Phishing como fraude informático: eficacia del sistema de justicia en la persecución penal

Alexander Rios Taculi[1]

Resumen

El *phishing* es una modalidad de fraude informático que, mediante engaños y el uso de las Tecnologías de la Información y la Comunicación (TIC), busca obtener ilícitamente información confidencial, como claves bancarias y datos financieros. La presente investigación analiza su impacto en el patrimonio y la seguridad digital en el Perú, a partir de la Ley N° 30.096 y de estándares internacionales como el Convenio de Budapest. Asimismo, se examina la relación entre la dogmática penal del *phishing*, las obligaciones de *compliance* bancario —en las que las entidades financieras actúan como gatekeepers o guardianes del sistema financiero— y los factores que dificultan una persecución penal eficaz. El estudio es de tipo aplicado y adopta un enfoque cualitativo basado en el análisis documental de normas legales, doctrina jurídica y jurisprudencia especializada. Además, se analizan estadísticas oficiales del Ministerio Público y de la Defensoría del Pueblo con la finalidad de evaluar la eficacia de la persecución penal de estos delitos. La investigación presenta un alcance descriptivo-explicativo y un diseño no experimental, debido a que no existe manipulación de variables. En este sentido, se busca describir el fenómeno del *phishing* en el ordenamiento jurídico peruano y explicar las causas que afectan la eficacia del sistema de justicia frente a este delito. Los resultados evidencian una brecha crítica en la persecución penal: pese al incremento de denuncias, el 58 % de los casos es archivado por falta de identificación de los autores y solo el 2 % culmina con una sentencia condenatoria, debido principalmente a limitaciones técnicas, presupuestarias e institucionales. Asimismo, en el ámbito administrativo y civil, la jurisprudencia de INDECOPI tiende a trasladar la responsabilidad por cargos indebidos a las entidades bancarias cuando estas incumplen sus deberes de seguridad y monitoreo de operaciones inusuales.

Palabras clave: ciberdelitos, *phishing*, *compliance*, suplantación de identidad.

Cómo citar: Rios, A. (2026). Phishing como fraude informático: eficacia del sistema de justicia en la persecución penal. En Del Castillo, G., Miranda, N. (Eds.). *Lex nova: fronteras jurídicas y desafíos globales*. High Rate Consulting/Universidad Andina del Cusco. https://doi.org/10.38202/lexnova4

1. https://orcid.org/0000-0001-9225-7433, arios@uandina.edu.pe | Universidad Andina de Cusco, Perú.

Phishing as Cyber Fraud: The Effectiveness of the Justice System in Its Criminal Prosecution

Abstract

Phishing is a form of cyber fraud that, through deception and the use of Information and Communication Technologies (ICTs), seeks to unlawfully obtain confidential information, such as banking credentials and financial data. This research analyzes its impact on property and digital security in Peru, based on Law N° 30,096 and international standards such as the Budapest Convention. Likewise, the study examines the relationship between the criminal law doctrine of phishing, banking compliance obligations —in which financial institutions act as gatekeepers of the financial system— and the factors that hinder effective criminal prosecution. The study is applied in nature and adopts a qualitative approach based on the documentary analysis of legal norms, legal doctrine, and specialized jurisprudence. In addition, official statistics from the Public Prosecutor's Office and the Ombudsman's Office are analyzed in order to evaluate the effectiveness of the criminal prosecution of these offenses. The research has a descriptive-explanatory scope and a non-experimental design, since there is no manipulation of variables. In this regard, the study seeks to describe the phenomenon of phishing within the Peruvian legal system and explain the causes that affect the effectiveness of the justice system in addressing this crime. The findings reveal a critical gap in criminal prosecution: despite the increase in complaints, 58 % of cases are dismissed due to the inability to identify the perpetrators, and only 2 % result in a conviction, mainly because of technical, budgetary, and institutional limitations. Likewise, in the administrative and civil spheres, INDECOPI's jurisprudence tends to assign liability for unauthorized charges to banking institutions when they fail to comply with their duties regarding security and the monitoring of unusual transactions.

Keywords: cybercrimes, phishing, compliance, and identity theft.

Introducción

La evolución de las Tecnologías de la Información y la Comunicación (TIC) ha transformado radicalmente el panorama financiero global, al facilitar las transacciones, pero también por abrir la puerta a sofisticadas modalidades delictivas como el *phishing*. Esta forma de fraude informático se basa en el engaño y la manipulación del usuario en el ciberespacio para obtener información confidencial —como claves y números de cuenta— mediante la suplantación de identidad o *spoofing*.

En el contexto peruano, la respuesta normativa se ha consolidado a través de la Ley N° 30.096 (Ley de Delitos Informáticos), la cual busca alinear el sistema jurídico con estándares internacionales, como el Convenio de Budapest para proteger bienes jurídicos de naturaleza pluriofensiva, que incluyen desde el patrimonio hasta la fe pública y la intimidad. No obstante, la normativa por sí sola es insuficiente si no se acompaña de una gestión de riesgos robusta por parte del sector privado. Aquí es donde cobra relevancia el *compliance* bancario, un sistema integral que ha pasado de ser una carga administrativa a un pilar de gobernabilidad que busca identificar y mitigar los riesgos operativos y legales.

