques.

• Desarrollo de una aplicación móvil gratuita que permita a los ciudadanos reportar mensajes sospechosos, ayudando a alimentar una base de datos nacional de amenazas.

6.2.5 5. Establecimiento de alianzas internacionales y cooperación regional

• Firmar tratados bilaterales y multilaterales con países líderes en ciberseguridad (Estados Unidos, España, Israel, Estonia), facilitando el acceso a tecnología avanzada, capacitación y bases de datos internacionales de ciberdelincuentes.

• Integración de Honduras a la Anti-Phishing Working Group (APWG) y a la Interpol

Cybercrime Division, fortaleciendo la capacidad del país para identificar y desmantelar redes de phishing transnacionales.

• Creación de una red centroamericana de ciberseguridad que permita compartir información en tiempo real entre Honduras, Guatemala, El Salvador, Nicaragua y Costa Rica, mejorando la capacidad regional para rastrear ciberdelincuentes que operan entre fronteras.

Resultado esperado global:

Estas recomendaciones buscan transformar la realidad digital de Honduras, posicionando al país como líder regional en la lucha contra el phishing. La combinación de una legislación sólida, una estructura institucional especializada, educación digital masiva, tecnología de defensa avanzada y cooperación internacional garantizará una disminución significativa en la incidencia de este delito y, lo más importante, devolverá la confianza a la población en el sistema de justicia penal hondureño.

# REFERENCIAS BIBLIOGRÁFICAS

(S/f). Unirioja.es. ¿Recuperado el 15 de febrero de 2025, de https://dialnet.unirioja.es/servlet/articulo?Código=7998377Andrés, G. (2019). El consentimiento y el reglamento de protección de datos—LegalToday.

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

Cook, S. (2023, enero 16). Estadísticas y datos sobre el phishing para 2019–2022. Comparitech. https://www.comparitech.com/es/blog/vpn-privacidad/phishing-estadisticas-datos/

Benavides, E., Fuertes, W., Sánchez, S., & Núñez-Agurto, D. (2020). Caracterización de los ataques de phishing y técnicas para mitigarlos. Ataques: una revisión sistemática de la literatura. Ciencia y Tecnología, 13(1), 97-104.

Diaz Pari, A. C. C., & Goita Cardenas, S. E. (2024). El delito de phishing en las entidades financieras del Perú. https://repositorio.autonoma.edu.pe/handle/20.500.13067/3416

Montes, S. (2022, mayo 17). El panorama del cibercrimen a nivel mundial en cinco estadísticas. Escudo Digital. https://www.escudodigital.com/ciberseguridad/panorama-cibercrimen-nivel-mundial-en-cinco-estadisticas_51740_102.html

Pérez, C., & Stiven, M. (2022). Panorama de Ciberataques más Recurrentes en Colombia 2021 y 2022. https://repository.unipiloto.edu.co/handle/20.500.12277/12279

Los ciberataques alcanzan cifras históricas por la guerra de Ucrania. (2022, marzo 21). Escudo Digital. https://www.escudodigital.com/ciberseguridad/ciberataques-alcanzan-cifras-historicas-por-guerra-ucrania_51239_102.html

Rodríguez, F. (2024, noviembre 23). ¡Cuidado hondureño! Nuevas estafas y hackeos cibernéticas que debes conocer: Los ciberdelincuentes están innovando. Televicentro. https://www.televicentro.com/cuidado-nuevas-estafas-y-hackeos-ciberneticas-que-debes-

contenidos. (2024, marzo 11). Conoce algunas estrategias contra el phishing en el mundo financiero digital. Banco Atlántida. https://transformaciondigital.bancatlan.hn/conoce-algunas-estrategias-contra-el-phishing-en-el-mundo-financiero-digital/

Hn, L. (2023, mayo 5). Honduras enfrenta desafíos en la lucha contra el “phishing”. La Prensa. https://www.laprensa.hn/premium/honduras-enfrenta-desafios-lucha-contra-phishing-LD13322180

https://www.bancoazteca.com.hn/beaHonduras/contenido/atencion/seguridad/phishing.jsp

