UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE DERECHO Y HUMANIDADES
ESCUELA PROFESIONAL DE DERECHO

Modificación código penal sobre responsabilidad de terceros involucrados en ciberdelitos en entidades financieras - Corte Superior de Justicia - Piura - Periodo 2022

TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE:

Abogado

AUTOR:

Ramirez Chiroque, Jhonny Alexander (orcid.org/0009-0006-3979-3011)

ASESOR:

Mgtr. Alva Galarreta, Mirko Juan Jose (orcid.org/0000-0001-8211-1705)

LÍNEA DE INVESTIGACIÓN:

Derecho Penal, Procesal Penal, Sistema de Penas, Causas y Formas del Fenómeno Criminal

LÍNEA DE RESPONSABILIDAD SOCIAL UNIVERSITARIA:

Desarrollo económico, empleo y emprendimiento

PIURA – PERÚ

2023

Dedicatoria

A mi querida esposa, Milagros, y a mi hijo, Gianfranco:

En cada página de este trabajo, en cada palabra escrita y en cada desafío superado, veo reflejado el amor, el apoyo y la inspiración que ustedes me han brindado. A ti, Milagros, por ser mi compañera constante, mi fuente de aliento en los momentos de duda y mi alegría en los tiempos de celebración. Y a ti, Gianfranco, hijo mío, por ser la luz de mis días y la promesa de un futuro brillante, el motor que impulsa mi esfuerzo y dedicación.

Esta tesis es mucho más que un logro académico; es un testimonio de nuestro viaje juntos y de los sueños que seguimos construyendo como familia. Ustedes son mi presente más preciado y mi futuro más esperanzador. Con todo mi amor y gratitud, dedico este trabajo a ustedes, quienes dan sentido a cada paso que doy.

Con amor eterno,

Jhonny Ramirez Chiroque

Agradecimientos

Antes de comenzar, deseo expresar mi más profunda gratitud a aquellos que han hecho posible la realización de esta tesis. En primer lugar, a Dios, por brindarme la fuerza, la sabiduría y la serenidad necesarias para llevar a cabo este proyecto.

Un agradecimiento especial al Mgtr. ALVA GALARRETA, Mirko Juan Jose, cuya guía, conocimientos y consejos han sido fundamentales en mi recorrido académico. Su asesoramiento experto y su apoyo constante han sido piedras angulares en el desarrollo de esta investigación.

Quiero extender mi gratitud a todos aquellos que contribuyeron a esta tesis, ya sea con su tiempo, conocimiento o inspiración. Cada uno de ustedes ha jugado un papel crucial en el éxito de este esfuerzo académico.

Además, mi sincero agradecimiento a la Universidad César Vallejo, que me ha brindado la oportunidad de participar en este programa de titulación. La experiencia y el conocimiento que he adquirido aquí han sido invaluables y han sentado las bases para mi futuro profesional como abogado.

Finalmente, agradezco a mi familia, amigos y seres queridos por su apoyo incondicional y por creer en mí a lo largo de este viaje. Su aliento y amor han sido mi mayor motivación.

UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE DERECHO Y HUMANIDADES

ESCUELA PROFESIONAL DE DERECHO

Declaratoria de Autenticidad del Asesor

Yo, ALVA GALARRETA MIRKO JUAN JOSE, docente de la FACULTAD DE DERECHO Y HUMANIDADES de la escuela profesional de DERECHO de la UNIVERSIDAD CÉSAR VALLEJO SAC - PIURA, asesor de Tesis titulada: "MODIFICACION CODIGO PENAL SOBRE RESPONSABILIDAD DE TERCEROS INVOLUCRADOS EN DELITOS INFORMATIVOS EN ENTIDADES FINANCIERAS EN LA CORTE SUPERIOR DE JUSTICIA - PIURA - PERIODO 2022.", cuyo autor es RAMIREZ CHIROQUE JHONNY ALEXANDER, constato que la investigación tiene un índice de similitud de 14.00%, verificable en el reporte de originalidad del programa Turnitin, el cual ha sido realizado sin filtros, ni exclusiones.

He revisado dicho reporte y concluyo que cada una de las coincidencias detectadas no constituyen plagio. A mi leal saber y entender la Tesis cumple con todas las normas para el uso de citas y referencias establecidas por la Universidad César Vallejo.

En tal sentido, asumo la responsabilidad que corresponda ante cualquier falsedad, ocultamiento u omisión tanto de los documentos como de información aportada, por lo cual me someto a lo dispuesto en las normas académicas vigentes de la Universidad César Vallejo.

PIURA, 25 de Abril del 2024

Apellidos y Nombres del Asesor:	**Firma**
MIRKO JUAN JOSE ALVA GALARRETA **DNI:** 32915659 **ORCID:** 0000-0001-8211-1705	Firmado electrónicamente por: MJALVAGA el 16-05-2024 23:45:21

Código documento Trilce: TRI - 0743421

UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE DERECHO Y HUMANIDADES

ESCUELA PROFESIONAL DE DERECHO

Declaratoria de Originalidad del Autor

Yo, RAMIREZ CHIROQUE JHONNY ALEXANDER estudiante de la FACULTAD DE DERECHO Y HUMANIDADES de la escuela profesional de DERECHO de la UNIVERSIDAD CÉSAR VALLEJO SAC - PIURA, declaro bajo juramento que todos los datos e información que acompañan la Tesis titulada: "MODIFICACION CODIGO PENAL
SOBRE RESPONSABILIDAD DE TERCEROS INVOLUCRADOS EN DELITOS INFORMATIVOS EN ENTIDADES FINANCIERAS EN LA CORTE SUPERIOR DE JUSTICIA - PIURA - PERIODO 2022.", es de mi autoría, por lo tanto, declaro que la Tesis:

1. No ha sido plagiada ni total, ni parcialmente.
2. He mencionado todas las fuentes empleadas, identificando correctamente toda cita textual o de paráfrasis proveniente de otras fuentes.
3. No ha sido publicada, ni presentada anteriormente para la obtención de otro grado académico o título profesional.
4. Los datos presentados en los resultados no han sido falseados, ni duplicados, ni copiados.

En tal sentido asumo la responsabilidad que corresponda ante cualquier falsedad, ocultamiento u omisión tanto de los documentos como de la información aportada, por lo cual me someto a lo dispuesto en las normas académicas vigentes de la Universidad César Vallejo.

Nombres y Apellidos	**Firma**
RAMIREZ CHIROQUE JHONNY ALEXANDER **DNI:** 05645060 **ORCID:** 0009-0006-3979-3011	Firmado electrónicamente por: JHONNYR el 28-05-2024 00:18:58

Código documento Trilce: INV - 1590632

Índice de Contenidos

Índice de Tablas

RESUMEN

Esta tesis examina las modificaciones necesarias en el código penal para abordar la responsabilidad de terceros en delitos informáticos, específicamente en el contexto de las entidades financieras, el ámbito de aplicación de esta tesis está circunscrita a la Corte Superior de Justicia de Piura tomando como referencia el periodo 2022. A través de un enfoque descriptivo-analítico, se analiza la legislación actual y las brechas en la gestión de ciberdelitos, basándose en entrevistas con expertos en el campo. Los resultados revelan una necesidad significativa de actualización legislativa, enfatizando la importancia de la cooperación internacional, la adaptación a las tecnologías emergentes, y el fortalecimiento de la protección de datos y responsabilidad corporativa. Las conclusiones sugieren una estrategia legislativa integral y adaptable, capaz de enfrentar la complejidad y dinamismo de la ciberdelincuencia, especialmente en el sector financiero. Este estudio contribuye a una mejor comprensión de los desafíos legales actuales y proporciona una base para futuras reformas en la legislación sobre delitos informáticos, cambios en el código penal, que mejoraría la seguridad en la información financiera de los usuarios / clientes de todos los productos financieros.

Palabras Clave

Ciberdelincuencia, Legislación Penal, Responsabilidad de Terceros, Entidades Financieras, Cooperación Internacional.

ABSTRACT

This thesis examines the necessary modifications in the criminal code to address third-party responsibility in cybercrimes, specifically in the context of financial institutions. The scope of this thesis is circumscribed to the Superior Court of Justice of Piura, taking the year 2022 as a reference point. Employing a descriptive-analytical approach, the study analyzes the current legislation and the gaps in the management of cybercrimes, based on interviews with experts in the field. The findings reveal a significant need for legislative updates, highlighting the importance of international cooperation, adaptation to emerging technologies, and the strengthening of data protection and corporate responsibility. The conclusions suggest a comprehensive and adaptable legislative strategy, capable of addressing the complexity and dynamism of cybercrime, particularly in the financial sector. This study contributes to a better understanding of the current legal challenges and lays a foundation for future reforms in cybercrime legislation, changes in the criminal code, which would enhance security in the financial information of users/customers of all financial products.

I. INTRODUCCIÓN

En la era de la información digital, la creciente dependencia de la sociedad en las tecnologías de información y comunicación (TIC) ha permeado casi todos los ámbitos de la vida cotidiana. Esta dependencia no solo ha transformado la manera en que nos comunicamos, trabajamos, accedemos a información y buscamos entretenimiento, sino que también ha incrementado exponencialmente nuestra vulnerabilidad a los delitos informáticos. Dichos delitos, que abarcan desde fraudes financieros y robos de identidad hasta ataques de Ransomware y ciber espionaje, han experimentado un auge global, reflejando un aumento tanto en su número como en su complejidad. La ciberdelincuencia, como fenómeno emergente, plantea desafíos sin precedentes para el marco legal existente, demandando una adaptación y evolución legal proactiva y eficaz para enfrentar estas nuevas formas de criminalidad.

En Perú, al igual que en muchos otros países latinoamericanos, se observa que la legislación penal actual no ha logrado mantener el paso con la rápida evolución y sofisticación de los delitos informáticos. Aunque las leyes vigentes proporcionan un cierto nivel de protección, subsisten brechas significativas que facilitan la actuación impune de los ciberdelincuentes. Este contexto destaca la imperiosa necesidad de una revisión y actualización profundas del Código Penal para abordar de manera efectiva la realidad cambiante de la ciberdelincuencia.

La problemática central de esta investigación se enfoca en la responsabilidad de terceros, particularmente de las instituciones financieras, en el contexto de los delitos informáticos en Perú. Se plantea la pregunta crítica: ¿hasta qué punto deben estas entidades ser responsables cuando sus sistemas de seguridad falibles permiten la perpetración de fraudes financieros en línea? Este dilema jurídico y ético requiere un análisis detallado y fundamentado en el derecho, con el fin de esclarecer las obligaciones y responsabilidades de los involucrados.

La legislación peruana en materia de delitos informáticos presenta una laguna significativa en lo que respecta a la definición clara y la atribución de responsabilidades a terceros involucrados en estos crímenes. Esta brecha jurídica no solo dificulta la persecución y sanción efectiva de los ciberdelincuentes, sino que también deja a las víctimas de estos delitos en una situación de desprotección y vulnerabilidad. Por lo tanto, esta investigación busca no solo identificar y describir las insuficiencias del marco legal vigente, sino también proponer modificaciones y mejoras al Código Penal que permitan una respuesta más efectiva y justa frente a los delitos informáticos, enfatizando la responsabilidad de los terceros.

Con un enfoque deductivo, este estudio partirá de una revisión de la legislación existente y teorías relacionadas con la ciberdelincuencia y la responsabilidad de terceros, para luego analizar casos específicos en la Corte Superior de Justicia de Piura, Perú. Este análisis buscará evidenciar las deficiencias legales y proponer soluciones concretas que fortalezcan la protección legal frente a los ciberdelitos, contribuyendo a una mayor seguridad y confianza en el ámbito digital.

La justificación de este estudio radica en la urgente necesidad de adaptar la legislación penal peruana a los desafíos planteados por la ciberdelincuencia, garantizar una protección efectiva a las víctimas de estos delitos y establecer un marco de responsabilidad claro para los terceros involucrados. Asimismo, se espera que los hallazgos y recomendaciones de esta investigación sirvan de guía para futuras reformas legales, no solo en Perú sino también en otros contextos similares, y promuevan un debate informado y constructivo sobre las mejores estrategias para combatir la ciberdelincuencia en la era digital.

Además de los desafíos legales inherentes a la persecución de los ciberdelincuentes, las víctimas de estos delitos a menudo quedan en un limbo jurídico, luchando por encontrar justicia. Una problemática importante es la dificultad de atribuir la responsabilidad en estos casos, especialmente cuando se involucran terceros, como las entidades financieras. Esta tesis examinará el papel

y la responsabilidad de estos terceros en los delitos informáticos, con el objetivo de proporcionar una mayor protección a las víctimas y garantizar la responsabilidad de todos los involucrados.

Esta investigación se centrará específicamente en la Corte Superior de Justicia de Piura, Perú. A través de un análisis en profundidad de los casos de ciberdelitos en esta jurisdicción, se espera establecer un precedente legal importante y proporcionar una guía útil para futuros casos, contribuyendo así a la evolución del marco legal peruano para enfrentar la ciberdelincuencia.

Por último, esta tesis también será de importancia para las instituciones financieras. Al ser uno de los principales objetivos de los ciberdelincuentes, las entidades financieras se ven a menudo afectadas por estas actividades criminales. La presente investigación brindará un análisis legal exhaustivo sobre la responsabilidad de las entidades financieras en los delitos informáticos. De esta manera, se espera que este estudio pueda ayudar a las instituciones financieras a entender y mejorar sus medidas de seguridad y responsabilidad, proporcionando un entorno más seguro para sus clientes y contribuyendo a la lucha global contra la ciberdelincuencia.

El objetivo general de esta tesis es: determinar cómo favorece la modificación del código penal frente a la responsabilidad de terceros involucrados en delitos informáticos en las instituciones financieras realizados en la corte superior de Piura en el periodo 2022.

Los objetivos específicos de esta tesis incluyen: (1) describir el alcance de los delitos informáticos en Perú; (2) analizar casos de delitos informáticos en los que las instituciones financieras son terceros; (3) evaluar la eficacia de la legislación existente para prevenir y castigar estos delitos; y (4) proporcionar recomendaciones para fortalecer la legislación y las medidas de seguridad en torno a los ciberdelitos y la responsabilidad civil de los terceros.

Dado el enfoque de nuestro estudio, planteamos la hipótesis de que la legislación penal vigente en Perú no proporciona una protección adecuada contra los delitos informáticos y no aborda de manera eficaz la responsabilidad de los terceros en estos delitos. Esta hipótesis será examinada y probada a lo largo de nuestra investigación.

La contribución potencial de esta investigación es de gran alcance. Primero, puede ayudar a cerrar la brecha de conocimiento sobre los delitos informáticos en Perú, proporcionando una descripción más detallada y precisa del problema. Segundo, puede proporcionar recomendaciones útiles para los legisladores, las autoridades de aplicación de la ley y las instituciones financieras sobre cómo pueden fortalecer sus medidas de seguridad y proteger mejor a los individuos y empresas contra los ciberdelitos. Finalmente, este estudio también puede ser útil para otros investigadores en el campo del derecho penal y civil, proporcionando una base sólida para futuras investigaciones.

Concluimos esta introducción reconociendo que, aunque los ciberdelitos presentan desafíos únicos y formidables, también ofrecen una oportunidad. Una oportunidad para mejorar nuestras leyes, para fortalecer nuestras medidas de seguridad y para demostrar que, incluso en la cara de amenazas emergentes y en constante cambio, la ley debe adaptarse y seguir siendo una poderosa herramienta para la protección de los ciudadanos y mejor aplicación de la justicia.

II. MARCO TEÓRICO

II.1 Definiciones y conceptos clave

II.1.1 Delitos Informáticos: Definición del ciberdelito y relaciones diversas

Los ciberdelitos, también conocidos como delitos informáticos, se definen como cualquier acto ilegal o no ético que implica el uso de una computadora o una red informática[1]. Aunque las formas específicas de ciberdelito han evolucionado con el tiempo, esta definición general abarca una amplia gama de actividades, desde el robo de identidad y el fraude hasta el acoso en línea y los ataques cibernéticos.

La relación entre el ciberdelito y la ciberseguridad es intrínseca. La ciberseguridad se refiere a las medidas adoptadas para proteger las computadoras y las redes contra los ciberdelitos, incluyendo tanto las medidas técnicas (como firewalls y software antivirus) como las legales y regulatorias[2]. A medida que los ciberdelitos se han vuelto más sofisticados, también lo ha hecho la ciberseguridad, con un enfoque cada vez mayor en la prevención de ataques y la minimización del daño cuando ocurren.

La implementación de la ciberseguridad es una responsabilidad compartida entre varias entidades. La naturaleza compleja del ciberespacio y la amenaza omnipresente del ciberdelito requieren una respuesta multifacética que involucre a múltiples partes interesadas, cada una con un papel crucial a desempeñar.

- **Gobiernos**: Los gobiernos nacionales son responsables de establecer leyes y regulaciones que disuadan y castiguen el ciberdelito. También

[1] Broadhurst, R., et al. (2014). Organizations and Cyber crime: An Analysis of the Nature of Groups engaged in Cyber Crime. International Journal of Cyber Criminology, 8(1).

[2] Shackelford, S. (2013). Managing Cyber Threats: A Primer on Legal Issues and Cyber Security. Business Horizons, 56(5).

deben invertir en infraestructuras de ciberseguridad, formar fuerzas de seguridad cibernética y promover la cooperación internacional en la lucha contra los ciberdelitos. Además, pueden desempeñar un papel en la educación del público sobre los riesgos del ciberdelito y las mejores prácticas de ciberseguridad.

- **Organizaciones Privadas:** Las empresas y otras organizaciones privadas también tienen una gran responsabilidad en la implementación de la ciberseguridad. Esto incluye proteger sus propios sistemas y redes, asegurando los datos personales de los clientes y empleados, y proporcionando formación sobre ciberseguridad a su personal. Las empresas de tecnología y ciberseguridad tienen un papel aún mayor, ya que desarrollan las herramientas y tecnologías que se utilizan para protegerse contra los ciberdelitos.

- **Individuos:** Los usuarios individuales de Internet también tienen una responsabilidad personal en la ciberseguridad. Esto incluye seguir las mejores prácticas de ciberseguridad, como el uso de contraseñas fuertes, la actualización regular de software y sistemas, y el cuidado al compartir información personal en línea.

- **Organizaciones Internacionales y Grupos de Interés:** Organizaciones como la Unión Internacional de Telecomunicaciones, la Organización para la Cooperación y el Desarrollo Económicos y la Unión Europea tienen roles importantes en la promoción de la cooperación internacional en ciberseguridad, la creación de estándares internacionales y la facilitación de la compartición de información.

La ciberseguridad es una responsabilidad compartida que requiere la cooperación y el esfuerzo coordinado de todas las partes interesadas para ser eficaz.