Sin embargo, el sistema de justicia enfrenta una brecha crítica en su eficacia. A pesar de que las denuncias por ciberdelitos se han incrementado drásticamente, una gran parte de estas son archivadas debido a la dificultad técnica para identificar a los autores en el anonimato de la red. Ante esta situación, la jurisprudencia actual —liderada por organismos como INDECOPI— ha comenzado a exigir una mayor responsabilidad a las entidades financieras, obligándolas a monitorear patrones de consumo inusuales y estableciendo que el incumplimiento de estos deberes de seguridad traslada la responsabilidad del fraude al banco.

El presente análisis se propone explorar la interconexión entre la dogmática penal del *phishing*, las obligaciones de cumplimiento de las entidades financieras y los desafíos institucionales que impi-

den una persecución penal efectiva, con el fin de determinar la verdadera eficacia del sistema de justicia peruano frente a esta amenaza digital.

Marco Teórico

El phishing como modalidad de fraude informático

El *phishing* se define como una modalidad de fraude o estafa informática que consiste en la obtención de información confidencial de manera fraudulenta, tales como claves de acceso, números de cuentas y códigos bancarios. Según el Consejo General del Poder Judicial, esta conducta se clasifica dentro de la modalidad sociológica de la estafa informática, ya que requiere un despliegue de engaño por parte del autor y una relación con las víctimas mediada por el uso de las Tecnologías de la Información y la Comunicación (TIC) [Cooperación Española Conocimiento/Interconecta (Aula Iberoamericana) & Consejo General del Poder Judicial, 2021].

Desde una perspectiva técnica, el *phishing* es considerado un delito propiamente informático, puesto que es una figura delictiva que no podría existir sin la informática o el internet (Gobierno de la Provincia de Buenos Aires, 2022). Su ejecución implica que el atacante utiliza el engaño en el ciberespacio para manipular la voluntad del usuario y lograr que este facilite voluntariamente, aunque bajo error, sus credenciales o datos sensibles. El objetivo final de esta práctica suele ser el beneficio lucrativo del delincuente o de un tercero, lo que afecta tanto el patrimonio económico del sujeto pasivo como el derecho fundamental a la protección del entorno virtual (Arroyo Zapatero & Nieto Martín, 2013) [Cooperación Española Conocimiento/Interconecta (Aula Iberoamericana) & Consejo General del Poder Judicial, 2021].

En ese contexto, se tiene que esta modalidad "se produce cuando se utiliza la identidad personal de otro (*spoofing*) mediante la falsificación de sitios web, para conducir a los consumidores a quienes confíen en la veracidad del mensaje y divulguen los datos objetivos" (Miró Llinares, 2012). En ese sentido, el *phishing* requiere el uso de la red de internet para acceder a información sensible. De este modo, el agente activo remite un mensaje de texto o SMS al agente pasivo, quien, al confiar en la veracidad de la información, ingresa al link o enlace que permite el acceso a la información sensible de su cuenta bancaria o financiera.

Esta condición hace que el *phishing* sea catalogado como delito de tipo propio, ya que el uso del sistema informático o de internet, resulta necesario para la comisión del fraude informático. En este contexto, el agente activo hace uso de este medio para enviar mensajes con aparente validez, crear confianza en el agente pasivo y así acceder a información sensible.

El compliance bancario

Este procedimiento se define como un sistema integral de gestión y cultura organizacional diseñado para identificar, prevenir, gestionar y reaccionar ante los riesgos de incumplimiento de normativas legales, regulaciones externas y estándares éticos internos (Alvear-Tobar, 2024). En el sector financiero, este concepto trasciende la mera observancia de leyes, constituyéndose como un pilar fundamental de la gobernabilidad corporativa que busca garantizar la estabilidad del sistema y proteger los intereses de los depositantes y otros portadores de riesgo (van Greuning & Brajovic Bratanovic, 2010).

El término proviene del inglés *to comply with* (cumplir, respetar) y, en el contexto bancario, implica un procedimiento robusto para asegurar que la entidad y sus empleados sigan tanto el *hard law* (leyes obligatorias) como el *soft law* (códigos de conducta voluntarios). Según Alvear-Tobar (2024), el *compliance* no debe entenderse solo como un sistema de control, sino como una filosofía de buen gobierno que busca dotar a la persona jurídica de un carácter íntegro y cumplidor.

Dentro de la banca, el *compliance* está intrínsecamente ligado al riesgo operacional, el cual es definido por el Comité de Basilea como el riesgo de sufrir pérdidas por fallos en procesos, personal o sistemas, e incluye explícitamente el riesgo legal (Pineda Galarza, 2022). Este último se entiende como la posibilidad de que sentencias adversas o contratos inaplicables perturben las operaciones de un banco (Pineda Galarza, 2022).

En el contexto de la sociedad del riesgo y el cibercrimen, se define como el conjunto de medidas de autorregulación adoptadas por las entidades financieras para controlar sus plataformas tecnológicas y evitar que funcionen como fuentes de peligro. Este rol preventivo implica que las instituciones asuman la posición de garante de vigilancia, implementen programas de cumplimiento normativo que permitan filtrar contenidos, monitorear transacciones y mitigar riesgos antes de que ocurra una lesión a los bienes jurídicos de terceros (Jiménez Bernales, 2023).