Zapata, D. (2024, agosto 10). Instituciones del Estado, las más vulnerables a los ciberataques. El Heraldo. https://www.elheraldo.hn/honduras/instituciones-estado-vulnerables-

Zelaya, O. (2021, abril 23). HONDURAS - La protección de datos en Honduras. Central Law; Your International Central American Firm. https://central-law.com/honduras-la-proteccion-de-datos-en-honduras/

(S/f). Unirioja.es. Recuperado el 19 de febrero de 2025, de https://dialnet.unirioja.es/servlet/articulo?codigo=8758428

Gallego, D., & Norela, D. (2025). Estrategia para la prevención de ataques de ingeniería social en las empresas del sector financiero en la ciudad de Bogotá. https://repository.unad.edu.co/handle/10596/65793

Hn, L. (2023, abril 20). Diseñan ley para proteger datos ante ciberdelincuentes. La Prensa. https://www.laprensa.hn/honduras/disenan-ley-proteger-datos-ante-ciberdelincuentes-honduras-AA13131010?utm_source=chatgpt.com

¿Qué es el spear phishing? Definición y riesgos. (2017, noviembre 9). /. https://latam.kaspersky.com/resource-center/definitions/spear-phishing?srsltid=AfmBOooHUuPAqdl8cSl7Hu65O5UBoy1kJmi4l4edZducxvwEogd1ogpK

¿Qué es la ingeniería social? (2017, diciembre 6). /. https://latam.kaspersky.com/resource-center/definitions/what-is-social-engineering?srsltid=AfmBOoqG6bYhCCs5LPjfiZCsY7TiUKCfSmhCv_NkVhoypD3iYJTPx

Muñoz, R., & Antonio, J. (2017). Ransomware: análisis y contramedidas. https://repositorio.uam.es/handle/10486/679544

Blázquez, R., & Luis, J. (2014). Cibercrimen y ciberterrorismo: ¿exageración mediática o realidad? https://oa.upm.es/32868/

López, D. del V. (2018). Evidencia digital.

Estévez Herrera, J. (2025). Estrategias Disruptivas de Ciberseguridad: Abordando las Amenazas Informáticas Emergentes en el Ámbito Empresarial, Educativo y Gubernamental. https://repository.unad.edu.co/handle/10596/66386

Pérez Rojas, D. R. O. (2023). Inteligencia artificial aplicada a la ley de protección de datos. Editorial E-books.

Cristian, M. C., & Erick, R. C. (2021). Aspectos teórico-prácticos de la firma digital en Colombia y su referente en Latinoamérica. Editorial Universidad del Rosario.

Ciberseguridad: Protección de Datos e IA en América Latina. (2024, Junio 14). Sherlock Communications. https://www.sherlockcomms.com/es/ciberseguridad-proteccion-de-datos-e-ia-en-america-latina/

(S/f). Unirioja.es. Recuperado el 25 de febrero de 2025, de https://dialnet.unirioja.es/servlet/revista?codigo=4370

Kiss, T. (s/f). Investigación exploratoria: qué es, características, ejemplo. https://concepto.de/investigacion-exploratoria/

Medina Romero, M. Á., Hurtado Tiza, D. R., Muñoz Murillo, J. P., Ochoa Cervantes, D. O., & Izundegui Ordóñez, G. (2023). Método mixto de investigación: Cuantitativo y cualitativo. Instituto Universitario de Innovación Ciencia y Tecnología Inudi Perú.

https://dialnet.unirioja.es/servlet/articulo?codigo=7746475

https://gc.scalahed.com/recursos/files/r161r/w26022w/Arias_S2.pdf

Hernández, R., Fernández, C., & Baptista, M. del P. (2014). Metodología de la Investigación (6th ed.). Mc Graw Hill Education. https://www.uca.ac.cr/wpcontent/uploads/2017/10/Investigacion.pdf

Olvera, J. (2015). Metodología de la Investigación Jurídica para la Investigación y la elaboración de tesis de licenciatura y posgrado (1st ed.). Universidad Autónoma del Estado de México.