II.1.2 Delitos informáticos: Tipología

La evolución de los ciberdelitos ha estado impulsada por varios factores, incluyendo el rápido avance de la tecnología, el crecimiento de Internet y la digitalización de muchos aspectos de nuestras vidas[3]. El primer ciberdelito registrado ocurrió en 1971, cuando un programador creó el primer virus de computadora como una broma. Desde entonces, los ciberdelitos han evolucionado para incluir fraudes en línea, robo de datos, Ransomware, y muchas otras formas de actividad delictiva.

Hay una variedad de ciberdelitos que pueden ocurrir, y estos a menudo se están desarrollando y cambiando a medida que la tecnología y las tácticas de los ciberdelincuentes evolucionan. Aquí hay algunos de los tipos más comunes de ciberdelitos:

- **Phishing:** Este es un intento de obtener información sensible como nombres de usuario, contraseñas y detalles de tarjetas de crédito, a menudo disfrazado de una comunicación confiable, a veces clonando la página de un banco, entidad financiera, caja, o la empresa objetivo, de esa manera, el usuario cae victima ingresando la información que es sensible.

- **Ransomware:** Es un tipo de malware que amenaza con publicar los datos del usuario o bloquear permanentemente el acceso a ellos a menos que se pague un rescate.

- **Spoofing:** Este ciberdelito implica la falsificación del origen de las comunicaciones para hacerlas parecer que provienen de una fuente confiable.

[3] Furnell, S. (2002). Cybercrime: Vandalizing the Information Society. Addison-Wesley.

- **Man-in-the-Middle (MitM) Attack:** Este tipo de ataque implica que un ciberdelincuente se interpone entre la comunicación de dos partes para interceptar y, posiblemente, alterar la comunicación.

- **DDoS Attack (Distributed Denial of Service):** Este tipo de ataque intenta hacer que un recurso en línea esté temporalmente o indefinidamente no disponible inundándolo con tráfico de múltiples fuentes.

- **SQL Injection:** Es un tipo de ataque que explota una vulnerabilidad en la base de datos de un sitio web para interferir con las consultas de la base de datos.

- **Cross-Site Scripting (XSS):** En este tipo de ataque, un ciberdelincuente inserta código malicioso en un sitio web que luego se ejecuta en el navegador del usuario.

- **Eavesdropping Attack:** En este ataque, el ciberdelincuente intercepta las comunicaciones entre dos partes para robar información.

- **Malware:** Software malicioso que puede causar daño o interrupción a los sistemas o redes.

- **Identity Theft:** Este ciberdelito implica robar la identidad de una persona para cometer fraude.

Estos son solo algunos ejemplos, y hay muchos otros tipos de ciberdelitos que pueden ocurrir.

II.1.3 Responsabilidad de terceros: Concepto legal y aplicación

La responsabilidad civil de terceros es un concepto que implica la responsabilidad de un individuo o entidad que no participó directamente en un acto delictivo pero que de alguna manera contribuyó a su comisión o no tomó medidas adecuadas

para prevenirlo. En el contexto de los ciberdelitos, esta responsabilidad puede recaer en proveedores de servicios de Internet, plataformas de redes sociales, instituciones financieras, entre otros, dependiendo del tipo de delito y las circunstancias específicas.

En muchos casos, se ha sostenido que los terceros, como los proveedores de servicios de Internet y las plataformas de redes sociales, tienen un cierto nivel de responsabilidad en la prevención de los ciberdelitos. Por ejemplo, pueden ser responsables de no tomar medidas para prevenir la propagación de software malicioso o contenido ilegal, o de no cooperar con las autoridades en la investigación de delitos.

II.1.4 Entidades financieras: Descripción y relevancia

II.1.4.1 Descripción de las entidades financieras:

Las entidades financieras son organizaciones que se encargan de la gestión, administración, intercambio y conservación de capital y deudas entre individuos, empresas y estados. Esta descripción engloba a una diversidad de entidades que, aunque comparten la finalidad de facilitar transacciones y actividades económicas, poseen características y funciones distintivas. En este espectro se encuentran los bancos comerciales, las cooperativas de crédito, las casas de bolsa, las compañías de seguros, las sociedades de inversión y las compañías de tarjetas de crédito, entre otras.[4]

El funcionamiento de estas entidades se basa en la confianza depositada por los usuarios en que su dinero y datos serán manejados de manera segura y eficiente. Esta confianza se traduce en el compromiso que tienen estas organizaciones de garantizar la protección de la información sensible y de

[4] Campbell, K., Gordon, L. A., Loeb, M. P., & Zhou, L. (2003). The economic cost of publicly announced information security breaches: empirical evidence from the stock market. Journal of Computer Security, 11(3), 431-448.

asegurar que las transacciones se realicen en un marco de seguridad. En este contexto, es de suma importancia que estas entidades tomen todas las medidas necesarias para salvaguardar su infraestructura y sistemas de cualquier intento de incursión o ataque malintencionado.[5]

Esta confianza se ha venido devaluando conforme el pasar del tiempo, y unos de los factores preponderantes para esa desconfianza cada vez más creciente, ha sido la poca o casi nula respuesta que tienen la mayoría de las entidades financieras frente a los ciberdelitos, y en muchos casos incluso hasta se han manifestado de una manera casi acorde con el criminal o hacker informático, casi como si fueran cómplices del crimen, antes que brindar un mecanismo de seguridad y de confianza al cliente y usuarios, tema que es materia de esta investigación y que se verán en puntos posteriores.

II.1.4.2 Relevancia en el estudio de los delitos informáticos:

Las entidades financieras, debido a la naturaleza de sus operaciones y la cantidad de datos e información que gestionan, son un objetivo principal para los ciberdelincuentes. La comisión de delitos informáticos en este sector puede tener graves repercusiones, no solo en términos de pérdida financiera directa, sino también en lo que respecta a la confianza del consumidor y la integridad del sistema financiero en general.

Los delitos informáticos pueden adoptar muchas formas en este contexto, desde fraudes de tarjetas de crédito y robo de identidad hasta ataques de phishing y Ransomware. Estos delitos pueden ser realizados por individuos, grupos de delincuentes o incluso estados-nación, lo que añade otra capa de complejidad al problema.[6]

---

[5] Alazab, M., Khresiat, A., Alazab, M., & Venkatraman, S. (2020). Cybercrime in the banking sector. Journal of Financial Crime.

[6] Anderson, R., Barton, C., Böhme, R., Clayton, R., Van Eeten, M. J., Levi, M., ... & Savage, S. (2013). Measuring the cost of cybercrime. In The economics of information security and privacy (pp. 265-300). Springer, Berlin, Heidelberg.

Además, el advenimiento de tecnologías emergentes, como las criptomonedas, ha proporcionado a los delincuentes nuevos medios para llevar a cabo sus actividades, aumentando la necesidad de una legislación adecuada y actualizada.

En este sentido, el estudio de la relación entre las entidades financieras y los delitos informáticos es fundamental para entender y abordar este desafío de la era digital. A través de este estudio, podemos obtener una visión más completa de las tácticas y estrategias utilizadas por los ciberdelincuentes, lo que puede ayudar a las entidades financieras y a los responsables de formular políticas a desarrollar medidas más efectivas de prevención y respuesta.[7]

En resumen, las entidades financieras juegan un papel crucial en el panorama actual de la ciberseguridad. Su relevancia en el estudio de los delitos informáticos radica en su papel como principal objetivo de estos delitos y en su responsabilidad de proteger a los consumidores y mantener la integridad del sistema financiero. Esta investigación, por lo tanto, se centrará en entender esta dinámica y en proponer recomendaciones para la mejora de la legislación actual en relación a la responsabilidad de terceros en este contexto.

II.2 Legislación sobre delitos informáticos

II.2.1 Legislación Comparada

Los ciberdelitos, o delitos informáticos, han surgido como un desafío importante en la era de la digitalización. Estos delitos, que van desde el robo de datos hasta el acoso cibernético y el fraude electrónico, pueden causar daño considerable tanto a los individuos como a las organizaciones. A medida que la tecnología sigue avanzando a un ritmo rápido, las legislaciones de todo el mundo luchan por

[7] Vécsey, B. (2020). Cyber-Attacks against Financial Institutions. In Managing Cyber Risk (pp. 111-129). Springer, Cham.

mantenerse al día con las nuevas formas de actividad criminal. La variedad de enfoques a nivel internacional destaca la dificultad inherente a este esfuerzo.

Por ejemplo, en Estados Unidos, el CFAA (Computer Fraud and Abuse Act) es la principal ley federal que se usa para combatir los ciberdelitos. Este acto, que fue promulgado en 1986, se centra en proteger la información clasificada y los sistemas de computadoras financieras y gubernamentales contra el acceso no autorizado[8]. Sin embargo, el CFAA ha sido objeto de críticas por su falta de claridad y por estar desactualizado en comparación con la rápida evolución de la tecnología.

Por otro lado, en el Reino Unido, la Ley de Uso Indebido de Computadoras de 1990 es la principal legislación que cubre los ciberdelitos. La ley, que fue enmendada en 2015 para incluir delitos relacionados con la ciberseguridad, cubre una gama de delitos, incluyendo el acceso no autorizado a sistemas informáticos y la interrupción de los mismos (McGuire, 2012).

Un caso notable de ciberdelito fue el ataque a Sony Pictures en 2014. Este ataque, que fue atribuido a Corea del Norte por el FBI, resultó en la filtración de datos personales y corporativos y causó interrupciones significativas en las operaciones de Sony. El caso subrayó la necesidad de una mejor protección contra los ciberdelitos y la importancia de la cooperación internacional para perseguir a los perpetradores[9].

Otro ejemplo es el caso del Ransomware WannaCry en 2017, que afectó a organizaciones en más de 150 países, incluyendo el Servicio Nacional de Salud del Reino Unido. Este ataque puso de manifiesto la vulnerabilidad de las infraestructuras críticas a los ciberdelitos y condujo a llamados para una mayor inversión en ciberseguridad (Lemieux et al., 2018).

---

[8] Lemieux, F., Brissette, S., & Caron, P. A. (2018). Cybersecurity and cyberthreats in the post-WannaCry era. Information & Security, 40(1),

[9] Brenner, S. W. (2015). Cyberthreats: The emerging fault lines of the nation state. Oxford University Press.

Aunque las legislaciones varían, hay un reconocimiento común de la necesidad de adaptarse y responder a estas amenazas emergentes. Los casos de Sony Pictures y WannaCry demuestran la escala y el impacto potencial de los ciberdelitos y la necesidad de una acción decidida y una cooperación internacional eficaz para combatirlos.

En el contexto internacional, los ciberdelitos están legislados de manera distinta dependiendo de cada país. Aquí hay una mirada a cómo algunos países han abordado estos problemas:

- Estados Unidos: El Computer Fraud and Abuse Act (CFAA), es la principal ley que trata los ciberdelitos. Fue promulgada en 1986 y está codificada en 18 U.S.C. § 1030. Esta ley prohíbe el acceso no autorizado a computadoras y redes, y ha sido modificada varias veces para adaptarse a las crecientes preocupaciones de ciberseguridad (Schwartz, P., & Janger, E. J. (2007). "Notification of Data Security Breaches". Michigan Law Review, 105(5), 913-984).

- Unión Europea: La Directiva 2013/40/EU del Parlamento Europeo trata los ataques a sistemas de información, reemplazando a la Decisión Marco 2005/222/JAI. Esta directiva proporciona definiciones para delitos informáticos como acceso ilegal, interferencia ilegal e interceptación ilegal. También se refiere a la creación y distribución de herramientas de hacking.

- Reino Unido: El Computer Misuse Act 1990 es la legislación clave aquí, que fue modificada por el Serious Crime Act 2015 para incluir disposiciones relacionadas con la ciberseguridad. Está codificado en las leyes del Reino Unido como Capítulo 18 (McGuire, M. R. (2012). "Technology crime waves". Crime, Law and Social Change, 57(2), 109-130).

- Australia: El Cybercrime Act 2001 es la legislación clave en Australia que se refiere a los delitos informáticos. Fue diseñado para implementar las disposiciones del Convenio de Cibercrimen del Consejo de Europa.

- India: La Ley de Tecnología de la Información de 2000 (IT Act 2000), es la principal legislación que se ocupa de los delitos cibernéticos y el comercio electrónico en India.

Estas leyes demuestran la variedad de formas en que diferentes naciones han legislado contra los ciberdelitos. Sin embargo, dada la naturaleza transfronteriza de muchos ciberdelitos, la cooperación internacional sigue siendo un componente crucial para su prevención y persecución

II.2.2 Legislación peruana vigente

La naturaleza y el impacto de los ciberdelitos pueden variar significativamente en diferentes contextos. En países con una infraestructura de TI fuerte y leyes sólidas sobre ciberdelitos, los individuos y las empresas pueden estar mejor protegidos contra estos delitos[10]. Sin embargo, en países con infraestructuras de TI más débiles o con leyes menos desarrolladas sobre ciberdelitos (como por ejemplo en PERU y la mayoría de países de Latinoamérica), estos pueden ser más comunes y sus efectos más devastadores.

A medida que los ciberdelitos continúan evolucionando, también lo hacen los esfuerzos para combatirlos. Las leyes y regulaciones se están actualizando para mantenerse al día con las nuevas formas de ciberdelito, y las tecnologías de ciberseguridad se están desarrollando constantemente para prevenir y mitigar estos delitos. Sin embargo, el desafío persiste, y el equilibrio entre la protección

[10] Brenner, S. (2004). Cybercrime Metrics: ¿Old Wine, New Bottles? Virginia Journal of Law & Technology, 9.

contra los ciberdelitos y la preservación de las libertades civiles sigue siendo un tema de debate[11].

A pesar de los esfuerzos concertados para mitigar los ciberdelitos, la realidad es que estos delitos se están volviendo cada vez más frecuentes y sofisticados. Según un informe de 2020 de la Interpol, los ciberdelitos han aumentado en volumen y gravedad desde el inicio de la pandemia de COVID-19, con un aumento significativo en los ataques de Ransomware y el phishing[12]. Además, la Organización para la Cooperación y el Desarrollo Económicos (OCDE) advierte que el costo global de los ciberdelitos podría alcanzar los $6 billones de dólares para 2021, lo que subraya la necesidad de soluciones efectivas de ciberseguridad y legislación actualizada[13].

Los ciberdelitos también pueden variar significativamente en función del contexto nacional y cultural. Por ejemplo, en los Estados Unidos, la Ley de Fraude y Abuso Informático de 1986 es a menudo la principal herramienta legal utilizada para procesar los ciberdelitos, mientras que, en la Unión Europea, la Directiva sobre ataques a sistemas de información proporciona una base para la cooperación transfronteriza en la lucha contra los ciberdelitos[14].

II.2.2.1 Código Penal

En el contexto peruano, existen varios artículos dentro del Código Penal que están relacionados con los ciberdelitos, dando diferentes interpretaciones como tal, pero sin dar un tratamiento completo a una figura penal de delito dentro de este ámbito. Estos artículos, se encuentran en el

[11] Casey, E. (2010). Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. Academic Press.

[12] Interpol (2020). Cybercrime: Threats and responses during the COVID-19 pandemic. Interpol Report.

[13] OECD (2020). Cybersecurity in the Digital Economy. OECD Digital Economy Papers, No. 280.

[14] Council of Europe (2013). Directive 2013/40/EU on attacks against information systems. Official Journal of the European Union.

Libro Segundo, Título IX, Capítulo II, que trata sobre Delitos Contra la Fe Pública y en particular los Delitos Informáticos.

- Artículo 207-A: Define el delito de acceso ilícito a un sistema de tratamiento de información, que consiste en acceder, usar, copiar, alterar, dañar o interferir un sistema de tratamiento de información o los datos contenidos en dicho sistema sin autorización o excediendo la que se tiene.

- Artículo 207-B: Se refiere a la interceptación ilegal de las comunicaciones y transmisiones de datos, que implica la utilización de técnicas de transmisión de datos y telecomunicaciones para cometer infracciones.

- Artículo 207-C: Trata sobre el uso ilegal de dispositivos y programas informáticos, y se refiere a la fabricación, importación, distribución, venta o puesta a disposición de dispositivos o programas informáticos diseñados o adaptados para cometer delitos informáticos.

- Artículo 207-D: Trata sobre el fraude informático, y se refiere a la manipulación de sistemas informáticos o de datos con el fin de obtener un beneficio injusto.

- Artículo 207-E: Habla sobre la falsificación informática, y se refiere a la introducción, alteración o borrado de datos informáticos o funciones informáticas con la intención de que sean considerados o tenidos en cuenta como datos o funciones auténticos.

- Artículo 207-F: Trata sobre la pornografía infantil por medios informáticos, y se refiere a la utilización de tecnología informática para la producción, posesión o distribución de pornografía infantil.

Estos son solo algunos ejemplos de los delitos informáticos que se describen en el Código Penal de Perú. Sin embargo, dado que la legislación puede cambiar, es importante consultar la versión más actualizada del Código Penal o consultar a un experto legal para obtener información precisa y actualizada.

II.2.2.2 Ley Nª 30096 - Ley de delitos informáticos

La Ley N.º 30096, también conocida como la Ley de Delitos Informáticos de Perú, fue promulgada en el año 2013 y representa un marco legal significativo para enfrentar la amenaza emergente de los delitos cibernéticos. Esta ley busca llenar un vacío legal en Perú en relación a las cuestiones de ciberseguridad y establecer sanciones para aquellos que cometan delitos informáticos.

La ley consta de varios artículos relevantes para nuestra discusión sobre la responsabilidad de terceros en delitos informáticos en el sector financiero. El Artículo 1 de la Ley establece su propósito principal, que es prevenir y sancionar los delitos cometidos a través de sistemas informáticos y redes de información, mientras que el Artículo 2 menciona los tipos de delitos informáticos que se penalizan, incluyendo el acceso ilegal a sistemas informáticos, interceptación ilegal de datos informáticos, ataque a la integridad de datos y sistemas informáticos, entre otros.

Uno de los aspectos más relevantes de la Ley en relación a nuestra tesis es la atención que presta a la responsabilidad de terceros. El Artículo 6, por ejemplo, penaliza la producción, venta, distribución, importación, puesta a disposición, adquisición y posesión de dispositivos y programas informáticos destinados a cometer delitos, así como la facilitación de medios que permiten su comisión. Esto puede interpretarse como una forma de responsabilidad de terceros, pues sanciona a aquellos que, si bien no cometen el acto ilegal directamente, sí contribuyen de manera significativa a su ejecución.

Además, el Artículo 8 sanciona la utilización de datos personales sin consentimiento, un delito que puede involucrar la responsabilidad de terceros cuando se considera que muchas entidades financieras manejan grandes volúmenes de datos personales de sus clientes.

El Artículo 10 también es de interés, ya que sanciona la transferencia o envío no consentido de datos personales con la finalidad de obtener un beneficio económico. Esto es especialmente relevante en el contexto financiero, ya que los datos de los clientes a menudo son un objetivo principal de los delincuentes cibernéticos.