Según Ospina Díaz y Sanabria Rangel (2020), un componente esencial del *compliance* es la implementación de Sistemas de Gestión de Seguridad

de la Información (SGSI), los cuales permiten que los riesgos cibernéticos sean conocidos, asumidos y gestionados de forma sistemática y estructurada. Estos sistemas se fundamentan en estándares internacionales como la ISO/IEC 27001, que proporciona una metodología para reducir los riesgos hasta niveles aceptables, asegurando la confidencialidad, integridad y disponibilidad de los activos de información financiera.

Componentes y objetivos del compliance bancario

Para que un programa de cumplimiento sea efectivo, y no sea considerado un simple "paper compliance" (cumplimiento superficial sin impacto real), debe contar con elementos mínimos que las fuentes sistematizan de la siguiente manera:

a. *Identificación y gestión de riesgos:* determinar las actividades donde pueden cometerse delitos o infracciones, priorizándolas según su severidad y probabilidad de ocurrencia (Alvear-Tobar, 2024, p 131).
b. *Debida diligencia y KYC:* los bancos tienen la obligación de implementar políticas de "Conocimiento del Cliente" (Know Your Customer) para entender los negocios de sus usuarios y prevenir el lavado de activos y el financiamiento del terrorismo (Pineda Galarza, 2022, p. 49).
c. *Independencia y autonomía:* la función de cumplimiento debe estar separada de las líneas de negocio, contar con un oficial de cumplimiento con autoridad suficiente y línea directa con el Directorio (van Greuning & Brajovic Bratanovic, 2010, p 42).
d. Cultura de integridad: el éxito del sistema depende del "tono desde lo alto" (*tone at the top*), donde la alta gerencia promueve el cumplimiento por convicción y no solo por miedo a la sanción.
e. Mecanismos de detección: incluye canales de denuncia (*whistleblowing*) seguros y confidenciales, además de auditorías internas y externas periódicas (Alvear-Tobar, 2024, p 131).

El compliance como salvaguarda sistémica

El *compliance* como salvaguarda sistémica se define como un proceso de integración social y organizacional que articula estrategias proactivas encaminadas a la anticipación, prevención y contención de los delitos cibernéticos (Díaz Samper *et al.,* 2023). Este concepto trasciende el mero cumplimiento normativo, constituyéndose como una barrera de contención de riesgos diseñada para proteger la funcionalidad informática como un bien jurídico supraindividual.

Desde una perspectiva analítica basada en las fuentes, el *compliance* bancario presenta una naturaleza dual que lo distingue del cumplimiento en otros sectores comerciales.

En primer lugar, existe una corresponsabilidad público-privada. El Estado delega en los bancos la función de ser los "ojos" del regulador en el mercado, especialmente en la detección de flujos de dinero ilícito (Alvear-Tobar, 2024). Esto convierte a los Oficiales de Cumplimiento en *gatekeepers* (guardianes) internos que asumen un deber de garante respecto de la peligrosidad de la actividad financiera (Arroyo Zapatero & Nieto Martín, 2013).

En segundo lugar, el impacto del incumplimiento en la banca es cualitativo y sistémico. Mientras que en una empresa ordinaria una multa puede constituir un costo de negocio, en un banco el riesgo legal puede derivar en una crisis de confianza que provoque retiros masivos de depósitos o incluso la revocación de la licencia bancaria, lo que afecta a la economía nacional (Arroyo Zapatero & Nieto Martín, 2013).

Finalmente, el análisis propio sugiere que el *compliance* bancario ha evolucionado de ser una carga administrativa a convertirse en una ventaja competitiva. Las entidades que demuestran una cultura de integridad sólida no solo mitigan sanciones penales o administrativas, sino que también reducen su costo de capital al generar una percepción de menor riesgo ante inversionistas y clientes (Alvear-Tobar, 2024).

Responsabilidad jurídica de las entidades financieras

El concepto de responsabilidad jurídica de las entidades financieras ha experimentado una transformación radical en el siglo XXI. Ha transitado de una inmunidad histórica, bajo el dogma *societas delinquere non potest*, hacia un sistema de corresponsabilidad penal y administrativa basado en el control interno (Arroyo Zapatero & Nieto Martín, 2013). En el marco del "capitalismo regulatorio", el Estado delega en las instituciones financieras funciones de vigilancia que antes eran exclusivas del poder público, lo que las convierte en auténticos *gatekeepers* o guardianes del sistema económico.

Esta responsabilidad se define como la obligación legal de estas organizaciones de responder ante el Estado —ya sea por la vía penal, administrativa o civil— por las infracciones cometidas en su seno que deriven de un defecto de organización o de la falta del debido control sobre sus directivos y

empleados (Arroyo Zapatero & Nieto Martín, 2013).

En el sistema español, tras la reforma del Código Penal de 2010 y 2015, esta responsabilidad no es meramente vicaria (por el hecho de otro), sino que se fundamenta en la culpabilidad por la propia desorganización de la entidad. Es decir, el injusto de la persona jurídica reside en no haber implementado medidas eficaces para contrarrestar el riesgo de comisión de delitos, como el blanqueo de capitales, la estafa o la corrupción (Arroyo Zapatero & Nieto Martín, 2013).

Desde mi perspectiva, la responsabilidad jurídica de las entidades financieras representa la privatización de la lucha contra la criminalidad económica. Al imponer penas graves, el legislador no solo busca castigar, sino motivar a las entidades a invertir en sus propios sistemas "policiales" internos.