# ANEXOS

## Encuesta sobre el Phishing de Datos en Honduras

Esta encuesta tiene como propósito conocer el nivel de percepción, conocimiento y experiencias de los ciudadanos hondureños sobre el phishing de datos, así como evaluar su opinión respecto a la efectividad del marco jurídico actual y posibles estrategias de prevención.

Pregunta *

1. ¿Sabe usted que es el phishing de datos?

- Si
- No
- No se

2. ¿Alguna vez, usted o alguien que conoce, ha sido víctima de phishing de datos en Honduras?

- Si
- No
- No se

4. ¿Considera que el phishing de datos ha aumentado en Honduras en los últimos 5 años?

- a. Totalmente de acuerdo
- b. De acuerdo
- c. Me es indiferente
- d. En desacuerdo
- e. Totalmente en desacuerdo.

6.Cree o conoce que las leyes actuales en Honduras son efectivas para combatir el phishing de Datos en el Pais?

- a. Totalmente de acuerdo
- b. De acuerdo
- c. Me es indiferente
- d. En desacuerdo
- e. Totalemente en desacuerdo

7. Confía en que las autoridades hondureñas puedan manejar adecuadamente los casos de phishing de datos?

- a. Totalmente de acuerdo
- b. De acuerdo
- c. Me es indiferente
- d. En desacuerdo
- e. Totalmente en desacuerdo

8. Bajo un contexto jurídico, cree que la cooperación internacional con convenios internacionales, como una estrategia legislativa, ¿ayudaría a reducir los ataques de phishing de datos en Honduras?

- a. Totalmente de acuerdo
- b. De acuerdo
- c. Me es indiferente
- d. En desacuerdo
- e. Totalmente en desacuerdo

9. Estaría dispuesto a recibir capacitación sobre cómo protegerse y evitar ataques de phishing de datos en Honduras?

- a. Totalmente de acuerdo
- b. De acuerdo
- c. Me es indiferente
- d. En desacuerdo
- e. Totalmente en desacuerdo.

## Entrevista en la Comisión Nacional de Bancas y Seguros (CNBS)

¿Qué tipos de phishing o robo de datos personales, ha identificado con mayor frecuencia en Honduras en los últimos 5 años?

**Respuesta del Ingeniero Carlos Augusto Funez**

- Envió de correos masivos para robo de credenciales.
- Envió de correos dirigidos para robo de credenciales.
- Patrocinio de páginas web suplantando a los bancos en los buscadores como Google

¿Cuáles considera que son las principales deficiencias del sistema de justicia penal en Honduras, en la lucha contra el phishing de datos?

**Respuesta del Ingeniero Carlos Augusto Funez**

- Como en la mayoría de los casos se trata de un crimen transnacional y Honduras no esta suscrito al Convenio de Budapest, ni ha homologado los tipos de delito informático. Se dificulta el proceso de investigación de los casos.
- Falta de recursos (Humanos, tecnológicos y capacitaciones) en el Ministerio Público para el proceso de investigación de este tipo de casos.
- Falta de una ley y estrategia nacional de Ciberseguridad.
- Falta de una ley de Protección de Datos

¿Cuál cree que es la forma de prevención más efectiva, que el marco legal en honduras podría implementar para prevenir más ataques de phishing de datos en el país?

**Respuesta del Ingeniero Carlos Augusto Funez**

- Campañas de concientización y culturización en el uso de tecnologías y seguridad de estas.
- Hacer Reformas para incluirlo en el pensum académico nacional de educación.
- Que las empresas tanto publicas como privadas implementen mejores practicas de seguridad de información en los servicios que ofrecen a la población en general.