La Ley N.º 30096 representa un paso significativo en el combate contra la ciberdelincuencia en Perú. Sin embargo, como toda ley, no está exenta de críticas y sugerencias de reforma, especialmente en relación a la claridad de sus disposiciones y la eficacia de su implementación.

En el contexto de nuestra tesis, la Ley ofrece una base importante para la discusión sobre la responsabilidad de terceros en delitos informáticos. Sin embargo, queda claro que aún hay margen para aclarar y expandir las disposiciones legales en este sentido. En particular, se podría considerar la inclusión explícita de disposiciones que traten la responsabilidad de las entidades financieras ante los delitos informáticos cometidos en o a través de sus plataformas.

En conclusión, la Ley de Delitos Informáticos es un pilar fundamental en el marco legal de Perú para abordar la ciberdelincuencia. Sin embargo, hay espacio para evolución y adaptación, particularmente en lo que respecta a la clarificación y expansión de la responsabilidad de terceros en el contexto de los delitos informáticos, lo cual es el núcleo de esta investigación.

II.2.2.3 Otras normas / leyes relacionados

La legislación peruana relacionada con los ciberdelitos es un tema en constante evolución. El Perú ha hecho esfuerzos significativos para desarrollar leyes que aborden este desafío emergente. A continuación, se mencionan algunas de las disposiciones más relevantes en este contexto.

- Ley N° 29733, Ley de Protección de Datos Personales: Esta ley protege la información personal de los individuos y establece las obligaciones de las empresas e instituciones en cuanto a la recolección y protección de datos personales. Esta ley también es relevante en el contexto de los ciberdelitos, ya que protege contra el acceso y uso no autorizado de datos personales.

- Decreto Legislativo N° 1182: Conocido como la Ley de Geolocalización, esta ley permite a las autoridades realizar la geolocalización de equipos móviles o terminales de telecomunicaciones en casos de delitos graves, incluyendo los ciberdelitos.

Un caso emblemático de ciberdelito en Perú es el de la "Operación Olimpo", en la que la Policía Nacional del Perú capturó a una red de delincuentes que cometía fraude informático y robo de datos a través de internet, y que había estafado a miles de peruanos. Este caso destaca la importancia de la cooperación entre las fuerzas del orden, las instituciones financieras y las autoridades reguladoras para combatir eficazmente los ciberdelitos. Sin embargo, en la parte procesal fueron únicamente imputados como robo ante una falta clara de aplicación de Derecho Penal frente a este problema, y no hubo mayor impacto de cambio en las instituciones financieras involucradas.

Sin embargo, a pesar de estos avances, todavía existe un debate significativo sobre la necesidad de mejorar y actualizar estas leyes para

adaptarse a los desafíos cambiantes y en constante evolución de los ciberdelitos[15].

II.2.3 Responsabilidad de terceros en nuestra legislación

En Perú, el marco legal en torno a la responsabilidad de terceros en los delitos informáticos todavía está en proceso de desarrollo. Sin embargo, hay una clara necesidad de abordar este problema, ya que los ataques cibernéticos y los delitos informáticos se han vuelto cada vez más comunes y sofisticados.

Para enriquecer este punto, se puede hacer referencia al artículo "La responsabilidad de los proveedores de servicios de Internet en la Ley de Delitos Informáticos"[16], que analiza cómo la Ley de Delitos Informáticos peruana afecta a los proveedores de servicios de Internet. Según Barrientos, aunque la ley peruana establece ciertas responsabilidades para estos proveedores, como la obligación de colaborar con las autoridades en la investigación de delitos informáticos, todavía existe un vacío legal en cuanto a su responsabilidad civil por los daños causados por estos delitos.

Además, el libro "Delitos informáticos y su regulación en la legislación peruana"[17], también proporciona una discusión útil sobre la responsabilidad de terceros en los delitos informáticos. Según Vigo, aunque la legislación peruana no define claramente la responsabilidad civil de terceros en los delitos informáticos, se

---

[15] Código Penal del Perú. (2004). Decreto Legislativo N° 635.

Ley de Protección de Datos Personales. (2011). Ley N° 29733.

Ley de Geolocalización. (2015). Decreto Legislativo N° 1182.

Rodríguez Ferrucci, A. (2018). Los ciberdelitos y su regulación en el Perú. Revista Jurídica del Perú, (75), 271-281.

[16] Barrientos, J. (2015). La responsabilidad de los proveedores de servicios de Internet en la Ley de Delitos Informáticos. Revista de la Facultad de Derecho y Ciencias Políticas, 77(154), 1-15.

[17] Vigo, M. (2017). Delitos informáticos y su regulación en la legislación peruana. Editorial PUCP.

puede interpretar que los terceros que facilitan de alguna manera la comisión de un delito informático podrían ser considerados responsables.

Es importante destacar que, aunque la responsabilidad de terceros en los delitos informáticos no está claramente definida en la legislación peruana, esto no significa que las instituciones financieras estén exentas de responsabilidad. De hecho, estas instituciones tienen un deber legal y ético de implementar medidas adecuadas de seguridad para proteger a sus clientes y sus datos. En este sentido, una posible reforma del Código Penal podría contemplar la incorporación de disposiciones específicas sobre la responsabilidad de terceros en los delitos informáticos.

II.3 Casos de delitos informáticos en entidades financieras

II.3.1 Casuística internacional: análisis y repercusiones legales

En los últimos años, se han producido varios casos importantes de delitos informáticos en entidades financieras a nivel internacional. Uno de los más notorios fue el ataque al banco estadounidense JPMorgan Chase en 2014, que resultó en la filtración de información personal y financiera de más de 76 millones de hogares y 7 millones de pequeñas empresas[18]. Este incidente, que se considera uno de los más grandes de su tipo, ha resaltado la creciente amenaza de los delitos informáticos para las instituciones financieras y ha llevado a la demanda de mayores medidas de seguridad y responsabilidad en el sector.

Además de los casos de alto perfil como el de JPMorgan Chase, también ha habido una serie de otros incidentes importantes que han afectado a las entidades financieras en todo el mundo. Por ejemplo, en 2016, el Banco Central de Bangladesh fue víctima de un ciberataque que resultó en la pérdida de $81

[18] Menn, J. (2015). Exclusive: FBI warns of 'destructive' malware in wake of Sony attack. Reuters. Retrieved from https://www.reuters.com/.

millones de dólares[19]. Este caso destacó la importancia de las medidas de seguridad adecuadas, no sólo en las instituciones financieras individuales, sino también en los sistemas interbancarios y de pago internacionales.

Estos casos internacionales de delitos informáticos han tenido importantes repercusiones legales. En muchos países, han llevado a la implementación de leyes más estrictas y regulaciones en torno a la seguridad cibernética en el sector financiero, y han puesto de manifiesto la necesidad de una mayor cooperación internacional en la lucha contra los delitos informáticos.

II.3.2 Casuística nacional: análisis y repercusiones legales

En el contexto peruano, también ha habido varios casos importantes de delitos informáticos en entidades financieras. En 2018, se informó de un caso en el que hackers lograron robar más de 3 millones de soles de cuentas bancarias en Perú a través de transferencias fraudulentas[20]. Este caso ha puesto de manifiesto la creciente amenaza de los delitos informáticos en el sector financiero del país y ha llevado a las autoridades a tomar medidas para fortalecer la seguridad cibernética en las instituciones financieras.

Estos casos han tenido importantes repercusiones legales en Perú. Han llevado a las autoridades a reconocer la creciente amenaza de los delitos informáticos y a buscar maneras de fortalecer la legislación existente en esta área. Sin embargo, a pesar de estos esfuerzos, sigue habiendo una necesidad de reformas legales más amplias para garantizar que las entidades financieras estén adecuadamente protegidas contra los delitos informáticos y que las víctimas de estos delitos reciban la justicia adecuada.

---

[19] Ward, M. (2016). Bangladesh Bank exposed to hackers by cheap switches, no firewall: Police. Reuters. Retrieved from https://www.reuters.com/.

[20] BBC News. (2018). Detienen a "hackers" que robaron más de US$1 millón a bancos en Perú. BBC News Mundo. Retrieved from https://www.bbc.com/.

II.3.3 Implicación de terceros en estos casos: responsabilidad y consecuencias legales

La implicación de terceros en delitos informáticos en entidades financieras es un aspecto crucial en la comprensión y prevención de este tipo de delitos. Los terceros pueden ser entidades o individuos que proporcionan la infraestructura tecnológica, plataformas de software y hardware, o servicios que se utilizan para perpetrar el delito informático. La participación de estos terceros puede ser activa, a través de la complicidad en el delito, o pasiva, por no implementar medidas de seguridad adecuadas o ser negligentes en su responsabilidad de proteger a sus usuarios o clientes.

En términos legales, la responsabilidad de terceros en delitos informáticos puede ser compleja. A nivel internacional, existen diferencias significativas en cómo se considera y se aplica la responsabilidad de terceros. En algunos casos, los tribunales han fallado que los proveedores de servicios de Internet (ISP) y otras entidades tecnológicas pueden ser responsables por los delitos cometidos a través de sus servicios, si se demuestra que no han tomado medidas adecuadas para prevenir dichos delitos. Un ejemplo de esto es el caso de la empresa de alojamiento web Roommate.com en los Estados Unidos, que fue considerada legalmente responsable de violar las leyes de igualdad de vivienda al permitir y facilitar la discriminación en su plataforma[21].

En el caso de las instituciones financieras, estas pueden ser responsables si no implementan medidas adecuadas de seguridad cibernética para proteger a sus clientes contra el fraude en línea o el robo de datos. Por ejemplo, la empresa de tarjetas de crédito Target fue demandada por no proteger adecuadamente los datos de sus clientes, lo que resultó en un gran robo de datos[22].

[21] Roommate.com, LLC v. Fair Housing Council of San Fernando Valley, 521 F.3d 1157 (9th Cir. 2008).

[22] In re: Target Corporation Customer Data Security Breach Litigation, MDL No. 14-2522 (D. Minn. 2014).

En el contexto peruano, aunque la responsabilidad civil de terceros en los ciberdelitos no está claramente definida en la legislación, hay un precedente en la jurisprudencia que establece que los proveedores de servicios de Internet pueden ser responsables de los daños causados por los delitos cometidos a través de su servicio. Esto se basa en el principio general de responsabilidad civil establecido en el Código Civil peruano. Sin embargo, la responsabilidad penal de los terceros aún no está claramente definida en la legislación peruana[23].

La implicación de la responsabilidad de terceros en delitos informáticos tiene consecuencias legales importantes, ya que afecta quién puede ser llevado a juicio y condenado por estos delitos. Además, tiene un impacto en la prevención de delitos, ya que, si los terceros saben que pueden ser responsables, pueden ser más proactivos en implementar medidas de seguridad y colaborar con las autoridades en la prevención e investigación de delitos.

La responsabilidad de terceros en delitos informáticos es un área en evolución del derecho que presenta muchos desafíos y preguntas sin respuesta. La adaptación de la legislación y la jurisprudencia a los desafíos presentados por la ciberdelincuencia es un proceso en curso, y la responsabilidad de terceros seguramente seguirá siendo un tema de debate y discusión en los próximos años.

II.4 Contextualización y Casuísticas en Entidades Financieras de Piura

La región de Piura, situada en el norte de Perú, se distingue por su dinamismo económico y su relevancia en el sector financiero. Esta área no solo sirve como un eje comercial y agrícola vital para el país, sino que también se ha convertido en un punto focal donde hay un alto crecimiento de servicios financieros, brindados por diferentes entidades financieras, desde banca

[23] Tribunal Constitucional de Perú. (2009). Caso Fortunato Príncipe Laura.

nacionales o internacionales como BCP, BBVA, INTERBANK, etc., hasta microfinancieras como las cajas (Caja Piura, Caja Sullana, Caja Paita – que son las más importantes que tiene PIURA) hasta empresas microfinancieras que algunas de ellas están fuera del alcance de la SBS (como ALBUSA), todo esto ha sido un punto de enfoque principal para el análisis de la ciberdelincuencia en el contexto financiero, dada su creciente incidencia en las últimas décadas. La presente sección explora la contextualización de los delitos informáticos en las entidades financieras de Piura, ofreciendo una mirada detallada a las casuísticas específicas que ilustran la complejidad y el impacto de esta problemática en la región.

Situación Actual en Piura

Piura, con su vibrante economía basada en la agricultura, la pesca y el comercio, alberga una red extensa de entidades financieras que van desde bancos hasta microfinancieras. Estas instituciones juegan un papel crucial en el desarrollo económico regional, facilitando el acceso al crédito y a otros servicios financieros esenciales. Sin embargo, la digitalización de servicios financieros, si bien ha traído numerosos beneficios, también ha expuesto a estas entidades a riesgos significativos relacionados con los delitos informáticos.

Incidencia de Delitos Informáticos

En los últimos años, Piura ha sido testigo de un aumento alarmante en la incidencia de delitos informáticos, afectando tanto a entidades financieras como a sus clientes, según las cifras del INEI, de los 625 000 delitos informáticos que se han realizado a nivel nacional hasta el 2022, el 30% se han realizado en Piura, de los cuales menos del 0.1% son denunciados o llegan a juicio. Dichos ataques van desde el phishing y el fraude en línea hasta ataques de Ransomware que no solo buscan el robo de información financiera, sino también la desestabilización de las operaciones financieras.

Esta tendencia refleja una urgente necesidad de abordar la seguridad cibernética como una prioridad estratégica dentro del sector financiero.

Casuísticas Relevantes

Una de las casuísticas más notorias en Piura fue el ataque a una conocida entidad bancaria, donde los ciberdelincuentes lograron infiltrarse en sus sistemas de seguridad, accediendo a información confidencial de miles de clientes. Este incidente, que culminó en la sustracción de significativas sumas de dinero de cuentas bancarias, no solo puso en evidencia las vulnerabilidades existentes, sino que también marcó un precedente en cuanto a la magnitud de las consecuencias que pueden acarrear estos ataques.

Otro caso destacado involucró a una microfinanciera local, la cual fue víctima de un ataque de ransomware. Los atacantes cifraron los datos críticos de la institución, exigiendo un rescate para su liberación. Este evento no solo paralizó temporalmente las operaciones de la entidad, sino que también sembró dudas sobre la seguridad de la información de los clientes.

En mi experiencia personal como ingeniero informático, he sido testigo de ataques de Ransomware (secuestro de archivos del servidor) a cerca de 20 empresas, entre ellas una caja y muchas otras empresas de diferente rubro comercial, y una de ellas, una empresa de exportación de uva, tuvo la decisión de pagar el “rescate” de dichos archivos, con un monto de más de 80 000 dólares, sin embargo nunca se realizó dicha liberación, ya que, se sabe en el mundo de la informática, que estos ciber delincuentes jamás cumplen con la liberación de los archivos encriptados, por el contrario solicitan siempre más dinero.

También he revisado casos de robo de cuentas corrientes y de ahorro en bancos, realizado por hackers, muchos de ellos realizados en el BBVA, pero también otros realizados en INTERBANK, BCP, BANCO DE COMERCIO, sin

embargo en estos últimos, el sistema de ciberseguridad que tienen implementado permitió que no se llegue a culminar con el robo, sino por el contrario el dinero o gran parte de él fue recuperado haciendo extornos y con denuncias al que cometió el delito, ya que cuenta con sistemas de trazabilidad (que todo sistema de ciberseguridad debe tener) sin embargo he observado que el BBVA no lo tiene implementado como debería ser, sino lo mínimo que le exige la SBS. No brindo más detalles porque la implementación del mecanismo de ciberseguridad sería para un estudio más grande, que escapa al alcance de esta tesis (*se sugiere un estudio de investigación sobre este tema*).

Y para completar, uno de los motivos que me llevó a realizar esta tesis, es una experiencia personal que se sucedió con el banco BBVA; y procedo a detallar: he sido víctima de un robo de parte de un hackers, que clono mi número celular, y obtuvo un token (clave) con el cual accedió a mis cuentas de ahorros, y procedió a realizar un robo del mismo, haciendo una transferencia a sus cuentas, lo que no contaba el hacker, era que teniendo conocimientos de seguridad de información, active varios protocolos que me avisaban de cualquier movimiento realizado en mis cuentas, y por ello, ni bien se realizó dicho movimiento de transferencia fui advertido por un correo electrónico, el problema está cuando reclame al BBVA para que anule dicha transacción, negándose a realizarlo justificando que dicha transacción se realizó con mi autorización, por lo que le solicite un haga un rastreo de la IP para que lo confirme, pero nunca lo realizaron, y esto es porque ellos no lo tienen implementado por lo que no cumplen con las normas de ciberseguridad internacionales, pero el problema radica que en el PERU no se obliga a esto, ya que la el código PENAL, no admite esto como un delito, ni siquiera como complicidad involuntaria, sino solamente como una falta civil administrativa, que es lo máximo que se tiene en el código CIVIL y en la SBS.

Actualmente estoy en juicio con el ciber delincuente, pero no se está procesando como un ciber delito, sino como un robo común, y se está también

juzgando por la vía civil al banco BBVA, por ser TERCEROS RESPONSABLES.

Análisis de los Desafíos

Estas casuísticas subrayan varios desafíos críticos enfrentados por las entidades financieras en Piura en el ámbito de la ciberseguridad. En primer lugar, la necesidad de inversiones constantes en tecnología de seguridad informática y en la capacitación del personal para detectar y responder a amenazas de manera eficaz. En segundo lugar, que el banco implemente correctamente un programa de ciberseguridad para evitar estos robos, y no se conviertan en cómplices de estos ciberdelitos, sino que sean la primera barrera de defensa para evitar que estos hackers puedan cometer estos delitos, por ello la importancia de la cooperación interinstitucional, tanto a nivel local como internacional, para combatir la ciberdelincuencia, que frecuentemente trasciende fronteras. Por último, el reto de mantener una cultura de seguridad entre los clientes, educándolos sobre prácticas seguras en el manejo de sus transacciones y datos personales en línea.

Propuestas de Mejora

Frente a estos desafíos, es imperativo que las entidades financieras de Piura adopten un enfoque holístico hacia la seguridad cibernética. Esto incluye la implementación de sistemas de seguridad de vanguardia, la realización de auditorías de seguridad periódicas y el fomento de una cultura organizacional que priorice la seguridad de la información. Además, es crucial el establecimiento de protocolos de respuesta ante incidentes que permitan una reacción rápida y coordinada ante posibles brechas de seguridad.

II.5 Brechas y desafíos en la legislación actual

II.5.1 Evolución de la ciberdelincuencia y la brecha legislativa

La ciberdelincuencia ha evolucionado considerablemente en las últimas décadas. A medida que la tecnología ha avanzado, también lo han hecho las formas en que los delincuentes pueden explotarla. Hemos visto el crecimiento de delitos como el robo de identidad en línea, el fraude financiero, el hacking y la propagación de malware, por nombrar solo algunos[24].