Sin embargo, existe un riesgo inherente de "cosmética jurídica", donde las entidades adquieren programas de cumplimiento como un "seguro antimultas" sin intención real de cambiar su cultura corporativa. La verdadera responsabilidad no debería nacer solo de la existencia del programa, sino de su eficacia operativa. En el sector financiero, donde el impacto de un delito puede tener efectos sistémicos en la economía nacional, la responsabilidad jurídica debe entenderse no solo como una carga punitiva, sino como un factor de buen gobierno que genera valor y protege la reputación institucional ante los grupos de interés.

El "debido control" en el sector financiero

El concepto de debido control en el ámbito digital se traduce en la adopción de medidas técnicas y organizativas adecuadas para proteger la funcionalidad informática y la confidencialidad de los datos (Mayer Lux & Oliver Calderón, 2020). Según las fuentes, el Perú se encuentra todavía en una etapa inicial del Modelo de Madurez de Capacidades en Ciberseguridad (CMM), lo que indica que muchas instituciones poseen una capacidad institucional restringida para enfrentar riesgos de manera proactiva. Por ello, un programa de cumplimiento robusto debe integrar modelos de madurez que traduzcan las obligaciones legales en acciones operativas sostenibles. Esto permite pasar de la simple comprensión técnica al cumplimiento normativo real (Torres Gamarra & Zúñiga Carnero, 2026).

En el sector financiero, el debido control implica una inversión significativa en infraestructura y talento humano especializado, así como una colaboración estrecha con el gobierno para desarrollar protocolos de seguridad sólidos. Las fuentes destacan que el factor humano sigue siendo una de las mayores vulnerabilidades; por tanto, el *compliance* debe incluir programas de concienciación y alfabetización digital que reduzcan el riesgo de errores internos que faciliten el acceso ilícito a los sistemas.

Para las entidades financieras, la responsabilidad jurídica está intrínsecamente ligada al cumplimiento de normativas sectoriales específicas que exigen un estándar de diligencia superior al de otras empresas. Según Arroyo Zapatero & Nieto Martín (2013), las instituciones de crédito tienen la obligación de presentar una "organización comercial ordenada" que garantice el respeto a la legalidad.

a. **Prevención de blanqueo de capitales:** las entidades deben desarrollar sistemas de aseguramiento y control específicos (como la identificación del cliente o *know your client*) para prevenir la entrada de capitales ilícitos en el circuito financiero (Arroyo Zapatero & Nieto Martín, 2013).
a. **Mercado de valores:** se impone la creación de unidades de cumplimiento independientes que eviten el abuso de información privilegiada y garanticen la transparencia en la contratación (Arroyo Zapatero & Nieto Martín, 2013).

Desde la perspectiva legal, el acceso ilícito a sistemas informáticos en el Perú se tipifica bajo la premisa de que se deben haber vulnerado medidas de seguridad establecidas para impedirlo. Esto refuerza la importancia del debido control: si una entidad financiera implementa medidas de seguridad lógica (como autenticación robusta o cifrado) y estas son superadas por un tercero, la existencia de tales controles demuestra la diligencia de la organización (Elías Puelles, 2023). Por el contrario, la ausencia de estas medidas o un control deficiente podrían invalidar cualquier intento de utilizar el cumplimiento como eximente.

El programa de compliance como eximente o atenuante

Un elemento central en la configuración de esta responsabilidad es el Programa de Cumplimiento (Compliance Program). Este no es simplemente un documento estático, sino un sistema dinámico de gestión de riesgos (Arroyo Zapatero & Nieto Martín, 2013). Según la Asociación Española de Compliance (ASCOM, 2024), la función de cumplimiento debe gozar de autonomía e independencia para ser considerada efectiva por los tribunales.

Para que un programa de cumplimiento tenga efectos jurídicos (eximiendo o atenuando la pena),

debe cumplir con:

a. **Identificación de riesgos:** conocer las amenazas específicas según el giro y volumen de la entidad (Asociación Española de Compliance - ASCOM, 2017).
a. **Cultura de cumplimiento:** no basta con una "fachada" o cosmética legal; se requiere que la alta dirección promueva activamente el respeto a la norma (*tone at the top*) (Arroyo Zapatero & Nieto Martín, 2013).
a. **Canales de denuncia:** existencia de mecanismos confidenciales para reportar irregularidades sin temor a represalias (Arroyo Zapatero & Nieto Martín, 2013; Asociación Española de Compliance - ASCOM, 2017).

La responsabilidad jurídica también abarca el control de los riesgos internos. El concepto de abuso de confianza se aplica cuando un agente accede a un sistema informático y excede la autorización conferida (por ejemplo, un técnico o empleado con credenciales legítimas que accede a archivos personales no autorizados). Las leyes agravan la responsabilidad cuando el delito se comete mediante el abuso de una posición especial de acceso a información reservada, debido al ejercicio de un cargo o función dentro de la entidad.

Las entidades financieras tienen la responsabilidad jurídica de mantener la funcionalidad informática, definida como el conjunto de condiciones que permiten que los sistemas realicen operaciones de almacenamiento y transferencia de datos dentro de un marco de riesgo tolerable. Al tratarse el fraude informático de un delito pluriofensivo, la falla en los sistemas de una entidad no solo afecta el patrimonio individual del cliente, sino que también lesiona un bien jurídico supraindividual: la confianza en el sistema financiero digital.