**Respuesta del Ingeniero Carlos Augusto Funez**

- El phishing nunca va a terminar por el avance de las tecnologías y nuevas metodologías que encuentran los ciberdelincuentes.
- No obstante se puede mitigar con la implementación de buenas prácticas y tecnologías que disminuyen el riesgo por ejemplo, uso de 2FA, passwordless, 2FA resistente al phishing, Biometría y sistemas de monitoreo basados en el comportamiento del usuario para detectar patrones inusuales etc..

¿Cómo considera que el sistema de justicia penal en Honduras podría responder eficazmente al delito de phishing de datos?

**Respuesta del Ingeniero Carlos Augusto Funez**

- Capacitación de los jueces y fiscales en esta temática.

## Entrevista a CONATEL (Comisión Nacional de Telecomunicaciones de Honduras)

Abogada Belkis Amaya

Ingeniero José Luis Espinoza

1.) ¿Qué estrategias de phishing de datos o robo de datos personales, ha identificado con mayor frecuencia en Honduras en los últimos 5 años?

Abogada Belkis: Ataques de Phishing vía whatsapp y correos electrónicos masivos.

Ingeniero José Luis Espinoza: Robos de Whatsapp, Swim swap o clonación de chips, el ingeniero manifestó que esto es causado por personas adentro de las compañías telefonicas que están confabuladas y brindan información a cambio de intereses personales a los ciberdelincuentes. Faltas de Multiples Factor de Autenticación en dispositivos de los usuarios, Deep Fake, rayar los biométricos.

2.) ¿Cuáles considera que son las principales deficiencias del sistema de justicia penal en Honduras, en la lucha contra el phishing de datos?

Abogada Belkis: Falta de una firma de un convenio convenio como el de Budapest, tambien la falta de formación tecnológica, técnica en ciberseguridad en los operadores de justicia como jueces en materia de cibercrimen.

Ingeniero José Luis: Falta de convenios mas completo como los que esta promoviendo la ONU, Honduras no le da la importancia requerida a los ciberdelitos, lo que dificulta promover las herramientas correctas para la protección de datos. Ley de información pública, muchos vacíos legales. Los Jueces y Fiscales no están educados sobre el debido proceso del phishing de datos, la conceptualización de esta terminología, esto incluye todo el proceso cuando este delito se ejecuta en la victima.

3.) ¿Cuál cree que es la forma de prevención más efectiva, que el marco legal en honduras podría implementar para prevenir más ataques de phishing de datos en el pais?

Abogada Belkis: La Firma del convenio de Budapest en Honduras, estandarizar a todos los ciberdelitos con la misma consonancia del significado de estos, entre todos los delitos regulados por el marco legal hondureño y el sistema de justicia penal. Estandarizar los criterios que tipifican a cada uno de los delitos a nivel internacional, para facilitar los procesos de cooperación en caso de investigación. Por que puede ocurrir que el pais del cual se requiere información por la comisión de un delito en dicho pais, no lo sea y no esté obligado a brindarla.

4.) ¿Qué estrategia o estrategias tecnológicas considera que se deben implementar en Honduras, para comenzar a darle fin a los ataques de phishing de datos en el pais?

Ingeniero José Luis: Que las máximas autoridades de todas las empresas privadas y las entidades gubernamentales, promuevan, exijan y obliguen por propósitos exclusivamente de seguridad y concienciación, a todos los empleados a realizar antes de iniciar cualquier actividad laboral que requiera el uso de cualquier aparato digital, un pequeño Phishing Quiz de Google, donde el usuario ingresa a phishing quiz Google.com y vera 2 escenarios diferente, muy difíciles de identificar a simple vista, las diferencias definitivas entre uno del otro. Esto permitirá al hondureño estar alerta, constantemente consciente sobre la amenaza presente de ser victimas de cualquier ataque de phishing de datos.

Ingeniero José Luis: La importancia de la utilización de 2 step verification o verificación de 2 pasos en whatsapp, Instagram, facebook y cualquier red social por parte del usuario.