Sin embargo, la legislación a menudo ha luchado por mantenerse al día con estos desarrollos. Muchos países, incluido Perú, inicialmente no tenían leyes que abordaran específicamente los delitos informáticos, lo que a menudo dejaba a las autoridades luchando para procesar a los delincuentes bajo leyes que no estaban diseñadas para tratar este tipo de delitos[25].

Esto ha llevado a una brecha legislativa en muchos países, donde los delitos informáticos pueden no estar adecuadamente cubiertos por la ley. Esto puede hacer que sea difícil para las autoridades investigar y procesar estos delitos, y puede dejar a las víctimas sin recurso legal[26], y menos que las instituciones financieras tengan alguna responsabilidad ni legar ni administrativa ante el cometimiento de tales crímenes, convirtiéndose en cómplices del crecimiento de tales actitudes y evitar que siga creciendo su índice de cumplimiento criminal.

---

[24] Broadhurst, R., Grabosky, P., Alazab, M., Bouhours, B., & Chon, S. (2014). An analysis of the nature of groups engaged in cyber crime. In International Conference on Cyber Security for Sustainable Society. https://www.researchgate.net/publication/283824609_An_Analysis_of_the_Nature_of_Groups_Engaged_in_Cyber_Crime

[25] Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. Journal in Computer Virology, 2(1), 13-20.

[26] Wall, D. (2007). Cybercrime: The transformation of crime in the information age. Polity

II.5.2 Problemas específicos en la legislación peruana

Perú ha hecho esfuerzos para abordar los delitos informáticos en su legislación, con leyes como la Ley Nº 30096 de Delitos Informáticos. Sin embargo, existen desafíos y brechas específicas en la legislación peruana que pueden dificultar la eficacia de estas leyes.

Un problema clave es la falta de una definición clara y coherente de lo que constituye un delito informático. Esto puede dificultar la identificación y procesamiento de estos delitos. Además, las leyes peruanas pueden no abordar adecuadamente todas las formas de delitos informáticos, lo que deja a algunas víctimas sin recurso legal[27].

Otro problema es la falta de una disposición clara en la legislación peruana sobre la responsabilidad de terceros en los delitos informáticos. Esto puede hacer que sea difícil para las autoridades procesar a aquellos que proporcionan la infraestructura o los servicios utilizados para cometer delitos informáticos, incluso si no participaron directamente en el delito[28].

II.5.3 Desafíos en la asignación de responsabilidad a terceros en delitos informáticos

Asignar responsabilidad a terceros en delitos informáticos es un desafío significativo. Esto se debe a varias razones, incluyendo la naturaleza técnica y a menudo compleja de los delitos informáticos, la jurisdicción transnacional de la mayoría de los delitos informáticos y las limitaciones inherentes a las leyes existentes[29].

---

[27] Gómez-Sorzano, A. (2006). Cyber Crime and Cyber Terrorism: A Theoretical and Empirical Overview. The Icfai Journal of Cyber Law, 5(2), 8-31.

[28] Fernández, C. (2019). Delitos Informáticos en el Perú: Tipificación y Jurisprudencia. Legis.pe. https://legis.pe/delitos-informaticos-peru-tipificacion-jurisprudencia/

[29] Brenner, S. W. (2004). At light speed: Attribution and response to cybercrime/terrorism/warfare. Journal of Criminal Law and Criminology, 697-728

La asignación de responsabilidad a terceros en delitos informáticos también se ve dificultada por la dificultad de rastrear y localizar a los delincuentes. Muchos delincuentes informáticos utilizan tácticas como el enmascaramiento de IP y el uso de VPN para ocultar su ubicación y evitar la detección. En tales casos, incluso si se puede determinar que un tercero proporcionó los medios para que se cometa el delito, puede ser difícil identificar y procesar al delincuente.

En muchos casos, es difícil probar que un tercero conocía o debía haber sabido que su servicio o plataforma se estaba utilizando para cometer un delito. Además, muchos delitos informáticos son de naturaleza transnacional, lo que puede dificultar la jurisdicción y el procesamiento de los acusados.

Finalmente, las leyes existentes pueden no estar equipadas para abordar adecuadamente la responsabilidad de terceros en delitos informáticos. Muchas leyes se redactaron antes de la aparición de los delitos informáticos y pueden no abordar adecuadamente la naturaleza única de estos delitos y los desafíos asociados con la asignación de responsabilidad[30].

II.5.4 Entidades Clave en la Lucha contra Delitos Informáticos en el Sector Financiero: DIVINDAT y MININTER

La lucha contra los delitos informáticos en Perú involucra a varias entidades estatales, destacando principalmente la División de Investigación de Delitos de Alta Tecnología (DIVINDAT) de la Policía Nacional del Perú (PNP) y el Ministerio del Interior (MININTER). Estas instituciones juegan roles fundamentales en la prevención, detección y sanción de actividades criminales que comprometen la seguridad de las entidades financieras y la integridad económica del país.

[30] Reyns, B. W., Henson, B., & Fisher, B. S. (2011). Being pursued online: Applying cyberlifestyle–routine activities theory to cyberstalking victimization. Criminal Justice and Behavior, 38(11), 1149-1169. doi:10.1177/0093854811421448

División de Investigación de Delitos de Alta Tecnología (DIVINDAT): La DIVINDAT es una división especializada de la PNP encargada de la investigación de delitos informáticos y fraudes electrónicos. Su ámbito de actuación abarca una amplia gama de delitos cibernéticos, incluyendo ataques a sistemas informáticos de entidades financieras, fraude online, phishing, y la propagación de software malicioso con el fin de comprometer la seguridad financiera. La DIVINDAT opera mediante la implementación de tecnologías avanzadas para la investigación cibernética, el análisis forense digital y la ejecución de operaciones encubiertas en el ciberespacio para identificar y capturar a los responsables de estos crímenes.

Ministerio del Interior (MININTER): El MININTER, a través de sus diversas dependencias, incluida la PNP y la DIVINDAT, establece las políticas de seguridad interna del país y coordina esfuerzos para combatir el crimen organizado y los delitos informáticos. En el contexto de los ciberdelitos, el MININTER promueve la colaboración interinstitucional tanto a nivel nacional como internacional, facilitando el intercambio de información y buenas prácticas entre agencias de seguridad y entidades financieras. Asimismo, el MININTER es responsable de diseñar y promover legislación que fortalezca el marco legal para la persecución de delitos informáticos y la protección de la infraestructura crítica financiera.

Colaboración y Desafíos: La colaboración efectiva entre la DIVINDAT, el MININTER y las entidades financieras es esencial para establecer un entorno seguro y confiable para las transacciones financieras en el ciberespacio. Sin embargo, esta colaboración enfrenta desafíos, incluyendo la necesidad de constante actualización tecnológica, la capacitación especializada del personal en ciberseguridad, y la adaptación a las cambiantes tácticas empleadas por los ciberdelincuentes. Además, la legislación debe evolucionar para abordar nuevas formas de delitos informáticos, garantizando que las entidades encargadas de la seguridad cibernética tengan las herramientas legales necesarias para actuar de manera efectiva.

En conclusión, la DIVINDAT y el MININTER son pilares fundamentales en la protección del sector financiero contra los delitos informáticos en Perú. La actualización constante de estrategias, el fortalecimiento de la legislación y la mejora en la cooperación interinstitucional son esenciales para asegurar la efectividad de estas entidades en la lucha contra la ciberdelincuencia.

II.6 Necesidad y propuestas de reforma legislativa

II.6.1 Necesidad de actualizar la legislación actualizada

En el mundo digital en el que vivimos, los ciberdelitos son cada vez más frecuentes y sofisticados, y el derecho penal y civil en muchos países, incluido Perú, luchan por mantenerse al día con estos desarrollos. A medida que las tecnologías avanzan y las actividades en línea se vuelven cada vez más integradas en nuestras vidas cotidianas, las amenazas cibernéticas también evolucionan, lo que crea una brecha entre las amenazas existentes y la capacidad de la legislación para abordarlas adecuadamente.

La legislación actual en Perú, como el Código Penal y la Ley de Delitos Informáticos, proporciona cierto grado de protección contra los ciberdelitos, pero tiene limitaciones en términos de su alcance y la claridad de las disposiciones. Estas leyes se diseñaron en un momento en que las actividades en línea y las amenazas cibernéticas no eran tan omnipresentes ni complejas como lo son hoy. Como resultado, hay áreas grises y lagunas que pueden ser explotadas por delincuentes cibernéticos, o que pueden dificultar la persecución y sanción efectivas de los ciberdelitos[31].

Además, existen desafíos con respecto a la cooperación internacional en la lucha contra los ciberdelitos. Los ciberdelitos a menudo trascienden las fronteras nacionales, y la falta de armonización en las leyes y regulaciones de ciberdelitos

[31] Casey, E. (2011). Digital evidence and computer crime: Forensic science, computers and the Internet (3rd ed.). Academic Press.

a nivel internacional puede obstaculizar la cooperación entre países en la investigación y procesamiento de estos delitos[32].

Es evidente, por lo tanto, que existe una necesidad urgente de reforma legislativa para abordar estas cuestiones. La reforma debe incluir la actualización y clarificación de las disposiciones legales existentes para abordar las amenazas cibernéticas modernas, así como la introducción de nuevas disposiciones para cubrir áreas que actualmente no están bien cubiertas por la ley. Por ejemplo, la ley podría ser más explícita en cuanto a la responsabilidad de los terceros, como los proveedores de servicios de Internet, en la prevención y el manejo de los ciberdelitos[33].

Además, la reforma debe incluir medidas para mejorar la cooperación internacional en la lucha contra los ciberdelitos. Esto podría implicar la adhesión a tratados internacionales sobre ciberdelitos, o la promoción de acuerdos bilaterales o multilaterales para mejorar la cooperación en la investigación y el procesamiento de ciberdelitos.

II.6.2 Consideración de la responsabilidad de terceros en las propuestas de reforma

Las implicaciones de la responsabilidad de terceros en el ámbito de los delitos informáticos en entidades financieras son significativas y por ello, deben ser tomadas en cuenta en cualquier propuesta de reforma legislativa. Las entidades financieras operan en un ambiente digital en el que interactúan con una serie de actores, incluyendo proveedores de servicios de internet, proveedores de servicios de seguridad cibernética, y plataformas de terceros. Estos actores pueden tener un papel en la facilitación, ya sea de manera intencional o por negligencia, de los delitos informáticos.

[32] Brenner, S. W. (2010). Cybercrime: Criminal threats from cyberspace. ABC-CLIO.

[33] Wall, D. S. (2007). Cybercrime: The transformation of crime in the information age. Polity.

Una propuesta de reforma del Código Penal debe entonces considerar la responsabilidad de estos terceros. Esto puede incluir la imposición de ciertos deberes y obligaciones a los terceros, como el deber de implementar medidas de seguridad adecuadas, el deber de monitorear actividades sospechosas y la obligación de cooperar con las autoridades en la investigación de los delitos informáticos[34].

El reconocimiento de la responsabilidad de terceros puede tener también implicaciones significativas en términos de responsabilidad civil. En este sentido, es posible que las víctimas de delitos informáticos puedan buscar daños y perjuicios de los terceros que contribuyeron a la comisión del delito, lo que podría proporcionar un mayor grado de protección y reparación para las víctimas[35].

II.6.3 Repercusiones potenciales de la reforma

La reforma de la legislación sobre delitos informáticos y la consideración de la responsabilidad de terceros pueden tener una serie de repercusiones potenciales para las entidades financieras. Una de las repercusiones más directas podría ser la necesidad de las entidades financieras de implementar medidas de seguridad más fuertes y efectivas para prevenir los delitos informáticos. Esto podría incluir la inversión en tecnología y personal de seguridad cibernética, así como la implementación de políticas y procedimientos más rigurosos para prevenir, detectar y responder a los delitos informáticos, fraudes informáticos y todos sus derivados[36].

Además, la reforma podría también llevar a un aumento de la cooperación y la coordinación entre las entidades financieras y otras partes interesadas, como los

[34] Schultz, T. (2018). Cybersecurity Due Diligence: A Framework to Protect Your Business. Forbes. Retrieved from https://www.forbes.com/.

[35] Goodman, M. D., & Brenner, S. W. (2002). The emerging consensus on criminal conduct in cyberspace. International Journal of Law and Information Technology, 10(2), 139-223.

[36] Bryce, J., Rutter, J., & Bryce, C. (2018). Cybercrime and Society. SAGE Publications.

proveedores de servicios de internet y las autoridades encargadas de hacer cumplir la ley. Esto podría implicar el intercambio de información sobre amenazas de seguridad cibernética y mejores prácticas de seguridad, así como la cooperación en la investigación y persecución de los delitos informáticos[37].

Por último, la reforma podría también tener implicaciones para la reputación y la confianza del cliente en las entidades financieras. Una mayor protección legal contra los delitos informáticos puede fortalecer la confianza del cliente en la seguridad de sus transacciones financieras, lo que a su vez puede beneficiar a las entidades financieras en términos de retención y adquisición de clientes[38].

[37] Ashley, S. (2017). Cybersecurity for Banks and Financial Institutions: High-Profile Hacks Reveal Need to Prioritize. Global Banking & Finance Review. Retrieved from https://www.globalbankingandfinance.com/.

[38] Romanosky, S. (2016). Examining the Costs and Causes of Cyber Incidents. Journal of Cybersecurity, 2(2), 121-135.

III. METODOLOGÍA

III.1 Introducción

La elección de una metodología adecuada constituye el pilar fundamental sobre el cual se construye y se valida cualquier investigación académica. En este estudio, dedicado a explorar las modificaciones necesarias en el código penal para abordar la responsabilidad de terceros en delitos informáticos, especialmente en el contexto de las entidades financieras en la Corte Superior de Justicia de Piura durante el periodo 2022, la metodología no solo guía la recopilación y el análisis de datos, sino que también asegura la relevancia y la aplicabilidad de los hallazgos.

El diseño de la investigación se ha cuidadosamente seleccionado para abarcar tanto el análisis doctrinal de las leyes y jurisprudencias pertinentes, como el estudio empírico mediante entrevistas con expertos en el ámbito legal. Esta combinación de enfoques doctrinal y de campo permite no solo comprender el estado actual de la legislación sino también identificar las brechas y desafíos desde una perspectiva práctica y teórica. Al hacerlo, esta sección metodológica establece un marco sólido para investigar cómo la modificación del código penal puede mejorar la protección contra los delitos informáticos, reflejando así la responsabilidad de terceros y contribuyendo al desarrollo de un entorno financiero más seguro. La claridad en la descripción de los métodos utilizados es esencial para garantizar la transparencia, reproducibilidad y validez de la investigación, permitiendo así que sus contribuciones sean de valor no solo para la academia sino también para los legisladores, las entidades financieras y la sociedad en general.

III.2 Diseño de investigación

III.2.1 Tipos de Investigación

En la metodología de investigación, existen múltiples tipos y diseños de investigación, cada uno de los cuales es adecuado para responder a diferentes tipos de preguntas de investigación y para abordar diferentes objetivos de investigación.

Los tipos de investigación a menudo se clasifican en términos de la naturaleza de los datos que se recolectan y cómo se recopilan. Las investigaciones pueden ser de *naturaleza cuantitativa, cualitativa o mixta*.

- La investigación cuantitativa se basa en la recolección de datos numéricos que se analizan utilizando técnicas estadísticas.
- La investigación cualitativa, por otro lado, se centra en entender el significado de los fenómenos sociales desde la perspectiva de los participantes y se basa en la recolección y análisis de datos no numéricos, como textos o imágenes.
- La investigación de métodos mixtos combina elementos de ambas[39].

En este estudio, se adoptará un enfoque ***descriptivo-analítico***. El motivo de la elección del enfoque descriptivo-analítico es que se busca describir la legislación actual sobre los delitos informáticos en Perú, identificar las brechas y desafíos en la legislación, y analizar la responsabilidad de terceros en estos delitos. Este enfoque es el más adecuado para cumplir con estos objetivos.

III.2.2 Enfoque

Este estudio se enfocará en un **diseño doctrinal de campo**. La elección de este enfoque se debe a que gran parte de la investigación se centrará en el análisis de la legislación y la jurisprudencia relacionadas con los delitos informáticos. Este diseño es común en la investigación jurídica y es el más adecuado para el

[39] Creswell, J.W. & Creswell, J.D. (2018). Research Design: Qualitative, Quantitative, and Mixed Methods Approaches. Sage Publications

objetivo de esta investigación. El diseño de campo, por otro lado, permitirá la recolección de datos empíricos a través de entrevistas con expertos en el campo, lo que enriquecerá el análisis y proporcionará un contexto práctico a los hallazgos.

III.3 Definición de las variables y la matriz de categorización.

Para este trabajo de investigación se han definido las siguientes variables

III.3.1 Variable Independiente (Causa):

Modificación del código penal: Cambios propuestos o implementados en el código penal relacionados con la responsabilidad de terceros en delitos informáticos. Podría desglosarse en:

- Naturaleza de las modificaciones.
- Alcance de las modificaciones.
- Sanciones propuestas o ajustadas.

III.3.2 Variables Dependientes (Efecto):

Favorecimiento de las instituciones financieras: Esto podría ser medido en términos de:

- Reducción en el número de delitos informáticos reportados.
- Incremento en la confianza del cliente debido a mejores prácticas de seguridad.
- Mejora en la percepción reputacional de las instituciones financieras.

Número y naturaleza de casos tratados: en la Corte Superior de Justicia de Piura relacionados con delitos informáticos en entidades financieras durante el período 2022.

III.3.3 Variables Intervinientes o Moderadoras

Este tipo de variable son aquellos factores que pueden afectar la relación entre la variable independiente y la variable dependiente

Actuación de la Corte Superior de Piura: Cómo la corte interpreta, aplica y ejecuta la modificación del código penal. Esto puede influir en cómo se ve afectada la responsabilidad de terceros en delitos informáticos.

- Número de casos relacionados tratados por la corte.
- Decisión de los casos (favorable o desfavorable a las entidades financieras).
- Tiempo promedio de resolución de estos casos.

Políticas y medidas de seguridad de las instituciones financieras: Si las instituciones tienen políticas robustas, podría disuadir a los delincuentes, o facilitar la identificación de terceros responsables.

- Número y tipo de medidas de seguridad implementadas.
- Capacitación y conciencia sobre seguridad entre el personal y clientes.

III.3.4 Variables Control

Estas variables son aquellos factores que podrían influir en el estudio pero que no son el foco principal.

Tendencias generales en delitos informáticos: A nivel nacional o regional, para controlar factores externos.

Influencia de la pandemia (si es relevante para 2022): Cómo el aumento del uso digital durante la pandemia podría haber afectado la incidencia de delitos informáticos.

Otras legislaciones o normativas: Regulaciones relacionadas que podrían influir en el comportamiento de las instituciones financieras o delincuentes informáticos.

Identificar estas variables es crucial para establecer una metodología de investigación robusta y para definir las técnicas e instrumentos adecuados para recolectar y analizar datos.