Metodología

En el presente trabajo se ha empleado una investigación de tipo aplicado, con enfoque cualitativo, dado que se basa en el análisis documental. Si bien se hace uso de estadísticas, estas no han sido objeto de manipulación por el investigador, sino de análisis del fenómeno objeto de estudio. En ese contexto, Hernández Sampieri *et al.* (2014) refieren que el enfoque cualitativo se "selecciona cuando el propósito es examinar la forma en que los individuos perciben y experimentan los fenómenos que los rodean, profundizando en sus puntos de vista, interpretaciones y significados" (p. 358).

En ese sentido, en el presente trabajo se analizan las normas, la doctrina y la jurisprudencia especializada en materia penal y administrativa relacionada con el *phishing*. En la vía administrativa se sanciona a empresas financieras por no haber ejecutado debidamente el *compliance*, el cual finalmente ha sido utilizado por la ciberdelincuencia. Esto permite conocer la eficacia del sistema jurídico en cuanto a la persecución de los delitos vinculados al fraude informático.

En lo que respecta al diseño, es no experimental, dado que no se realiza ninguna manipulación de las variables. En cuanto al alcance, es de tipo descriptivo-explicativo, ya que, desde el enfoque cualitativo, se describe el fenómeno y su regulación en el sistema jurídico peruano, y se analizan las posibles causas de la eficacia en la administración de justicia respecto de este delito.

Resultados

El análisis de la ciberdelincuencia en el ordenamiento jurídico peruano revela una estructura normativa en constante evolución, que busca equilibrar el avance tecnológico con la protección de derechos fundamentales. Los resultados se sistematizan en cuatro ejes principales:

Sistematización y evolución del marco normativo

La investigación muestra que el Perú ha transitado de una respuesta penal inicial limitada (hurto telemático) a un sistema especializado robusto encabezado por la Ley N° 30.096 (Ley de Delitos Informáticos) (Defensoría del Pueblo, 2023; Ley de Delitos Informáticos - Ley N° 30.096, 2023). Este marco legal tiene por objeto prevenir y sancionar conductas ilícitas que afectan sistemas y datos informáticos, y se alinea con los estándares del Convenio de Budapest para garantizar una lucha eficaz contra la criminalidad transnacional (Ley de Delitos Informáticos - Ley N° 30.096, 2023).

Se observa una diversificación de las conductas punibles, categorizadas según el bien jurídico afectado:

- **Datos y sistemas informáticos:** acceso ilícito, atentado a la integridad de datos y sistemas, y abuso de dispositivos (Defensoría del Pueblo, 2023).
- **Indemnidad y libertad sexual:** proposiciones sexuales a menores (*grooming*) y pornografía infantil (Ley de delitos informáticos - Ley N° 30.096, 2023).
- **Patrimonio:** fraude informático (Ley de delitos informáticos - Ley n° 30.096, 2023).
- **Fe pública e intimidad:** Suplantación de

identidad y tráfico ilegal de datos(Ley de delitos informáticos - Ley N° 30.096, 2023).

Análisis dogmático de los tipos penales

Desde una perspectiva dogmática, el bien jurídico tutelado es de naturaleza pluriofensiva (Defensoría del Pueblo, 2023).

Si bien el objeto central es la información (su confidencialidad, integridad y disponibilidad), la conducta típica suele colisionar con otros intereses como el patrimonio, la libertad sexual o la fe pública.

El análisis de la tipicidad revela dos estructuras fundamentales:

- **Delitos de mera actividad:** como, por ejemplo,el acceso ilícito (art. 2), que se consuma al vulnerar las medidas de seguridad de un sistema sin necesidad de un resultado posterior (Villavicen cio Terreros, 2014).
- **Delitos de resultado:** como, por ejemplo, el fraude informático (art. 8) y la suplantación de identidad (art. 9), que exigen la acreditación de un perjuicio real o la obtención de un provecho ilícito para su consumación (Villavicencio Terreros, 2014).

Respecto al sujeto activo, la doctrina destaca un perfil especializado, a menudo vinculado a "delincuentes de cuello blanco" con habilidades técnicas avanzadas (*hackers* o *crackers*) (Villavicencio Terreros, 2014).

Jurisprudencia y responsabilidad civil-administrativa del sector financiero

Un resultado crítico de la investigación es la delimitación de la responsabilidad de las entidades financieras frente a ciberdelitos patrimoniales. El análisis de resoluciones de INDECOPI establece que el deber de idoneidad (art. 19 del Código de Protección al Consumidor) obliga a los bancos a implementar sistemas de monitoreo de operaciones inusuales (INDECOPI, 2022).

Los criterios jurisprudenciales actuales determinan que:

- Las entidades financieras deben detectar operaciones que no correspondan al comportamiento habitual de consumo del usuario (Defensoría del Pueblo, 2023) (INDECOPI, 2024).
- Ante una operación sospechosa (por ejemplo, un giro por un monto inusualmente alto), el banco tiene la obligación de levantar una alerta y bloquear preventivamente la cuenta (INDECOPI, 2022).
- La falta de adopción de estas medidas de seguridad traslada la responsabilidad del cargo indebido al proveedor financiero, incluso si se emplearon claves secretas, cuando se demuestra que la operación era manifiestamente inusual (INDECOPI, 2022 y 2024).