Implementar en las universidades públicas y privadas del pais, en que los estudiantes obligatoriamente saquen cursos digitales de ciberseguridad, como:
KnowBe4: Especializada en entrenamiento contra phishing y concienciación en ciberseguridad.
Cybrary: Ofrece cursos gratuitos y de pago sobre una amplia gama de temas de ciberseguridad.
Coursera, edX y Udemy: Que tienen programas desde nivel básico hasta avanzado, muchos de ellos con certificación.
SANS Institute: Provee cursos altamente especializados en ciberseguridad.

5.) ¿Como considera que el sistema de justicia penal en Honduras, podría responder eficazmente al delito de phishing de datos?

Abogada Belkis: Para responder eficazmente, el sistema de justicia penal en Honduras necesita leyes, no hay equipos en fiscalía de delitos informáticos. Formación de principios para llevar a cabo juicios justos ante cualquier ciberdelito, ya que hay muchos abogados que pierden casos por no entender terminologías, naturalezas de estos fenómenos digitales donde sus clientes son las víctimas, No es cercitivo.

Abogada Belkis: El sistema penal de Honduras debe de igualar las clases sociales ante estos delitos y tratarlos con la relevancia jurídica que todos tienen, no deben priorizar este tipo de delitos solamente en ciertas victimas de alto estrato social, renombre o hijos de funcionarios públicos o empresarios en el pais. Si una persona en una aldea o area rural es víctima de phishing de datos de cualquier especie, el sistema de justicia penal debe estar entrenado, actualizado y con la formación de principios en ciberseguridad, para poder llevar a cabo un juicio justo.

## 4.4 Análisis de la Entrevista a FE-PROSI (Fiscalía Especial de Propiedad Intelectual y Seguridad Informática) realizada al Abogado Hector Morales

En el marco de la investigación sobre el phishing de datos en Honduras, se llevó a cabo una entrevista con el abogado Héctor Morales, representante de la Fiscalía Especial de Propiedad Intelectual y Seguridad Informática (FE-PROSI). Sus respuestas brindaron información valiosa sobre las modalidades de phishing más frecuentes, las deficiencias del sistema de justicia penal y las posibles soluciones para abordar este creciente problema en el país.

### 4.4.1 ¿Qué tipos de phishing de datos o robo de datos personales, ha identificado con mayor frecuencia en Honduras en los últimos 5 años?

*Respuesta del Abogado Hector Morales:* Entre los delitos que más se dan, son el robo de datos vía la aplicación de whatsapp, que consiste en que le bloquean su whatsapp a través de otro número de teléfono, le mandan un mensaje a su whatsapp donde le dicen que sus datos quieren actualizarlos a través de un click. Con ese click le hackean, le roban toda su información y queda bloqueada su cuenta de whatsapp. Una vez robada la cuenta de whatsapp, usted queda bloqueado de whatsapp, la persona que le extrajo la información, se lleva todos los contactos de la víctima y empieza a mandarle mensajes a cada uno de ellos para continuar con el robo, haciéndose pasar como titulares de esos números robados.

### 4.4.3 ¿Cuáles considera que son las principales deficiencias del sistema de justicia penal en Honduras, en la lucha contra el phishing de datos?

Respuesta del Abogado Hector Morales: Como Ministerio Publico tenemos deficiencias en investigación, por el hecho de que no tenemos en este momento la práctica, ni el conocimiento para decir por donde vamos a investigar un delito de phishing o un delito de acceso no autorizado a sistemas informáticos.

Estamos dando respuesta a la sociedad en la presentacion de requerimientos fiscales, pero sin capacitación externa o interna hemos aprendido, ha sido con las buenas prácticas que hemos aprendido como investigar ciberdelitos, por ejemplo, que elementos de prueba vamos a buscar, para poder presentar las acciones ante la autoridad judicial. Por qué el ente investigativo como tal, llamado DPI, no realiza su trabajo como tal, entonces, las acciones que hemos presentado, es por las investigaciones que hemos hecho aquí en interno como Fiscalía Especial de Propiedad Intelectual y Seguridad Informática y ministerio público.