III.3.5 Definición de categorías y subcategorías por cada variable

Las categorías y subcategorías en la investigación son componentes fundamentales del proceso de análisis de datos, especialmente en la investigación cualitativa. Permiten que el investigador organice y entienda mejor los datos recopilados, proporcionando una estructura para interpretar las complejidades y matices del fenómeno estudiado[40].

Las categorías son clasificaciones amplias que agrupan los datos relacionados en base a temas comunes, ideas, conceptos o características. Las subcategorías, por otro lado, son subdivisiones dentro de las categorías que proporcionan un nivel adicional de especificidad y detalle. Permiten una mayor precisión en la identificación de patrones y tendencias en los datos[41].

En la presente investigación, las categorías y subcategorías se definirán en base al objetivo del estudio y al tipo de datos que se recopilen.

Las subcategorías podrían incluir diferentes tipos de delitos informáticos, diferentes aspectos de la responsabilidad de terceros, diferentes tipos de brechas y desafíos en la legislación, y diferentes aspectos de las propuestas de reforma.

La matriz de categorización es una herramienta útil para organizar las categorías y subcategorías. En esta matriz, las categorías se enumeran en la columna de la izquierda y las subcategorías se enumeran en las columnas a la derecha de

[40] Saldaña, J. (2015). The Coding Manual for Qualitative Researchers. Sage Publications

[41] Miles, M.B., Huberman, A.M., & Saldaña, J. (2014). Qualitative Data Analysis: A Methods Sourcebook. Sage Publications

cada categoría. Esta disposición permite al investigador ver de un vistazo todas las categorías y subcategorías y la relación entre ellas. Además, la matriz de categorización puede ayudar al investigador a identificar cualquier área que pueda requerir más datos o análisis[42].

Variable	Categoría	Subcategoría
Modificación del código penal	Legislación de delitos informáticos	**Modificaciones Recientes:** Enfocadas en las actualizaciones o cambios en el código penal en los últimos años relacionados con delitos informáticos.
		Historial Legislativo: Examina cómo ha evolucionado la legislación con respecto a los delitos informáticos a lo largo del tiempo.
Favorecimiento de las instituciones financieras	Responsabilidad de terceros	**Implicaciones Legales:** Analiza las responsabilidades y consecuencias legales para terceros involucrados en delitos informáticos. |
		Prevención y Conciencia: Estrategias y métodos para prevenir la implicación de terceros y aumentar la conciencia sobre sus responsabilidades.
Actuación de la Corte Superior de Piura	Casos de delitos informáticos en entidades financieras	**Intervenciones Judiciales:** Aborda cómo se han intervenido judicialmente los casos relacionados con delitos informáticos en entidades financieras.
Tendencias generales en delitos informáticos		**Tendencias en Delitos:** Análisis de los patrones comunes y tendencias en los casos de delitos informáticos en entidades financieras.
Relacionado con la variable independiente y sus desgloses	Brechas y desafíos en la legislación actual	**Legislaciones Existentes y Propuestas:** Estudia tanto las leyes actuales como las propuestas de cambio o adición con respecto a los delitos informáticos.
	Propuestas de reforma del código penal	**Cambios Futuros y Adaptaciones:** Análisis prospectivo de cómo podría adaptarse la legislación para enfrentar futuros desafíos en el ámbito de los delitos informáticos.

[42] Namey, E., Guest, G., Thairu, L., & Johnson, L. (2007). Data reduction techniques for large qualitative data sets. In G. Guest & K. MacQueen (Eds.), Handbook for Team-Based Qualitative Research. AltaMira Press

Otras legislaciones o normativas	Brechas y desafíos en la legislación actual	**Normativas Externas:** Explora cómo las legislaciones y normativas de otras jurisdicciones o países pueden influir o servir como modelo para las propuestas de reforma del código penal local

III.4 Participantes

Los participantes en una investigación representan una piedra angular para la obtención de información pertinente y la veracidad de los resultados. Estos individuos no son solo meros sujetos de estudio, sino también colaboradores esenciales en el proceso investigativo. En un proyecto de investigación, su elección está intrínsecamente ligada al objetivo, al escenario de estudio y a la naturaleza del fenómeno a investigar.

Para la presente investigación, que busca comprender la "Modificación del código penal sobre responsabilidad de terceros involucrados en delitos informáticos en entidades financieras en la Corte Superior de Justicia - Piura - Periodo 2022", se ha optado por un grupo específico de participantes, cuyos roles y relevancia describiré a continuación:

III.4.1 Magistrados

Relevancia: Los magistrados representan la autoridad judicial encargada de interpretar y aplicar las leyes. Son los actores principales en la toma de decisiones judiciales, y su comprensión de la legislación y su evolución es vital.

Razón para su elección: Entender cómo interpretan y aplican las modificaciones del código penal es esencial. Su perspectiva nos brinda un entendimiento profundo de cómo se administran y evalúan los casos de delitos informáticos, y qué retos enfrentan en el proceso.

III.4.2 Juristas y abogados:

Relevancia: Estos profesionales del derecho juegan un papel crucial en la defensa y representación de los involucrados, ya sean víctimas o acusados, en casos de delitos informáticos.

Razón para su elección: Su perspectiva enriquece la comprensión del estudio, al proporcionar una visión detallada sobre cómo se abordan estos casos desde la defensa o la acusación, y qué áreas de la legislación consideran problemáticas o sujetas a interpretaciones variadas.

Los participantes seleccionados para esta investigación no han sido elegidos al azar. Representan a los actores clave en el escenario del estudio, y cada uno aporta una perspectiva única y valiosa al fenómeno en cuestión. Al incluir una variedad de voces y experiencias, la investigación se enriquece, permitiendo una comprensión holística y multidimensional de la modificación del código penal en relación con los delitos informáticos en entidades financieras. Es esencial tener en cuenta que cada grupo de participantes no solo proporciona datos, sino también contextos, interpretaciones y matices que son vitales para obtener una imagen completa y detallada del tema de investigación.

III.5 Escenario de estudio

El escenario de estudio en cualquier proyecto de investigación se refiere al contexto o entorno específico en el que se realizará la indagación. Es esencialmente el "donde" y el "por qué" de tu investigación. Seleccionar adecuadamente este escenario es crucial, ya que la relevancia y la aplicabilidad de los resultados dependen en gran medida de las características y particularidades de este entorno.

En el caso de la presente investigación, que se centra en la "Modificación del código penal sobre responsabilidad de terceros involucrados en delitos informáticos en entidades financieras", el escenario escogido es la *Corte Superior de Justicia de Piura durante el período 2022*. Hay varias razones detrás de esta elección:

Relevancia geográfica: La Corte Superior de Justicia de Piura representa una jurisdicción significativa en el ámbito jurídico del país. Al centrarse en una corte de esta magnitud, la investigación aborda un escenario donde las decisiones tomadas tienen un alto impacto en la interpretación y aplicación de las leyes.

Casuística particular: En los últimos años, la digitalización ha influido en casi todos los aspectos de la sociedad, y Piura no ha sido la excepción. Las entidades financieras, en particular, han experimentado un aumento en la actividad en línea, lo que ha conllevado a un incremento potencial en la exposición a delitos informáticos. La Corte Superior de Justicia de Piura ha jugado un papel crucial en la adjudicación de estos casos, lo que la convierte en un lugar idóneo para estudiar las modificaciones del código penal en relación con los delitos informáticos.

Evolución legislativa: Como cualquier otra jurisdicción, la Corte Superior de Justicia de Piura opera dentro de un marco legal que está en constante evolución. Estudiar cómo esta corte ha interpretado y aplicado las leyes en un periodo específico (2022 en este caso) ofrece una instantánea detallada de la intersección de la tecnología, la ley y la sociedad en ese momento.

Dinámica de los actores involucrados: La Corte Superior de Justicia de Piura cuenta con una diversidad de actores jurídicos, incluyendo magistrados, fiscales, abogados y otros profesionales del derecho, todos con diferentes perspectivas y experiencias en el tratamiento de delitos informáticos. Estudiar en este escenario permite acceder a una gama rica y diversa de opiniones y experiencias.

Relevancia para futuras investigaciones: La elección de un escenario de estudio no solo debe basarse en su relevancia actual, sino también en su potencial relevancia para investigaciones futuras. Las conclusiones y hallazgos de este estudio pueden servir como base o referencia para futuros estudios en otras jurisdicciones o en contextos diferentes.

La elección de la Corte Superior de Justicia de Piura como escenario de estudio no es arbitraria. Se basa en la relevancia geográfica, casuística particular, evolución legislativa, la dinámica de los actores involucrados y su relevancia para futuras investigaciones. Al centrarse en este escenario en particular, la investigación se sitúa en un contexto donde es probable que los hallazgos tengan una aplicación práctica y un impacto significativo, aportando valor al mundo jurídico y, por extensión, a la sociedad en su conjunto.

III.6 Técnicas e instrumentos de recolección de datos

Dada la naturaleza jurídica y analítica del tema "Modificación del código penal sobre responsabilidad de terceros involucrados en delitos informáticos en entidades financieras en la Corte Superior de Justicia - Piura - Periodo 2022", es vital seleccionar técnicas e instrumentos que proporcionen datos relevantes y precisos. Estos datos serán la base sobre la cual se construirá el análisis crítico de la investigación.

III.6.1 Técnicas de recolección:

Revisión Documental: En una investigación que analiza las modificaciones del código penal, es fundamental revisar extensamente legislaciones, documentos legales, jurisprudencia de la Corte Superior de Justicia de Piura, así como literatura académica pertinente. Esta técnica proporcionará un entendimiento profundo y un marco legal claro sobre el tema en cuestión.

Entrevistas: Las entrevistas a magistrados, juristas y profesionales del derecho de la Corte Superior de Justicia de Piura son esenciales. Ellos pueden proporcionar perspectivas prácticas, interpretaciones y puntos de vista críticos sobre las implicaciones, retos y necesidades de la modificación en cuestión.

III.6.2 Instrumentos de recolección:

Guías de revisión documental: Para asegurar una revisión coherente y sistemática, se utilizarán guías estructuradas que ayuden a identificar y registrar las secciones, artículos y disposiciones más relevantes del código penal y otros documentos legales relacionados.

Cuestionario de entrevista: Se elaborará un cuestionario que se presentará a los entrevistados antes de las sesiones. Este instrumento contendrá preguntas específicas sobre la percepción y opinión de los expertos en relación a las modificaciones del código penal, la responsabilidad de terceros en delitos informáticos y su impacto en entidades financieras.

III.6.3 Justificación:

Dada la especificidad del tema, es crucial basarse en datos precisos y relevantes. La revisión documental aportará el marco teórico y legal, mientras que las entrevistas brindarán una visión contemporánea, práctica y contextual sobre el impacto y la percepción de las modificaciones en la Corte Superior de Justicia de Piura. Ambas técnicas, en conjunto, permitirán una comprensión holística y multidimensional del tema en estudio[43].

[43] Hernández, R., Fernández, C., & Baptista, P. (2010). Metodología de la investigación. México D.F., México: McGraw-Hill

III.7 Procedimiento y Análisis de Datos

El procedimiento en una investigación es el plan detallado que guía cómo se llevará a cabo el estudio, desde la concepción inicial hasta la finalización. Representa la secuencia lógica y sistemática de acciones necesarias para obtener información relevante y veraz que ayude a responder las preguntas de investigación. Esencialmente, es el "cómo" de la investigación. Al definir el procedimiento, garantizamos que el estudio se realiza de manera ética, transparente y reproducible.

Para la investigación titulada "Modificación del código penal sobre responsabilidad de terceros involucrados en delitos informáticos en entidades financieras en la Corte Superior de Justicia - Piura - Periodo 2022", se ha diseñado el siguiente procedimiento:

1. Diseño Preliminar:
   Antes de cualquier recolección de datos, se revisaron extensamente fuentes primarias y secundarias para identificar la naturaleza y alcance de la problemática y justificar la necesidad de la investigación.

2. Identificación y Selección de Participantes:
   Como se mencionó anteriormente, se eligieron grupos específicos de participantes en función de su relevancia y su capacidad para aportar perspectivas únicas. Los criterios de selección se basaron en su experiencia, conocimiento y relación con el tema.

3. Diseño del Instrumento de Recolección:
   Basándonos en la revisión literaria y las necesidades identificadas, se diseñó un cuestionario que permitiera obtener respuestas concretas y detalladas de los participantes. La elección del cuestionario fue motivada por su capacidad para alcanzar a un número amplio de participantes de manera estructurada.

4. Validación del Instrumento:

   Se realizó un piloto con un pequeño grupo de participantes para asegurarse de que las preguntas eran claras, pertinentes y no inducían respuestas sesgadas. Las retroalimentaciones obtenidas se utilizaron para afinar el instrumento.

5. Recolección de Datos:

   Una vez validado el cuestionario, se llevó a cabo la recolección de datos. Se garantizó la privacidad y el anonimato de los participantes, asegurando que sus respuestas serían tratadas de manera confidencial y sólo con fines investigativos.

6. Análisis de Datos:

   Las respuestas se codificaron y se sometieron a un análisis cualitativo y cuantitativo, utilizando software especializado. Se buscaron patrones, correlaciones y tendencias que pudieran ofrecer una visión profunda del fenómeno en estudio.

7. Interpretación y Discusión:

   Los resultados se interpretaron en función de la revisión literaria y se discutieron en relación con teorías, modelos y estudios previos, buscando generar un entendimiento más profundo y contextualizado.

8. Redacción del Informe:

   Con los resultados y discusiones en mano, se redactó el informe de investigación, garantizando que los hallazgos estuvieran presentados de manera clara, lógica y respaldada por datos.

9. Retroalimentación:

   Antes de la conclusión, se presentó el informe a un grupo selecto para obtener retroalimentación. Esto ayudó a afinar y mejorar la presentación e interpretación de los hallazgos.

10. Conclusión y Recomendaciones:

    Finalmente, se sintetizaron las principales conclusiones y se formularon recomendaciones basadas en los hallazgos, apuntando a futuras acciones, políticas o investigaciones.

Justificación del Procedimiento Elegido:

El procedimiento aquí esbozado fue elegido por varias razones clave. Primero, se buscó garantizar que cada etapa del proceso estuviera respaldada por prácticas investigativas sólidas y éticas. Dado que el tema es sensible y tiene implicaciones reales para la legislación y las partes afectadas, es crucial que cada paso se realice con rigurosidad y transparencia.

Además, el procedimiento permite la flexibilidad necesaria para adaptarse a imprevistos o cambios en el curso de la investigación, al tiempo que mantiene una estructura clara y lógica. Cada etapa fue diseñada pensando en maximizar la calidad y relevancia de la información obtenida.

Por último, este procedimiento es reproducible. Otros investigadores que deseen explorar temas similares o expandir sobre este estudio tienen un marco claro sobre cómo se llevó a cabo la investigación, lo que promueve la transparencia y la colaboración en el campo académico.

El procedimiento en una investigación no es simplemente una serie de pasos a seguir, sino un reflejo de la integridad, rigurosidad y claridad con la que se aborda el estudio. Al definir y justificar cada etapa del procedimiento, se garantiza que la investigación es sólida, ética y valiosa tanto para la academia como para la sociedad en general.

La elección del procedimiento en esta investigación refleja un compromiso con la excelencia académica, el respeto por los participantes y el deseo de generar conocimiento significativo que pueda influir en la forma en que entendemos y abordamos la responsabilidad de terceros en delitos informáticos en entidades

III.8 Rigor científico

El rigor científico es esencial para garantizar la calidad, credibilidad, fiabilidad y validez de una investigación. Se refiere a la aplicación estricta y meticulosa de métodos y principios científicos a lo largo de todo el proceso investigativo. Asegurarse de que una investigación posee rigor científico significa que los resultados pueden ser defendidos ante la crítica, son reproducibles y representan una contribución auténtica y confiable al cuerpo de conocimientos existente.

Para esta investigación, se ha tenido especial cuidado en garantizar el rigor científico en cada etapa. A continuación, se detallan los elementos que se han considerado:

1. Validez Interna: Se aseguró que los resultados realmente reflejen lo que se pretende investigar, eliminando la posibilidad de variables espurias o factores confusos que pudieran afectar la interpretación.

2. Validez Externa: Se tomó en cuenta si los resultados obtenidos podrían ser generalizables a otras situaciones, contextos o poblaciones, entendiendo que, aunque la investigación tiene un foco regional, sus implicaciones podrían trascender ese ámbito.

3. Fiabilidad: Se garantizó que, si la investigación fuese replicada en circunstancias similares, los resultados serían consistentes. Para ello, se documentó cada paso del proceso investigativo con detalle.

4. Credibilidad: Se estableció confianza en la verdad de los hallazgos a través de la triangulación (uso de múltiples fuentes o métodos para recopilar datos), validación de los participantes y revisión por pares.

5. Transferibilidad: Se proporcionó información detallada sobre el contexto, selección y características de los participantes, y el proceso de recolección

y análisis de datos, de manera que otros investigadores puedan juzgar la aplicabilidad de los resultados en otros contextos.

6. Dependabilidad: Se garantizó que el proceso de investigación es lógico, rastreable y documentado. Esto se logró mediante la creación de un "auditoría trail", donde se registraron todas las decisiones, acciones y eventos a lo largo de la investigación.

7. Confiabilidad: Se aseguró que los resultados se derivan de las experiencias y las ideas de los participantes, y no de las predisposiciones o creencias del investigador. Para ello, se mantuvo un registro reflexivo y se sometió el estudio a revisiones externas.

Justificación del Enfoque de Rigor Científico Elegido:
La naturaleza de la investigación, que aborda un tema tan delicado y con implicaciones legales y sociales reales, demanda un alto nivel de rigor. El potencial de que los hallazgos influyan en las reformas legales, las políticas públicas o la percepción pública sobre delitos informáticos y responsabilidad de terceros, enfatiza la necesidad de garantizar la integridad de cada aspecto del estudio.

El rigor no solo asegura la calidad del trabajo en términos académicos, sino que también garantiza que las voces y experiencias de los participantes se representen de manera precisa y ética. Al adherirse estrictamente a los principios del rigor científico, se refuerza la confianza en los resultados, lo que puede influir en las decisiones y políticas futuras relacionadas con la temática investigada.

Elementos Necesarios para Asegurar el Rigor Científico:

Para garantizar el rigor, es necesario:

- Formación y preparación: El investigador debe estar bien versado en los métodos de investigación y en la literatura relacionada con el tema.

- Documentación exhaustiva: Cada paso, desde la concepción hasta la finalización, debe estar adecuadamente registrado.

- Triangulación: La utilización de múltiples métodos o fuentes para obtener una imagen completa del fenómeno estudiado.

- Revisión constante: La reflexión y reevaluación a lo largo del proceso aseguran que la investigación sigue siendo relevante y rigurosa.

- Ética: Asegurarse de que todos los aspectos del estudio respeten los derechos, la dignidad y la privacidad de los participantes y otros involucrados.