Diagnóstico situacional y eficacia de la persecución penal

Los datos estadísticos indican un crecimiento alarmante: las denuncias por ciberdelitos se cuadruplicaron entre 2018 y 2021. El fraude informático representa el 72 % de los casos, seguido por la suplantación de identidad (20%) (Defensoría del Pueblo, 2023).Sin embargo, existe una brecha significativa en la eficacia del sistema de justicia:

- **Archivamiento fiscal:** el 58% de las denuncias en el Ministerio Público han sido archivadas por falta de identificación de los autores (Defensoría del Pueblo, 2023).
- **Baja tasa de sentencias:** el Poder Judicial emitió condenas solo para el 2 % de las denuncias registradas entre 2015 y 2019 (Defensoría del Pueblo, 2023).
- **Limitaciones institucionales:** se evidencia una carencia de recursos especializados en los Departamentos de Investigación Criminal (Depincri). Solo el 9 % de los Depincri supervisados cuenta con un área específica de ciberdelincuencia y su capacidad tecnológica forense es calificada como casi nula (Defensoría del Pueblo, 2023).

Discusión

Para elaborar una discusión de resultados exhaustiva basada en las fuentes proporcionadas, se aplica el método de triangulación de resultados, que integra tres dimensiones fundamentales: la dimensión normativa y teórica (leyes y convenios), la dimensión empírica e institucional (estadísticas y retos de la fiscalía y la policía) y la dimensión jurisprudencial y práctica (casos de INDECOPI y de la Corte Suprema).

Dimensión normativa: el marco legal frente a la evolución del ciberdelito

Los resultados coinciden en que el ciberdelito es un fenómeno "hijo de su tiempo" que trasciende fronteras. La base de la persecución penal en el Perú es la Ley N° 30.096 (Ley de Delitos Informáticos), la cual se armoniza con el Convenio de Budapest.

- **La pluriofensividad:**la teoría y la norma coinciden en que estos delitos no solo afectan la información, sino un conjunto de bienes jurídicos como el patrimonio, la fe pública, la indemnidad sexual y la intimidad [Ministerio Público (Oficina de Análisis Estratégico contra la Criminalidad)], 2021].
- **El *compliance*penal:** las fuentes más recientes destacan que la prevención no debe ser solo estatal; se requiere que las personas jurídicas implementen programas de cumplimiento (*compliance*) para mitigar riesgos penales y evitar ser utilizadas para el lavado de activos derivado de ciberdelitos (Arroyo Zapatero & Nieto Martín, 2013)

Dimensión empírica: la brecha entre denuncias y sanciones

Al contrastar la norma con la realidad operativa, se observa una contradicción crítica entre el volumen de criminalidad y la capacidad de respuesta del Estado.

- **Predominio del fraude:** las estadísticas policiales y fiscales confirman que el fraude informático es el delito más recurrente, pues representael 78.2% de las denuncias vinculadas a la Ley N° 30.096[Ministerio Público (Oficina de Análisis Estratégico contra la Criminalidad), 2021].
- **Impunidad estructural:** un resultado alarmante es que el 58% de las denuncias son archivadas a nivel fiscal porque no se logra identificar a los autores [Ministerio Público Fiscalía de la Nación (Oficina de Análisis Estratégico contra la Criminalidad), 2021].
- **Cuellos de botella institucionales:** la Policía (DIVINDAT y DEPINCRI) reporta que la falta de recursos técnicos, el uso de *software* con licencias vencidas y la demora de más de dos meses en el trámite para levantar el secreto bancario o de comunicaciones impiden investigaciones eficaces (Defensoría del Pueblo, 2023).

Dimensión jurisprudencial: responsabilidad civil y bancaria

La triangulación con los casos prácticos (INDECOPI y casaciones) muestra cómo se aplica la protección al consumidor frente al ciberdelito financiero.

- **El deber de idoneidad y el patrón de consumo:** INDECOPI ha establecido un criterio sólido según el cual las entidades financieras tienen el deber de monitorear y detectar operaciones inusuales que no correspondan al historial de consumo del cliente (INDECOPI, 2022).
- **Responsabilidad compartida:** en el caso de transferencias no autorizadas, si bien el banco suele alegar la "ruptura del nexo causal" por negligencia del usuario al custodiar sus claves, la autoridad administrativa determina que la falta de alerta ante un consumo atípico genera responsabilidad en la entidad (INDECOPI, 2022).
- **Unidad de acción y bien jurídico:** la Corte Suprema aclara que un mismo acto en redes sociales (como publicar noticias falsas) puede derivar en delitos distintos (difamación y pánico financiero) sin vulnerar el *ne bis in idem*, ya que protegen bienes jurídicos diferentes (Corte Suprema de la República, 2021).

Tabla 1.
Tabla de evaluación, actores, evidencia, norma y jurisprudencia

Punto de interés	Teoría/norma	Realidad (cifras/instituciones)	Jurisprudencia/casos	Teoría/norma
Identificación del autor	El anonimato es una característica central del ciberdelito.	El 58% de casos se archivan por no identificar al autor.	Se dificulta el enjuiciamiento por falta de peritajes digitales oportunos.	El anonimato es una característica central del ciberdelito.
Rol de los bancos	El *compliance* sugiere controles internos robustos.	Los bancos tardan meses en responder a mandatos judiciales.	INDECOPI sanciona si el banco no detecta consumos inusuales de inmediato.	El *compliance* sugiere controles internos robustos.
Evidencia digital	Es volátil y requiere cadena de custodia estricta.	Los peritos fiscales tienen alta demanda y los fiscales envían requerimientos poco claros.	El valor probatorio depende de la "integridad" y "autenticidad" (valor Hash).	Es volátil y requiere cadena de custodia estricta.