Desde la entrada en vigencia del código penal en el mes de junio del 2023, en materia de delitos informáticos, solo hemos presentado como 3 casos, no han sido muchos los que hemos presentado, de los cuales no es fácil investigar, los hemos presentado por acceso no autorizados a sistemas informáticos, usurpación de identidades, por lavado de activos, porque, como el dinero lo mueven, de cuenta en cuenta, lo transforman, lo ocultan, lo convierten, entonces tambien va aparejado con el delito de lavado de activos, se necesitan bastantes pericias técnicas, hemos hecho uso de pericias técnicas a través del departamento técnico científico de la ATI, expreso.

### 4.4.5 ¿Cuál cree que es la forma de prevención más efectiva, que el marco legal en honduras podría implementar para prevenir más ataques de phishing de datos en el pais?

Respuesta del Abogado Hector Morales: El marco legal no le da una forma de prevención, una forma de prevenir es que cada uno de los ciudadanos pongamos de nuestra parte a través de la concienciación y tener conocimiento de en que consiste el phishing de datos, en que consiste un delito informático,



que la población sepa que es un delito informático, en que consiste una suplantación de identidad, expreso.

Que exista la cultura de la denuncia del altercado a la entidad competente

Que el Sistema Financiero Nacional, imponga mayor control de seguridad a lo interno de sus empleados, sobre los sistemas informáticos, ya que los empleados son quienes manejan las claves o los accesos a los sistemas informáticos, también expreso.

Que la Comisión Nacional de Bancas y Seguros como ente regulador, exija controles para mayor seguridad a nivel de sistemas informáticos para que el Sistema Financiero Nacional los implemente como protocolo de seguridad, a lo interno sus Bases de Datos para que los ciberdelincuentes no puedan tener acceso al mismo. Cada banco debe tener un protocolo de seguridad bastante rígido en la protección de datos.

### 4.4.7 ¿Como considera que el sistema de justicia penal en Honduras, podría responder eficazmente al delito de phishing de datos?

*Respuesta del Abogado Hector Morales:* Que exista la voluntad de todos los agentes involucrados en la investigación, llámese bien DPI, de hacer bien su trabajo, para que el ministerio público pueda responder a entablar las acciones correspondientes ante los entes correspondientes del poder judicial, dándole respuesta jurídica y eficiente a la sociedad.

Porque si usted le pregunta a la DPI, ellos le van a decir o le dijeron que están bien capacitados, que hacen bien su trabajo y que han mandado no sé cuántos informes, si yo le dijese cuantos informes han mandado. Aquí las acciones que hemos presentado en materia de Delitos informáticos, es porque el ministerio publico las ha investigado, pero no es porque la DPI ha pasado un informe. En este momento la DPI no ha pasado ningún informe definitivo que diga, okay, con este informe podemos concluir que fulano de tal, cometió el delito de phishing de datos, lo podemos rastrear, está ubicado en tal lugar, ya podemos ejercer acciones jurídicas. La DPI no hace bien su trabajo, expreso.

Hay problemas que salen del alcance de uno, porque dicen, el ministerio publico presento una acción y el Juez lo dejo libre, ¿pero ¿qué pasa? Si usted mira en las penas posibles a imponer de esos delitos, son penas bien bajas, según el Artículo 445 del Código Procesal Penal, estas no se consideran penas legales, manifestó.

121

Otro punto, es que cuando el phishing de datos se presenta como estafa, este se convierte en un delito perseguible a instancia de parte, manifestó. Artículo 26, Numeral 8, Código Procesal Penal. Acciones no autorizadas a sistemas informáticos Art. 398 Código, Procesal Penal, las penas son apenas de 6 a 18 meses de cárcel, no hay castigos más severos. Articulo 26 CPP.

Hay accesos no autorizados a sistemas informáticos y este sistema informático es de un particular, como tambien, hay accesos no autorizados a sistemas informáticos de la administración pública, y cuando sucede este tipo de accesos y violaciones, se le reconoce como Ciber terrorismo o Terrorismo Electronico, Articulo 592 del Código Procesal Penal, manifestó.