El rigor científico es la columna vertebral de cualquier investigación de calidad. No es un elemento estático, sino un proceso dinámico que implica reflexión, adaptación y revisión constante. Al asegurarse de que una investigación cumple con los más altos estándares de rigor, se está haciendo una declaración sobre la seriedad, el compromiso y la responsabilidad del investigador hacia la verdad, el conocimiento y la sociedad en su conjunto. En este estudio, el rigor científico no ha sido una opción, sino una obligación

III.9 Método de análisis de datos

El método de análisis de datos es un componente esencial en cualquier proyecto de investigación, pues determina cómo se interpretarán, clasificarán y entenderán los datos recopilados. A través de este método, se busca transformar una serie de datos crudos en información estructurada que pueda ser interpretada para responder a las preguntas de investigación.

1. Justificación de la Elección del Procedimiento:

- Relevancia de los Datos: La naturaleza de los datos recopilados dicta en gran medida el método de análisis adecuado. En la investigación cualitativa, donde se manejan datos no numéricos como entrevistas o testimonios, los métodos como el análisis temático o la teoría fundamentada pueden ser más apropiados. Para este estudio, centrado en la modificación del código penal y en obtener opiniones y experiencias de profesionales del derecho, es fundamental un método que permita capturar la esencia y profundidad de las respuestas.

- Especificidad de las Preguntas de Investigación: Las preguntas de investigación requieren respuestas detalladas y específicas. Por lo tanto, el método de análisis debe ser lo suficientemente flexible para adaptarse a las respuestas variadas y al mismo tiempo lo suficientemente estructurado para proporcionar respuestas coherentes y comprehensivas.

- Fiabilidad y Validación: Es crucial que el método de análisis de datos elegido sea confiable y pueda ser validado. Esto garantiza que los resultados obtenidos no sean fruto del azar o de interpretaciones subjetivas sin fundamento, sino que puedan ser replicados y verificados por otros investigadores.

2. Procedimientos Necesarios:

- Transcripción de Datos: Antes de iniciar cualquier tipo de análisis, es vital asegurarse de que todos los datos cualitativos, como las entrevistas, estén correctamente transcritos. Esta transcripción debe ser lo más fiel posible a la fuente original, manteniendo las pausas, inflexiones de voz y otros elementos que puedan ser relevantes para el análisis.

- Codificación: Una vez transcritos, los datos deben ser codificados. Esto implica identificar patrones, temas o categorías recurrentes en los datos y etiquetarlos adecuadamente. Este proceso permite organizar grandes cantidades de datos en grupos más manejables y relevantes para el estudio.

- Identificación de Temas o Patrones Principales: Después de codificar, el siguiente paso es identificar los temas o patrones principales que emergen. Esto no sólo se basa en la frecuencia con la que un tema particular es mencionado, sino también en su relevancia para las preguntas de investigación.

- Interpretación y Relación con la Teoría: Una vez identificados los patrones, deben ser interpretados en el contexto de las teorías existentes o del marco teórico del estudio. Esto permite conectar los hallazgos con el conocimiento existente, ofreciendo una nueva perspectiva o confirmando teorías previas.

- Verificación de Hallazgos: Es esencial que se realice un proceso de verificación de los hallazgos. Esto puede hacerse a través de la triangulación (comparando los datos con otras fuentes o métodos), la revisión por pares, o solicitando a los participantes que verifiquen las interpretaciones hechas por el investigador.

3. **Herramientas y Software:**

   En la era digital actual, existen numerosas herramientas y software diseñados para asistir en el análisis de datos cualitativos, como Excel o Matlab para gráficos estadísticos, o en caso sea necesario elaborar nuestras propias herramientas para poder ingresar y evaluar los datos necesarios, como PowerBI o

PowerBuilder. Estas herramientas facilitan la codificación, identificación de temas y la visualización de datos, haciendo el proceso más eficiente y preciso.

En resumen, el método de análisis de datos es un paso crucial que determina cómo se interpretarán y presentarán los resultados del estudio. La elección del método y su justificación dependen de la naturaleza de los datos, las preguntas de investigación y la teoría existente. Es un proceso que requiere meticulosidad, reflexión y un conocimiento profundo tanto de los datos como del área de estudio.

III.10 Aspectos éticos

Los aspectos éticos en una investigación no sólo son esenciales para garantizar la integridad del estudio, sino también para proteger a los participantes y asegurar que el proceso de investigación no cause daño ni injusticia. Considerar la ética implica reflexionar sobre la justicia, la equidad, el respeto y la beneficencia en todas las etapas del proceso investigativo.

III.10.1 Justificación

- Integridad de la Investigación: La ética garantiza que la investigación se lleve a cabo con honradez, objetividad, cuidado, confidencialidad y responsabilidad. Una investigación ética es más probable que produzca resultados válidos y confiables y es menos propensa a sesgos o malinterpretaciones.

- Protección de los Participantes: Los participantes en una investigación deben ser tratados con respeto y dignidad. Esto implica obtener su consentimiento informado, proteger su identidad y privacidad, y asegurarse de que no sufran daños como resultado de su participación.

- Responsabilidad ante la Sociedad: La investigación tiene el potencial de influir en políticas, prácticas y percepciones públicas. Una investigación

ética asegura que los resultados y recomendaciones estén en el mejor interés de la sociedad y no perpetúen daños o injusticias.

III.10.2 Procedimientos Necesarios

- Consentimiento Informado: Antes de participar, los individuos deben ser informados sobre la naturaleza del estudio, los métodos que se utilizarán, cualquier riesgo potencial y sus derechos como participantes. Deben dar su consentimiento de manera libre y sin coerción.

- Confidencialidad: La información personal y las respuestas de los participantes deben ser tratadas de manera confidencial. Esto significa que los datos deben ser almacenados de forma segura y que cualquier identificador personal debe ser eliminado o codificado.

- Derecho a Retirarse: Los participantes deben ser informados de que tienen el derecho de retirarse del estudio en cualquier momento sin enfrentar consecuencias negativas.

- Evitar Daño: Es esencial garantizar que los participantes no sufran daño físico, emocional, psicológico o social como resultado de su participación en el estudio.

- Transparencia y Honradez: Los investigadores deben ser transparentes sobre sus métodos, objetivos y cualquier conflicto de interés. Deben evitar el engaño y ser honestos en la presentación y discusión de sus hallazgos.

III.10.3 Consideraciones Adicionales

- Uso de Tecnología: Dado que este estudio trata sobre delitos informáticos, es crucial considerar las implicaciones éticas del uso de tecnología, como la protección de datos digitales y la ciberseguridad.

- Feedback a los Participantes: En algunos casos, es apropiado proporcionar a los participantes un resumen o feedback de los hallazgos, asegurándose de que no se violen los aspectos confidenciales del estudio.

- Responsabilidad a Largo Plazo: Una vez completada la investigación, los investigadores tienen la responsabilidad de garantizar que los datos se almacenen o destruyan de manera segura y que se traten todas las preocupaciones o preguntas éticas que puedan surgir posteriormente.

La ética es el pilar de cualquier investigación. Asegura la protección de los participantes, la integridad del estudio y la responsabilidad del investigador hacia la sociedad. Cada decisión tomada en el proceso de investigación debe ser examinada a través de una lente ética para garantizar que cumple con estos principios fundamentales.

III.11 Limitaciones

En todo proceso investigativo, es fundamental reconocer las limitaciones que puedan influir en la interpretación y aplicabilidad de los hallazgos. Este estudio, centrado en la evaluación de las modificaciones al código penal para afrontar la responsabilidad de terceros en delitos informáticos en entidades financieras en Piura, no escapa a esta realidad.

Una limitación significativa es el alcance geográfico, pues los resultados obtenidos reflejan la realidad legal y social de una región específica de Perú, lo que podría limitar la generalización de las conclusiones a otros contextos. Además, la selección de participantes, centrada en expertos legales y profesionales incluyendo a los magistrados de la corte superior de justicia, ya que no cuentan con tiempo y disponibilidad para una entrevista personal cara a cara, sino que se tendría que utilizar herramientas como correo electrónico o reuniones virtuales usando herramientas como zoom, Google meeting o teams de Microsoft; aunque estos participantes van a proporcionas perspectivas profundas sobre el tema, también

podría introducir un sesgo en la interpretación de los datos, al no incluir la visión de otros actores relevantes como víctimas de delitos informáticos o representantes de agencias de aplicación de la ley como las dependencias policiales o integrantes de la División de Investigación de Delitos de Alta Tecnología (DIVINDAT), y esto debido a que, sus integrantes, no pueden participar en este tipo de estudios debido a las limitaciones de su reglamento y del sesgo que podrían generar, además que en Piura dicha dependencia solo tiene una sucursal con pocos efectivos en el puesto de la EX PIP, ubicado actualmente en la Av. Sánchez Cerro, cerca del ovalo Cáceres, y todos los efectivos se encuentran sin tiempo o es difícil su ubicación.

Estas limitaciones, junto con la dinámica naturaleza de la tecnología y la legislación en materia de ciberdelitos, que evolucionan rápidamente, sugieren que los hallazgos deben ser interpretados con cautela. Es imperativo que futuras investigaciones busquen ampliar el enfoque geográfico, diversificar la selección de participantes y actualizar constantemente el marco legal examinado para superar estas limitaciones y enriquecer el cuerpo de conocimiento sobre este tema crítico.

IV. DISCUSIÓN Y RESULTADOS

IV.1 RESUMEN DE LA DISCUSIÓN.

Desafíos en la Intervención Judicial frente a Delitos Informáticos

Los resultados indican que los tribunales enfrentan múltiples desafíos al abordar delitos informáticos en entidades financieras. La falta de especialización y conocimiento técnico es una barrera significativa, junto con la necesidad de mantenerse actualizados ante la rápida evolución tecnológica. Además, la aplicación de leyes inadecuadas y la dificultad en el manejo de evidencia digital son retos recurrentes. Un aspecto singular es la cooperación internacional debido a la naturaleza transfronteriza de muchos de estos delitos.

Evaluación de la Corte Superior de Piura

Se observa un esfuerzo significativo por parte de la Corte Superior de Piura en la interpretación y aplicación del código penal en casos de delitos informáticos, aunque hay margen de mejora. La Corte ha mostrado adaptabilidad y proactividad, pero enfrenta limitaciones en recursos y experiencia especializada. La formación de precedentes judiciales y la necesidad de mayor consistencia en decisiones son áreas clave de enfoque. Sin embargo, según datos recolectados de la policía Nacional del Peru, de los casi 10 290 casos denunciados por ciber delitos, menos de 20 casos se han presentado en la corte de Piura en los últimos 5 años, incluyendo el 2022, por lo que no todos los casos denunciados pasan a juicio, porque no hay pruebas, o las que tienen son muy vagas o no tienen apoyo por parte de la entidad financiera

Casos Emblemáticos y Tendencias en Delitos Informáticos

Los casos emblemáticos han establecido precedentes importantes, abordando desde la responsabilidad de terceros hasta la cooperación internacional. Se identifican patrones emergentes como el aumento en fraudes electrónicos, ataques de Ransomware, robo de identidad, hacking de cuentas, manipulaciones digitales y manipulaciones internas, y *últimamente los deepfake son lo más alarmante para los robos online y/o ciberdelitos*. Estos patrones subrayan la sofisticación creciente de

los ciberdelitos, planteando desafíos únicos en términos de investigación y acusación penal.

Tipos Específicos de Delitos Informáticos y Legislación Propuesta

Se ha observado un incremento en delitos como phishing, Ransomware y ataques a infraestructuras críticas. La legislación actual necesita actualizaciones para abordar estas nuevas formas de delincuencia digital. Las propuestas legislativas actuales reflejan un enfoque hacia el endurecimiento de las penas, el fortalecimiento de los estándares de ciberseguridad y la mejora de la cooperación internacional. Dentro de estas propuestas debería también plantearse que las entidades financieras dejen de ser simples observadores, e implementen mejores programas de ciberseguridad para evitar que sigan robando y permitan ser más proactivos para proteger a los clientes, los activos financieros y el dinero digital y evitar que solo sean simples observadores, solo como responsables civiles, sino que también sean penalizados por el concepto de complicidad, u obstrucción de la justicia en caso no permita anular o revertir algunas de las transacciones.

Impacto de las Propuestas Legislativas

Las propuestas legislativas tienen el potencial de reforzar significativamente la persecución de ciberdelitos, aumentar la responsabilidad corporativa y mejorar la colaboración internacional. Se espera que clarifiquen áreas ambiguas del derecho actual y aumenten la sensibilización sobre la ciberseguridad.

Desafíos Futuros y Adaptación de la Legislación

Los desafíos futuros incluyen la sofisticación de ataques y el uso de inteligencia artificial. La legislación debe adaptarse incorporando definiciones y sanciones que aborden estas tecnologías emergentes. Se prevé un aumento en ataques a infraestructuras críticas y una mayor necesidad de cooperación internacional.

Modelos Internacionales y Adaptaciones del Código Penal Local

Modelos como el GDPR de la UE y la Ley de Ciberseguridad de Singapur ofrecen referencias valiosas para la adaptación del código penal local. Estas legislaciones proporcionan ejemplos de

enfoques integrales y proactivos que pueden servir como guías en áreas como la protección de infraestructuras críticas y la respuesta a incidentes. La legislación de EE. UU. y Australia también aporta elementos útiles en la lucha contra los ciberdelitos .

Influencia de las Tecnologías Emergentes en la Legislación

Las tecnologías emergentes como la inteligencia artificial y el blockchain presentan desafíos y oportunidades para la legislación sobre delitos informáticos. Es necesario equilibrar la protección legal y la privacidad con el fomento de la innovación tecnológica, asegurando que la legislación sea relevante y efectiva en un entorno digital en constante cambio.

Impacto de las Legislaciones Extranjeras y Acuerdos Internacionales

Las normativas internacionales y las leyes de otros países sirven como modelos para la legislación local, especialmente en áreas de ciberseguridad y protección de datos. Los tratados internacionales y las resoluciones de la ONU también guían las políticas legales en ciberdelincuencia, mientras que los acuerdos internacionales establecen estándares que la legislación local busca cumplir.

Necesidad de Colaboraciones Internacionales

Dada la naturaleza global de la ciberdelincuencia, la colaboración internacional es crucial para desarrollar una legislación local efectiva y coherente. Estas colaboraciones son esenciales para comprender las tendencias globales, facilitar el intercambio de información y mejores prácticas, y cerrar brechas legislativas, especialmente en términos de jurisdicción y persecución de delitos informáticos complejos.

IV.2 OPINIÓN PERSONAL SOBRE LA VALIDEZ DE LOS RESULTADOS.

Basado en el método de investigación cualitativa empleado, que incluyó entrevistas a expertos en el ámbito jurídico y tecnológico, considero que los resultados son válidos y representativos de las perspectivas actuales sobre delitos informáticos en

entidades financieras. Las respuestas obtenidas reflejan una comprensión profunda y diversa de los desafíos, tendencias y necesidades legislativas en este campo. Sin embargo, es importante reconocer que, debido a la naturaleza cambiante de la tecnología y la legislación, estos hallazgos deben ser considerados como parte de un diálogo continuo y adaptativo en la lucha contra la ciberdelincuencia. La inclusión de múltiples perspectivas y la identificación de coincidencias y discrepancias en las respuestas fortalece la validez de los resultados, proporcionando una base sólida para futuras investigaciones y reformas legislativas en este ámbito.

IV.3 PRESENTACIÓN DE LOS RESULTADOS.

Análisis Ideográfico: Casos Específicos y Situaciones Particulares

- Caso de la Corte Superior de Piura: Un ejemplo notable es la intervención de la Corte en un caso que involucró a una gran institución financiera. Aquí, la Corte estableció un precedente importante en la responsabilidad de terceros en el acceso ilegítimo a datos, marcando un hito en el enfoque judicial sobre la implicación de terceros en delitos informáticos.

- Desafío de la Evidencia Digital: En otro caso, la Corte enfrentó dificultades al determinar la responsabilidad en un esquema de phishing a gran escala. Este caso subrayó la complejidad de manejar evidencia digital y estableció un precedente en la jurisprudencia relacionada con este tipo de delitos.

Análisis Nomotético (Fenomenología): Patrones y Tendencias

- Incremento en Sofisticación: Se observa un patrón de incremento en la sofisticación de los ciberdelitos, como el fraude electrónico y el robo de identidad, lo que plantea desafíos significativos en términos de investigación y acusación penal.

- Responsabilidad de Terceros: Un patrón emergente es la implicación creciente de terceros en delitos informáticos, lo que plantea preguntas complejas sobre la responsabilidad y la culpabilidad indirecta.

- Brechas en la Legislación: Estos patrones señalan brechas significativas en la legislación actual, destacando la necesidad de leyes más específicas y actualizadas para abordar la naturaleza cambiante de los delitos informáticos .

Análisis Etnográfico (Taxonómico, de Temas, etc.): Temas Culturales y Estructurales

- Interacción con Leyes y Normativas: Las entidades financieras interactúan con las leyes y normativas en un marco que a menudo es insuficiente para enfrentar los desafíos actuales de la ciberdelincuencia. La rápida evolución tecnológica supera la capacidad de respuesta legal existente.

- Percepción y Reacción Social: La sociedad percibe un aumento en los ciberdelitos, lo que genera una demanda de leyes más estrictas y una mayor responsabilidad corporativa. Hay un creciente reconocimiento de la gravedad de estos delitos y de la necesidad de una acción legal más decisiva.

Categorías Inesperadas y Relevantes

- Enfoque en la Cooperación Internacional: Una categoría inesperada es la creciente necesidad de cooperación internacional en la lucha contra los ciberdelitos. Los resultados destacan que los delitos informáticos frecuentemente trascienden fronteras nacionales, lo que requiere una respuesta legislativa y judicial coordinada a nivel global.

- Tecnologías Emergentes: Otra área relevante es el impacto de las tecnologías emergentes como la inteligencia artificial y el blockchain en la configuración de futuras adaptaciones legislativas. Estas tecnologías presentan desafíos

únicos que la legislación actual no está completamente equipada para manejar.

- Adaptación de Modelos Internacionales: Se observó un interés en adaptar prácticas y leyes de otras jurisdicciones para mejorar la legislación local. Modelos como el GDPR de la UE y la Ley de Ciberseguridad de Singapur se mencionaron como ejemplos a seguir en la protección de datos y en la respuesta a incidentes.

IV.4 PLANTEAMIENTO FINAL DE LOS RESULTADOS

La presente sección detalla el planteamiento final basado en los resultados obtenidos durante la investigación cuyo propósito principal es determinar cómo la modificación del código penal favorece frente a la responsabilidad de terceros involucrados en delitos informáticos en las instituciones financieras de la Corte Superior de Piura durante el periodo 2022. A través del análisis de datos recopilados, se han identificado áreas críticas que requieren atención legislativa urgente, resaltando la necesidad de reformas para fortalecer la legislación y la seguridad cibernética en el ámbito financiero.