Conclusiones

El *phishing* se define como una modalidad de estafa informática que utiliza el engaño en el ciberespacio —especialmente mediante la suplantación de identidad o *spoofing*— para obtener información confidencial de forma fraudulenta. Se considera un delito de tipo propio, ya que su ejecución resulta imposible sin el uso de las Tecnologías de la Información y la Comunicación (TIC).

El cumplimiento normativo (*compliance*) ha dejado de ser una carga administrativa para convertirse en una filosofía de buen gobierno y en una ventaja competitiva. Las entidades financieras actúan como *gatekeepers* (guardianes) del sistema y asumen una corresponsabilidad público-privada en la detección de flujos ilícitos. Un programa de cumplimiento efectivo debe ser operativo y no meramente cosmético para servir como atenuante o eximente de responsabilidad jurídica.

Según la jurisprudencia de INDECOPI, los bancos tienen un deber de idoneidad que los obliga a monitorear y detectar operaciones inusuales que no coincidan con el patrón de consumo del cliente. La ausencia de alertas o bloqueos preventivos ante consumos atípicos traslada la responsabilidad del cargo indebido a la entidad financiera, incluso si el atacante utilizó las claves secretas del usuario.

Aunque las denuncias por ciberdelitos se cuadruplicaron entre 2018 y 2021 —siendo el fraude informático el 72 % de los casos—, la tasa de sentencias condenatorias es de apenas el 2 %. Esta situación revela una crisis de eficacia en el sistema de persecución penal.

Existe una impunidad estructural, evidenciada en que el 58 % de las denuncias es archivado por la fiscalía debido a la imposibilidad de identificar a los autores. Esta situación responde a la carencia de recursos especializados: solo el 9 % de los Departamentos de Investigación Criminal cuenta con áreas de ciberdelincuencia, y los peritos operan con tecnología forense casi nula o con licencias vencidas.

La investigación de estos delitos se ve entorpecida por la volatilidad de la evidencia digital y por la excesiva demora —superior a dos meses— en los trámites judiciales para levantar el secreto bancario o de las comunicaciones. Esta situación constituye un problema para investigaciones futuras, dada la escasa bibliografía nacional vinculada a estos estudios, así como la limitada disponibilidad de informes periciales especializados en cibercrimen, lo que evidencia una insuficiente respuesta del Estado frente a este fenómeno.

Si bien existen normas jurídicas, estas no alcanzan plenamente los estándares internacionales necesarios para una adecuada persecución del cibercrimen y su debido juzgamiento. Prueba de ello es el creciente archivo de denuncias vinculadas a estos delitos, lo que se explica por la falta de capacitación de los órganos encargados de la persecución penal y por la insuficiente implementación de la policía peruana para rastrear el origen de estas defraudaciones. A ello se suma la demora en el levantamiento del secreto bancario, circunstancias que dificultan de manera significativa la persecución criminal.

Referencias

Alvear-Tobar, E.J. (2024). El compliance y la cultura de cumplimiento como mecanismos para prevenir la corrupción (Compliance and a culture of compliance as mechanisms to prevent corruption). *593 Digital Publisher CEIT, 9*(6-1), 124–133. https://doi.org/10.33386/593dp.2024.6-1.2975

Arroyo Zapatero, L., & Nieto Martín, A. (Dirs.). (2013). *El derecho penal económico en la era compliance (Economic criminal law in the compliance era)*. Tirant lo Blanch.

ASCOM (2024). *Libro blanco sobre la función de compliance* (Edición noviembre 2024) [White paper on the compliance function (November 2024 edition)].

Congreso de la República. (2013, octubre 22). Ley N° 30096, Ley de delitos informáticos (Law N° 30096, Law on Computer Crimes). El Peruano. https://www.leyes.congreso.gob.pe/Documentos/Leyes/30096.pdf

Cooperación Española Conocimiento/Interconecta [Aula Iberoamericana] & Consejo General del Poder Judicial. (2021, noviembre 2 al 12). *Curso "La ciberdelincuencia: tratamiento preventivo, procesal y sustantivo desde una perspectiva internacional 2.ª edición"* (Cybercrime course: preventive, procedural and substantive treatment from an international perspective, 2nd edition). https://www.ejemplo.com/ciberdelincuencia.pdf

Corte Suprema de Justicia de la República. (2021, 5 de abril). Casación N.° 1197-2019, Sullana: Difamación agravada, pánico financiero, ne bis in idem y concurso de delitos [Sentencia] (Cassation No. 1197-2019, Sullana: Aggravated defamation, financial panic, ne bis in idem and concurrence of crimes) [Judgment]. Poder Judicial del Perú. https://img.lpderecho.pe/wp-content/uploads/2021/10/Casacion-1197-2019-Sullana-LPDerecho.pdf

Defensoría del Pueblo. (2023, mayo). La ciberdelincuencia en el Perú: Estrategias y retos del Estado (Cybercrime in Peru: Strategies and challenges for the State) (Informe Defensorial N.° 001-2023-DP/ADHPD). https://www.defensoria.gob.pe/wp-content/uploads/2023/05/INFORME-DEF-001-2023-DP-ADHPD-Ciberdelincuencia.pdf