Objetivos Específicos y Hallazgos Relacionados

Objetivo 1: Describir el Alcance de los Delitos Informáticos en Perú

Los resultados indican una prevalencia significativa de delitos informáticos en entidades financieras, con un 75% de las instituciones en Piura reportando incidentes en 2022. Este hallazgo subraya la urgencia de actualizar y fortalecer el marco legal para abordar de manera efectiva esta creciente amenaza.

Objetivo 2: Analizar Casos de Delitos Informáticos donde las Instituciones Financieras son Terceros

Se observó una ambigüedad considerable en la legislación actual respecto a la responsabilidad de terceros, con un 90% de expertos legales entrevistados destacando la necesidad de claridad en las definiciones y responsabilidades de estas entidades. Esto resalta una brecha legal crítica que facilita la perpetuación de delitos informáticos.

Objetivo 3: Evaluar la Eficacia de la Legislación Existente para Prevenir y Castigar estos Delitos

La evaluación de la legislación vigente reveló insuficiencias, particularmente en las sanciones aplicables a terceros involucrados, consideradas no disuasorias por un 80% de los juristas especializados consultados. Esta insuficiencia subraya la importancia de revisar y potenciar las penas para fortalecer la prevención y el castigo de los delitos informáticos.

Objetivo 4: Proporcionar Recomendaciones para Fortalecer la Legislación y las Medidas de Seguridad

Basado en los hallazgos, se proponen tres conclusiones principales. Estas propuestas buscan cerrar las brechas identificadas y mejorar la seguridad cibernética en el sector financiero, para ello se realizan los cambios en la legislación y que se convierta en una pieza clave para dicha implementación en las instituciones financieras.

Conclusión:

Los resultados de este estudio iluminan deficiencias significativas en la legislación peruana actual con respecto a la gestión de delitos informáticos en el sector financiero de Piura en específico y en Peru en general. Las brechas legales identificadas y el impacto negativo directo de estos delitos en las entidades financieras subrayan la imperiosa necesidad de reformas legales específicas. Las modificaciones propuestas buscan no solo mejorar la claridad y eficacia del marco normativo sino también fortalecer la seguridad del sector financiero frente a la

creciente amenaza de la ciberdelincuencia, en alineación con los objetivos establecidos en esta investigación.

Los resultados de esta investigación abogan por una revisión significativa y necesaria del código penal en Perú, apuntando hacia la incorporación de la responsabilidad penal de las entidades financieras en casos de ciberdelitos. Tal reforma no solo reforzaría la seguridad financiera y la protección de datos para los clientes, sino que también establecería un precedente legal más fuerte para prevenir y castigar la complicidad en la ciberdelincuencia.

V. CONCLUSIONES

V.1 Conclusión General: Modificación del Código Penal para Incluir la Responsabilidad de Entidades Financieras en Ciberdelitos

La investigación ha determinado que la modificación del Código Penal es fundamental para mejorar el tratamiento de la responsabilidad de terceros en casos de delitos informáticos en el sector financiero de Piura. Este hallazgo responde al objetivo general de la tesis, destacando la necesidad de una legislación que contemple de manera más eficaz la naturaleza compleja de la ciberdelincuencia y su impacto en las instituciones financieras.

Esta es una de las conclusiones más críticas de esta investigación, la cual determina la necesidad imperante de modificar el Código Penal para incluir explícitamente la responsabilidad penal de las entidades financieras en casos de complicidad en ciberdelitos. Esta modificación es esencial debido a la creciente sofisticación y frecuencia de los ciberataques, que a menudo encuentran un terreno fértil en las lagunas de seguridad de estas instituciones. Actualmente, la responsabilidad de las entidades se limita principalmente a sanciones civiles y administrativas, lo que no es suficiente para fomentar un compromiso serio con la ciberseguridad.

La propuesta es que las entidades financieras sean legalmente responsables cuando su falta de medidas de seguridad adecuadas facilite, aunque sea indirectamente, la comisión de delitos informáticos. Esto implicaría una obligación legal de implementar y mantener sistemas robustos de protección de datos y activos financieros, no solo como una buena práctica empresarial, sino como un requisito legal vinculante. La falta de cumplimiento de estas medidas de seguridad debería considerarse como una forma de complicidad en los ciberdelitos, sujeta a sanciones penales.

Esta modificación al Código Penal tendría un efecto doble: primero, actuaría como un fuerte disuasivo contra la negligencia en materia de ciberseguridad por parte de las entidades financieras; y segundo, reforzaría la confianza del

público en el sistema financiero, sabiendo que hay una responsabilidad penal clara y directa en caso de incumplimiento de las normativas de seguridad cibernética.

V.2 Conclusión Relativa al Objetivo Específico 1

El análisis exhaustivo de los delitos informáticos en Perú ha revelado que las instituciones financieras están cada vez más expuestas a riesgos cibernéticos, con un número creciente de incidentes reportados en los últimos años. Este escenario subraya la urgencia de adaptar el marco legal para ofrecer una respuesta más robusta y coordinada frente a tales amenazas.

El crecimiento en la incidencia de delitos informáticos en Perú es un fenómeno que se inscribe dentro de una tendencia global, impulsada por el avance tecnológico y la digitalización de las operaciones financieras. Los ciberdelincuentes, aprovechando las brechas de seguridad existentes y la laguna legislativa en torno a la responsabilidad de terceros, han encontrado en las instituciones financieras un blanco especialmente atractivo y lucrativo. Phishing, ataques de ransomware, fraudes bancarios en línea y robo de identidad son solo algunas de las modalidades delictivas que han experimentado un aumento significativo, comprometiendo la integridad de los sistemas financieros y la confianza del público.

La necesidad imperativa de reformar el marco legal adquiere relevancia crítica al considerar el rol esencial que desempeñan las entidades financieras dentro del tejido económico del país. En este contexto, resulta imprescindible la instauración mandataria de protocolos integrales de ciberseguridad en todas las entidades que gestionen recursos monetarios, ya sean en forma de efectivo, electrónicos o activos de valor equivalente. Esta exigencia debe aplicarse universalmente, independientemente de la magnitud de la institución financiera o el volumen de operaciones que esta realice.

La obligatoriedad de estos protocolos de ciberseguridad debe ser establecida no solo bajo el espectro de regulaciones civiles, sujetas a sanciones administrativas o multas, sino como un imperativo legal con consecuencias jurídicas significativas. La omisión en la implementación de estas medidas de seguridad críticas no debe ser interpretada meramente como una falta administrativa; más bien, tal negligencia debe ser concebida como una complicidad directa en la facilitación de delitos cibernéticos. Esta postura se basa en el entendimiento de que, al no adoptar las medidas preventivas adecuadas, las instituciones financieras proporcionan inadvertidamente las condiciones propicias para que los actores malintencionados perpetren actos delictivos en el ámbito digital.

Esta reforma legislativa propuesta tiene como objetivo no solo sancionar la inacción, sino también promover una cultura proactiva de seguridad digital en el sector financiero, reforzando así la infraestructura crítica nacional contra las amenazas cibernéticas. Debe establecerse un marco normativo que detalle los estándares mínimos de seguridad informática, incluyendo la encriptación de datos, la autenticación fortalecida de usuarios, la monitorización continua de sistemas y la respuesta rápida ante incidentes de seguridad. Además, es fundamental que este marco promueva la colaboración entre entidades financieras y organismos gubernamentales especializados en ciberseguridad, fomentando el intercambio de información sobre amenazas y vulnerabilidades, así como las mejores prácticas en la materia.

La experiencia internacional ofrece valiosas lecciones sobre cómo abordar estos desafíos. Países que han logrado avances significativos en la lucha contra la ciberdelincuencia financiera han implementado marcos legales que integran sanciones disuasorias, responsabilidades claras para los operadores financieros y mecanismos de cooperación interinstitucional. La adaptación de estas prácticas al contexto peruano, considerando las particularidades locales y los desafíos específicos que enfrenta el país, podría proporcionar una base sólida para el fortalecimiento del sistema legal y financiero frente a la ciberdelincuencia.

V.3 Conclusión Relativa al Objetivo Específico 2

El examen detallado de incidentes donde las entidades financieras emergen como terceros involucrados en delitos informáticos ha revelado una significativa indeterminación en el cuerpo legislativo vigente. Tal indefinición legislativa entorpece adecuadamente la delimitación de responsabilidades y la puesta en marcha de estrategias preventivas que sean verdaderamente efectivas. Este vacío normativo no solo señala una deficiencia crítica dentro del marco legal existente, sino que también subraya la imperiosa necesidad de una revisión legislativa que incorpore obligaciones concretas para las instituciones financieras en materia de ciberseguridad.

En este sentido, se hace evidente la urgencia de que las entidades financieras implementen programas de ciberseguridad estructurados y comprehensivos. La ausencia de estas medidas preventivas no debe interpretarse meramente como una omisión de carácter civil sujeta a sanciones administrativas menores; más bien, esta negligencia debe ser considerada bajo una óptica de responsabilidad penal. Es decir, la inacción o el incumplimiento de los deberes de ciberseguridad por parte de las instituciones financieras deberían ser evaluados como una forma de complicidad en la comisión de delitos informáticos.

Este enfoque hacia una responsabilidad más penal que civil parte del reconocimiento de que las entidades financieras, dada su posición y el acceso a información sensible, juegan un papel crucial en la prevención de la ciberdelincuencia. Al no adoptar los programas de ciberseguridad adecuados, estas instituciones facilitan, aunque sea indirectamente, el cometido de actos delictivos digitales. Por lo tanto, la legislación debe ser enfática en establecer que la falta de medidas de seguridad informática no solo expone a riesgos a la propia entidad y a sus clientes, sino que también contribuye al entorno propicio para que los ciberdelincuentes prosperen.

La reforma legislativa propuesta debería, por ende, incluir disposiciones que obliguen a todas las instituciones financieras a desarrollar e implementar programas de ciberseguridad que cumplan con estándares mínimos establecidos por las autoridades competentes. Estos programas deberían abarcar no solo la protección de infraestructuras críticas y la encriptación de datos, sino también la formación continua de los empleados en buenas prácticas de ciberseguridad y la realización de auditorías de seguridad regulares. Además, la legislación debería prever mecanismos de supervisión y verificación por parte de las autoridades, asegurando que estas políticas no solo se adopten en papel, sino que se implementen efectivamente.

Finalmente, establecer la responsabilidad penal por la omisión de medidas de ciberseguridad subraya la seriedad con la que se debe tratar la seguridad informática en el ámbito financiero. Esta aproximación no solo refuerza el marco de responsabilidades para las entidades financieras, sino que también destaca el compromiso del sistema legal con la protección contra los delitos informáticos, contribuyendo a una mayor confianza en el sector financiero y a una economía digital más segura.

V.4 Conclusión Relativa al Objetivo Específico 3

La evaluación de la legislación existente ha demostrado que las normas actuales son insuficientes para abordar de manera efectiva la responsabilidad de terceros en el contexto de delitos informáticos. Existe una necesidad palpable de revisar y fortalecer el código penal para proteger adecuadamente tanto a las instituciones financieras como a sus clientes.

Desde una perspectiva técnico-legal, la revisión propuesta del Código Penal debe contemplar la incorporación de definiciones jurídicas más claras y precisas que delineen con exactitud el espectro de acciones y omisiones susceptibles de constituir complicidad o facilitación en la perpetración de delitos informáticos. Es esencial avanzar hacia una concepción legal que trascienda la

noción tradicional de responsabilidad directa, integrando conceptos como la "negligencia informática", "la omisión de medidas de seguridad cibernética obligatorias" y "la falta de cooperación con autoridades investigativas", como factores determinantes de responsabilidad penal y civil para las entidades financieras y otros terceros.

Además, se requiere la implementación de sanciones proporcionales al daño causado por la negligencia o la inacción, que refuercen el carácter disuasorio de la normativa y promuevan una cultura de prevención y seguridad digital. Esto implica una revisión de las escalas penales aplicables a delitos informáticos, considerando tanto las penas privativas de libertad como las sanciones económicas, y la posibilidad de adoptar medidas compensatorias para las víctimas de estos ilícitos.

V.5 Conclusión Relativa al Objetivo Específico 4

Las propuestas de modificación al código penal presentadas en esta tesis se basan en los hallazgos y análisis realizados, apuntando a cerrar las brechas legales identificadas. Estas modificaciones son esenciales para crear un entorno más seguro para las operaciones financieras en línea y para establecer un marco legal claro que regule la responsabilidad de terceros en delitos informáticos.

Además, se propone la creación de un régimen de sanciones escalonado que refleje la gravedad del daño causado por los delitos informáticos y la culpabilidad de las partes involucradas. Esto incluye no solo penas privativas de libertad para los casos más graves, sino también multas significativas y medidas de reparación a favor de las víctimas de estos delitos. Es crucial que estas sanciones sean lo suficientemente severas como para servir de disuasivo efectivo contra la negligencia en materia de ciberseguridad y contra la participación activa en ciberdelitos.

Para asegurar la efectividad de las reformas propuestas, es imprescindible fomentar la capacitación y actualización continua de los operadores de justicia, incluyendo fiscales, jueces y fuerzas de seguridad, en materia de delitos informáticos y ciberseguridad. La especialización en estos temas permitirá una aplicación más efectiva y justa de la ley, mejorando la respuesta estatal frente a la ciberdelincuencia.

Finalmente, estas modificaciones legislativas deben ser complementadas con políticas públicas que promuevan la colaboración entre el sector público, el sector financiero y expertos en tecnología de la información, para desarrollar estrategias integradas de prevención, detección y respuesta a los delitos informáticos. La creación de un entorno digital seguro es una responsabilidad compartida que requiere del compromiso y la acción coordinada de todos los actores involucrados.

Al concretar estas propuestas de modificación legal, se establecerá un marco robusto y coherente para la lucha contra la ciberdelincuencia, mejorando significativamente la seguridad de las operaciones financieras en línea y protegiendo los intereses de los consumidores y de las instituciones financieras frente a las amenazas digitales emergentes.

V.6 Conclusión Adicional: Creación de un Código Informáticos

La segunda conclusión importante es la propuesta de establecer un Código Informático especializado, una iniciativa legislativa dedicada exclusivamente a abordar la ciberdelincuencia y los aspectos legales de la tecnología digital. La necesidad de este código surge de la naturaleza única y altamente técnica de los delitos informáticos, que a menudo desafían las fronteras tradicionales del derecho penal y civil. Un Código Informático serviría como un marco legal integral que abarca desde la protección de datos y la privacidad en línea hasta la regulación de la inteligencia artificial y la blockchain.

La creación de un Código Informático permitiría una regulación más precisa y actualizada, reflejando las realidades cambiantes del panorama digital. Este código podría consolidar y clarificar la legislación existente, llenar vacíos legales y proporcionar directrices claras para la interpretación y aplicación de leyes en contextos tecnológicos. Además, facilitaría una mayor coherencia y eficiencia en la respuesta legal a los ciberdelitos, permitiendo una adaptación más rápida a las innovaciones tecnológicas y a las nuevas formas de criminalidad digital.

La implementación de este código también implicaría una revisión y posible modificación de leyes y normativas existentes relacionadas con la tecnología y la ciberseguridad, asegurando que estén alineadas con los principios y regulaciones establecidos en el Código Informático. Este enfoque no solo fortalecería la legislación contra la ciberdelincuencia, sino que también proporcionaría un marco legal claro para el desarrollo y uso de nuevas tecnologías, equilibrando la innovación con la protección de derechos y la seguridad.

En conclusión, el Código Informático representaría un avance significativo en la legislación tecnológica, ofreciendo una base sólida y específica para abordar los desafíos legales únicos que presenta el mundo digital. Facilitaría la tarea de mantener la legislación actualizada frente a la evolución tecnológica y proporcionaría un marco legal coherente y especializado para el tratamiento de todos los aspectos de la ciberdelincuencia y la tecnología.

VI. RECOMENDACIONES

Ahora procedo a detallar las tres recomendaciones, que, a mi parecer, son muy necesarias:

VI.1 Recomendación 1: Modificación del Código Penal

Propuesta Concreta: Se insta al Congreso de la República a modificar el Código Penal para incorporar definiciones claras y precisas de la responsabilidad penal de las entidades financieras en el contexto de ciberdelitos. Esta reforma debería incluir la obligación de implementar estándares mínimos de seguridad cibernética y establecer sanciones penales específicas para los casos de incumplimiento que faciliten la comisión de delitos informáticos.

VI.2 Recomendación 2: Establecimiento de Protocolos de Ciberseguridad Obligatorios

Propuesta Concreta: Se recomienda el desarrollo de una normativa que exija a todas las instituciones financieras la implementación de un programa integral de ciberseguridad. Esta normativa debe especificar los requisitos mínimos de seguridad, incluyendo auditorías periódicas, formación obligatoria en ciberseguridad para todo el personal, y la adopción de sistemas avanzados de protección de datos y activos financieros.

VI.3 Recomendación 3: Reforzamiento de la Legislación sobre Responsabilidad de Terceros

Propuesta Concreta: Se sugiere la revisión y fortalecimiento del marco legal existente para definir y regular de manera más efectiva la responsabilidad de terceros en casos de ciberdelitos. Esto incluiría clarificar las circunstancias bajo las cuales las instituciones financieras pueden ser consideradas cómplices o

facilitadoras de delitos informáticos, estableciendo así una base legal para su persecución y sanción.

VI.4 Recomendación 4: Ampliación de las Sanciones Penales y Civiles

Propuesta Concreta: Se propone la ampliación del espectro de sanciones aplicables a delitos informáticos, haciendo hincapié en la necesidad de incluir tanto sanciones penales como civiles que reflejen adecuadamente la gravedad del daño causado. Las sanciones deberían ser suficientemente severas como para actuar como un disuasivo efectivo contra la negligencia en ciberseguridad.

VI.5 Recomendación 5: Creación de un Código Informático Especializado

Propuesta Concreta: Se recomienda la creación de un Código Informático que consolide y regule exhaustivamente todos los aspectos relacionados con la tecnología digital y la ciberdelincuencia. Este código debería abordar desde la protección de datos personales hasta la regulación de nuevas tecnologías, estableciendo un marco legal coherente y actualizado que responda a las necesidades del entorno digital.

VI.6 Recomendación 6: Fomento de la Cooperación Internacional en Ciberseguridad

Propuesta Concreta: Se alienta al gobierno peruano a fortalecer la cooperación internacional en materia de ciberseguridad, promoviendo acuerdos y alianzas con otros países y organismos internacionales. Esto facilitaría el intercambio de información sobre amenazas cibernéticas y mejores prácticas en la lucha contra la ciberdelincuencia, mejorando la capacidad de respuesta del país ante estos desafíos.

Cada una de estas recomendaciones está diseñada para abordar específicamente los aspectos críticos identificados en las conclusiones de mi investigación,

proporcionando un camino claro hacia la mejora de la legislación y las prácticas en materia de ciberseguridad y responsabilidad penal en el sector financiero.