Díaz Samper, G.A.J., Molina Garzón, A.L., Serrador Osorio, L.E., & Cárdenas Beltrán, J.M. (2023). Aproximación al ciberdelincuente desde la perspectiva del control social (An approach to cybercriminals from the perspective of social control). *Revista Criminalidad, 65*(3), 81–95. https://doi.org/10.47741/17943108.508

Elías Puelles, R.N. (2023). El delito de hacking o acceso ilícito a sistemas informáticos (The crime of hacking or unauthorized access to computer systems). *THĒMIS-Revista de Derecho,* (83), 413-433. https://doi.org/10.18800/themis.202301.023

Gobierno de la Provincia de Buenos Aires. (2022). Cibercrimen y delitos informáticos (Cybercrime and computer crimes). *Revista institucional del Ministerio de Seguridad,* (1), https://www.mseg.gba.gov.ar/areas/Vucetich/MANUALES%20DE%20MATERIAS%202022/MANUAL%20Cibercrimen%20y%20delitos%20inform%C3%A1ticos.pdf

Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, M.P. (2014). *Metodología de la investigación (Research Methodology)* (6.ª ed.). McGraw-Hill.

Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (INDECOPI). (2022, febrero 15). Resolución Final N° 008-2022/CPC-INDECOPI-PUN (Expediente N° 47-2021-AP/CPC-INDECOPI-PUN) [Final Resolution N° 008-2022/CPC-INDECOPI-PUN (File N° 47-2021-AP/CPC-INDECOPI-PUN)]. https://img.lpderecho.pe/wp-content/uploads/2022/05/008-2022-CPC-INDECOPI-PUN-Juris.pe_.pdf

Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (INDECOPI). (2024, agosto 19). Resolución N° 2293-2024/SPC-INDECOPI (Expediente 0104-2023/CPC-INDECOPI-LAL) [Resolution N° 2293-2024/SPC-INDECOPI (File 0104-2023/CPC-INDECOPI-LAL)].

Jiménez Bernales, L. A. (2023). El estado actual del cibercrimen en Perú y el derecho alemán (The current state of cybercrime in Peru and German law). *Boletín Mexicano de Derecho Comparado,* (167), 197–219. https://doi.org/10.22201/iij.24484873e.2023.167.18367

Mayer Lux, L., & Oliver Calderón, G. (2020). El delito de fraude informático: concepto y delimitación (The crime of computer fraud: concept and delimitation). *Revista Chilena de Derecho y Tecnología, 9*(1), 151-184. https://doi.org/10.5354/0719-2584.2020.57149

Ministerio Público Fiscalía de la Nación (2021, febrero). Ciberdelincuencia en el Perú: pautas para una investigación fiscal especializada (Informe de análisis N.° 04) [Cybercrime in Peru: Guidelines for a specialized prosecutorial investigation (Analysis Report N° 04)]. Oficina de Análisis Estratégico contra la Criminalidad (OFAEC). https://www.gob.pe/institucion/mpfn/informes-publicaciones/1667473-ciberdelincuencia-en-el-peru-pautas-para-su-investigacion-fiscal-especializada

Miró Llinares, F. (2012). *El cibercrimen: Fenomenología y criminología de la delincuencia en el ciberespacio (Cybercrime: Phenomenology and criminology of crime in cyberspace)* (1a ed.). Marcial Pons. https://www.infoem.org.mx/doc/biblioteca/accesoytrans/ciberdelitos/el-cibercrimen.pdf

Ospina Díaz, M.R., & Sanabria Rangel, P.E. (2020). Desafíos nacionales frente a la ciberseguridad en el escenario global: un análisis para Colombia (National challenges in cybersecurity in the global arena: an analysis for Colombia). *Revista Criminalidad, 62*(2), 199-217. https://dialnet.unirioja.es/servlet/articulo?codigo=7667839

Pineda Galarza, J. (2022). El riesgo legal en el sistema financiero: Una mirada práctica a la naturaleza cualitativa de este riesgo y su impacto (Legal risk in the financial system: A practical look at the qualitative nature of this risk and its impact). *THEMIS Revista de Derecho,* (81), 43–61. https://doi.org/10.18800/themis.202201.010

Torres Gamarra, N., & Zúñiga Carnero, M. (2026). Panorama actual de la ciberseguridad: amenazas, legislación y brechas estructurales desde una revisión sistemática (Current cybersecurity landscape: threats, legislation and structural gaps from a systematic review). *Revista InveCom, 6*(1), 1-10. https://doi.org/10.5281/zenodo.15605545

Van Greuning, H., & Brajovic Bratanovic, S. (2010). *Análisis del riesgo bancario: Marco para valorar la gobernabilidad societaria y la administración de riesgos (Banking risk analysis: A framework for assessing corporate governance and risk management)* (3ª ed.). Banco Mundial; Mayol Ediciones. https://documents1.worldbank.org/curated/en/289411468167659269/pdf/482380PUB0SPAH1isk103rd0Ed10Spanish.pdf

Villavicencio Terreros, F. (2014). Delitos informáticos (Computer crimes). *Revista IUS ET VERITAS,* (49),284–299. https://revistas.pucp.edu.pe/index.php/iusetveritas/article/view/13630