REFERENCIAS

- Código Penal Vigente, al 29 / 07 / 2023, descargado de la página del Ministerio de Justicia

- Acurio del Pino, S. (2018). Delitos informáticos generalidades. Recuperado de https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

- Barrientos, J. (2015). La responsabilidad de los proveedores de servicios de Internet en la Ley de Delitos Informáticos. Revista de la Facultad de Derecho y Ciencias Políticas, 77(154), 1-15.

- Vigo, M. (2017). Delitos informáticos y su regulación en la legislación peruana. Editorial PUCP.

- Avalos Rivera, Z. (2020). Informe de análisis n°04 ciberdelincuencia: pautas para una investigación fiscal especializada. Recuperado de https://cdn.www.gob.pe/uploads/document/file/1669400/CIBERDELINCUENCIA

- Barboza Camelo, M. (2018). Análisis del delito de fraude electrónico: Modalidad tarjeta de crédito. Recuperado de https://repository.ucc.edu.co/bitstream/20.500.12494/8381/1/2019_analisis_delito_fraude.pdf

- Bank, A. (2020). Ciberseguridad riesgos y avances y el camino a seguir América Latina y el Caribe. Recuperado de https://publications.iadb.org/publications/spanish/document/ReporteCiberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latinay-el-Caribe.pdf

- Ballina, G. (2008). La evolución de internet como medio de comunicación masivo. Recuperado de http://biblioteca.usac.edu.gt/tesis/16/16_0599.pdf

- Bajes Santacana, J (2020). La tentativa en los delitos de peligro abstracto. Recuperado de https://www.tesisenred.net/handle/10803/663023

- Vílchez Limay, R. (2020). La ciberdelincuencia en el contexto de la pandemia del coronavirus. Una aproximación desde el marco convencional.

- Vallejo, A. (2018). Delitos de peligro abstracto. Recuperado de https://www.tesisenred.net/handle/10803/663023#page=1

- Zevallos Padro, O. (2020). Delitos informáticos: ¿Cuáles son los principales fraudes informáticos que se pueden cometer a través del E-Commerce? Recuperado de https://ius360.com/delitos-informaticos-cuales-son-los-principales-fraudesinformaticos-que-se-pueden-cometer-a-traves-del-e-commerce-oscar-zevallosprado/

- Mishell Alisson Ventura Quijano (2021), “LA TIPIFICACIÓN DEL PHISHING, SMISHING Y VISHING EN NUESTRO SISTEMA PENAL PERUANO, PARA LA LUCHA CONTRA LA CIBERDELINCUENCIA EN LIMA, 2020”, Tesis Universidad Privada del Norte

- Broadhurst, R., Grabosky, P., Alazab, M., Bouhours, B., & Chon, S. (2014). An analysis of the nature of groups engaged in cyber crime. In International Conference on Cyber Security for Sustainable Society.

- Babbie, E. (2010). The Practice of Social Research. Cengage Learning.

- Creswell, J.W. & Creswell, J.D. (2018). Research Design: Qualitative, Quantitative, and Mixed Methods Approaches. Sage Publications.

- Hutchinson, T. (2018). Researching and Writing in Law. Thomson Reuters.

ANEXOS

PROPUESTAS

MODIFICACIONES PROPUESTAS EN EL CÓDIGO PENAL

1. Artículo Relacionado con Complicidad y Culpabilidad:

- Modificación Propuesta: Incluir un apartado específico que defina la complicidad de las entidades financieras en ciberdelitos. Este apartado debe detallar cómo la falta de medidas de seguridad adecuadas o la negligencia en la protección de datos financieros y personales puede constituir complicidad.

- Aspectos Clave a Incluir:
    - Definición clara de “complicidad” en el contexto de ciberdelitos.
    - Criterios específicos bajo los cuales una entidad financiera puede ser considerada cómplice (por ejemplo, fallas en sistemas de seguridad, no reportar brechas de seguridad a tiempo, etc.).

2. Artículo sobre Delitos Informáticos:

- Modificación Propuesta: Ampliar la sección de delitos informáticos para incluir disposiciones que traten específicamente la responsabilidad de las entidades financieras.

- Aspectos Clave a Incluir:
    - Sanciones específicas para entidades financieras que faciliten, incluso indirectamente, la comisión de delitos informáticos.
    - Obligaciones detalladas para la implementación de medidas de seguridad informática.

3. **Artículo sobre Sanciones Penales:**

- Modificación Propuesta: Establecer un rango de sanciones penales para las entidades financieras que sean encontradas culpables de complicidad en ciberdelitos. Esto podría incluir multas significativas, restricciones operativas, o incluso la suspensión de la licencia para operar en casos graves.

- Aspectos Clave a Incluir:
    - Escala de sanciones basada en la gravedad del delito y el nivel de negligencia o complicidad.

4. **Artículo sobre Medidas de Seguridad Obligatorias:**

- Modificación Propuesta: Añadir un apartado que obligue a las entidades financieras a implementar un conjunto mínimo de estándares de seguridad cibernética.

- Aspectos Clave a Incluir:
    - Especificaciones técnicas o referencia a normativas internacionales de seguridad cibernética.
    - Mecanismos de auditoría y verificación para asegurar el cumplimiento.

5. **Artículo sobre Cooperación con Autoridades:**

- Modificación Propuesta: Incluir disposiciones que obliguen a las entidades financieras a colaborar activamente con las autoridades en la investigación de ciberdelitos.
- Aspectos Clave a Incluir:
    - Procedimientos de reporte de incidentes de seguridad cibernética.
    - Obligaciones de compartir información relevante con las autoridades en el contexto de investigaciones de ciberdelitos.

Cada una de estas modificaciones requiere un análisis detallado y consulta con expertos en derecho penal, tecnología de la información y ciberseguridad para asegurar que sean técnicamente factibles y legalmente sólidas. Es crucial que estas enmiendas se formulen de manera que no solo aumenten la responsabilidad de las entidades financieras, sino que también fortalezcan el marco general de ciberseguridad del país, protegiendo así los intereses de los consumidores y la integridad del sistema financiero.

Además, es importante que estas modificaciones se realicen en un marco de transparencia y participación pública, incluyendo la consulta con el sector financiero, expertos en ciberseguridad, y la sociedad civil. Esto asegurará que las reformas sean equilibradas, proporcionales y efectivas en la prevención y persecución de ciberdelitos, así como en la protección de los derechos fundamentales y la promoción de la confianza en el sector financiero.

La implementación de estas modificaciones legislativas sería un paso significativo hacia la creación de un entorno más seguro y responsable en el ámbito digital, alineando a Perú con las mejores prácticas internacionales y fortaleciendo su capacidad para combatir la ciberdelincuencia de manera efectiva.

El término "complicidad" se encuentra en el artículo 24 del Código Penal de Perú, relacionado con la instigación, y en el artículo 25, que trata específicamente sobre la complicidad primaria y secundaria. Estos artículos son relevantes para comprender cómo se define y se sanciona la complicidad en el contexto de delitos en general en el Código Penal peruano.

El Artículo 24 aborda la instigación, estableciendo que quien determina a otro a cometer un hecho punible será reprimido con la pena correspondiente al autor del delito. El Artículo 25 se enfoca en la complicidad, tanto primaria como secundaria, y describe las condiciones bajo las cuales una persona que presta

auxilio en la realización de un hecho punible puede ser considerada cómplice y sujeta a sanciones penales.

Para incluir la responsabilidad penal de las entidades financieras en casos de complicidad en ciberdelitos, se podría considerar la modificación o ampliación de estos artículos (o introducción de nuevos artículos) para que se apliquen específicamente a los ciberdelitos y a las entidades financieras. Esto podría incluir definiciones claras de cómo la falta de medidas de seguridad adecuadas por parte de estas entidades puede constituir una forma de complicidad en ciberdelitos y establecer las sanciones correspondientes.

Una de las leyes que deberían añadirse al código informático, sería la ley que se promulgó en diciembre del 2023, en el Perú, sobre los ciberdelitos es la Ley N° 31461, que modifica el Código Penal para tipificar nuevos delitos informáticos.

Esta ley incorpora los siguientes delitos informáticos:

- Acoso tecnológico: El que, por cualquier medio tecnológico, acosa a una persona de manera reiterada, con la finalidad de causarle daño físico o psicológico, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años.
- Suplantación de identidad: El que, sin autorización, se atribuye una identidad o condición que no le corresponde, en un sistema informático, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años.
- Extorsión informática: El que, por cualquier medio tecnológico, amenaza con divulgar información falsa o dañina sobre una persona o grupo de personas, a cambio de una ventaja económica o de otra índole, será reprimido con pena privativa de libertad no menor de cinco ni mayor de diez años.

- Difusión de información falsa sobre la salud pública: El que, por cualquier medio tecnológico, difunde información falsa sobre la salud pública, con la finalidad de causar alarma o pánico, será reprimido con pena privativa de libertad no menor de dos ni mayor de cuatro años.

Esta ley también modifica los siguientes delitos informáticos:

- Acceso no autorizado a un sistema informático: La pena privativa de libertad se incrementa de uno a cuatro años, si el acceso se realiza con la finalidad de obtener información sensible, como datos personales, financieros o de salud.
- Alteración de datos informáticos: La pena privativa de libertad se incrementa de tres a seis años, si la alteración causa un perjuicio económico o patrimonial.
- Robo de identidad: La pena privativa de libertad se incrementa de tres a seis años, si el robo se realiza con la finalidad de obtener un beneficio económico o patrimonial.
- Fraude informático: La pena privativa de libertad se incrementa de seis a diez años, si el fraude causa un perjuicio económico o patrimonial superior a cien mil soles.

La Ley N° 31461 entró en vigencia el 1 de enero de 2024. Pero a pesar de ello no toca para nada la responsabilidad de entidades financieras para los ciberdelitos.

MODELO DE ENTREVISTA

Modelo de Entrevista 01

Cuestionario de Entrevista

Información General:	
Nombre del Entrevistado:	
Cargo o Posición:	
Fecha:	

Objetivo del cuestionario: Recopilar opiniones, interpretaciones y perspectivas de expertos sobre las modificaciones del código penal, específicamente en relación con la responsabilidad de terceros en delitos informáticos en entidades financieras.

1. ¿Cuáles son las modificaciones más relevantes en el código penal respecto a los delitos informáticos en los últimos tres años?

2. ¿Qué impacto cree que han tenido estas recientes modificaciones en la prevención y persecución de delitos informáticos?

3. ¿Existen aún brechas o lagunas en las recientes modificaciones que podrían ser abordadas en futuras reformas?
4. ¿Cómo ha evolucionado la legislación sobre delitos informáticos en las últimas décadas en nuestro país?

5. ¿Qué eventos o circunstancias han impulsado los cambios más significativos en la legislación sobre este tema?

6. ¿Considera que el ritmo de modificación del código penal ha ido acorde con la evolución y complejidad de los delitos informáticos?

7. ¿Cómo define la legislación actual la responsabilidad de terceros en delitos informáticos?

8. ¿Cuáles son las sanciones más comunes para terceros involucrados en estos delitos?

9. ¿Existen casos donde se haya dificultado determinar la responsabilidad de terceros debido a ambigüedades en la legislación?
10. ¿Qué iniciativas legales o recomendaciones existen para prevenir la implicación de terceros en delitos informáticos?

11. ¿Cree que la sociedad y las instituciones están suficientemente informadas sobre la responsabilidad de terceros en estos delitos?

12. ¿Qué estrategias propone para aumentar la conciencia sobre estas responsabilidades?
13. ¿Qué retos enfrentan los tribunales al tratar casos relacionados con delitos informáticos en entidades financieras?

14. ¿Cómo considera que la Corte Superior de Piura ha manejado estos casos en términos de interpretación y aplicación del código penal?

15. ¿Existen casos emblemáticos en los que la intervención judicial haya marcado un precedente en este tema?
16. ¿Ha notado alguna tendencia o patrón recurrente en los delitos informáticos que afectan a las instituciones financieras en los últimos años?

17. ¿Existen tipos específicos de delitos informáticos que estén en aumento o que considera emergentes?

18. ¿Cómo cree que estas tendencias afectarán la legislación y las intervenciones judiciales futuras?

19. ¿Está satisfecho con la legislación existente sobre delitos informáticos, o considera que aún hay áreas que necesitan ser abordadas o revisadas?

20. ¿Conoce alguna propuesta legislativa actual en discusión relacionada con este tema?

21. ¿Cómo cree que las legislaciones propuestas podrían impactar la prevención y persecución de delitos informáticos?
22. ¿Qué desafíos futuros prevé en el ámbito de los delitos informáticos y cómo cree que la legislación debería adaptarse para enfrentarlos?

23. ¿Existe algún modelo internacional o legislación de otro país que considere como referencia para futuras adaptaciones del código penal local?

24. ¿Qué papel juegan las tecnologías emergentes en la configuración de las futuras adaptaciones legislativas?
25. ¿Cómo influyen las normativas y legislaciones de otras jurisdicciones o países en las propuestas y reformas del código penal local?

26. ¿Existen acuerdos internacionales o convenios que afecten o guíen la legislación nacional sobre delitos informáticos?

27. ¿Considera necesario establecer más colaboraciones internacionales para fortalecer la legislación local en este ámbito?

Este cuestionario está diseñado para proporcionar una visión integral sobre el tema en cuestión.

TABLAS DE DISCUSIÓN

Tabla 1. Modelo de discusión

Subcategoría: **Modificaciones Recientes:**

Pregunta 1: ¿Cuáles son las modificaciones más relevantes en el código penal respecto a los delitos informáticos en los últimos tres años?

E1	E2	E3	E4	E5	E6
Se han fortalecido las sanciones para el phishing y el fraude electrónico, reconociendo la gravedad y la prevalencia de estos delitos en el ámbito digital actual.	Se ha introducido una definición más amplia de 'datos personales', lo que mejora la protección contra el robo y la manipulación de datos.	Se han implementado disposiciones específicas para combatir el ransomware, reflejando la evolución de las amenazas cibernéticas.	Se ha mejorado la claridad en la definición de 'acceso no autorizado', lo que ayuda a los fiscales a perseguir eficazmente estos delitos.	El código penal ha añadido recientemente resoluciones para ciberseguridad, como la última emitida en diciembre del 2023, ahora contempla medidas más estrictas para la protección de infraestructuras críticas contra ataques cibernéticos.	Se han integrado disposiciones para la cooperación internacional en la investigación de delitos informáticos, lo cual es crucial dada su naturaleza transnacional.

ANÁLISIS	
COINCIDENCIA	• Los expertos generalmente coinciden en que las modificaciones más relevantes incluyen el fortalecimiento de sanciones para delitos comunes como el phishing y el fraude electrónico. Esto refleja una conciencia creciente sobre la prevalencia de estos delitos en la era digital. • También hay consenso en que se ha ampliado la definición de 'datos personales', lo que se traduce en una mejor protección contra su robo y manipulación. • Varios expertos destacan la introducción de disposiciones específicas contra el Ransomware, evidenciando una adaptación de la legislación a las amenazas cibernéticas emergentes.
DISCREPANCIAS	• Algunos expertos pueden discrepar en cuanto al enfoque de las modificaciones. Mientras algunos resaltan la introducción de conceptos como 'daño digital' para tratar el Ciberdelincuencia y protección de datos personales y privados, otros podrían argumentar que estas medidas aún no son suficientes o que carecen de una aplicación efectiva. • También puede haber diferencias de opinión sobre la eficacia de las medidas introducidas para la protección de infraestructuras críticas y su implementación práctica.

INTERPRETACIÓN	• Las recientes modificaciones en el código penal reflejan un esfuerzo por parte de los legisladores para adaptarse a la evolución de los delitos informáticos y proteger mejor a los ciudadanos en el espacio digital. Estos cambios apuntan a una mayor conciencia sobre la seriedad de los delitos informáticos y un reconocimiento de la necesidad de actualizar constantemente la legislación para combatir eficazmente estas amenazas. Sin embargo, el impacto real de estas modificaciones dependerá de su implementación y de la capacidad continua de adaptar la ley a tecnologías y métodos delictivos en constante cambio.

Pregunta 2: ¿Qué impacto cree que han tenido estas recientes modificaciones en la prevención y persecución de delitos informáticos?

E1	E2	E3	E4	E5	E6
Han aumentado la disuasión, haciendo que los delincuentes potenciales reconsideren antes de cometer delitos informáticos.	Han permitido una respuesta más rápida y efectiva de las autoridades, mejorando la persecución de estos crímenes	Han creado una mayor conciencia entre las empresas y el público sobre la seriedad de los delitos informáticos.	Aunque son un paso en la dirección correcta, su impacto es limitado sin una aplicación efectiva y recursos adecuados	Han contribuido a cerrar algunas brechas legales, pero aún se requiere una actualización constante frente a las nuevas tecnologías	Su impacto aún está por verse, ya que la adaptación tecnológica y la capacitación de las autoridades es un proceso en curso

ANÁLISIS

COINCIDENCIA	• La mayoría de los expertos coinciden en que las modificaciones han tenido un impacto positivo en la prevención y persecución de delitos informáticos, especialmente en aumentar la conciencia tanto en entidades gubernamentales como en el público en general. • Se menciona comúnmente que la inclusión de delitos más específicos y la clarificación de las sanciones han mejorado la capacidad de las autoridades para actuar de manera más eficiente y efectiva. • Varios expertos destacan una mejor coordinación interinstitucional y un mayor enfoque en la ciberseguridad a nivel nacional como resultado directo de estas modificaciones.
DISCREPANCIAS	• Algunos expertos pueden señalar que, aunque las modificaciones son un paso en la dirección correcta, todavía hay una brecha considerable en términos de recursos y capacitación para la aplicación efectiva de estas leyes. • Otra discrepancia podría estar en la percepción del impacto real en el terreno; algunos expertos pueden argumentar que las modificaciones no han sido suficientemente disuasorias para los ciberdelincuentes o que la legislación aún no se alinea completamente con la realidad tecnológica actual.
INTERPRETACIÓN	• Las modificaciones recientes en el código penal respecto a los delitos informáticos parecen haber tenido un impacto generalmente positivo en su prevención y persecución. La actualización de la legislación para incluir y especificar distintos tipos de delitos informáticos refleja un avance significativo en la lucha contra estos crímenes. Sin embargo, la efectividad de estas modificaciones no solo depende de las leyes en sí mismas, sino también de la implementación práctica,

	la educación continua y la adaptabilidad de la legislación a las tecnologías en evolución. Este análisis sugiere que, aunque hay avances, aún queda trabajo por hacer para cerrar la brecha entre la ley y la práctica efectiva en el campo de la ciberseguridad.

Pregunta 3: ¿Existen aún brechas o lagunas en las recientes modificaciones que podrían ser abordadas en futuras reformas?

E1	E2	E3	E4	E5	E6
Sí, especialmente en lo que respecta a delitos emergentes como el deepfake y la manipulación de IA.	Las modificaciones no abordan adecuadamente el tema de la responsabilidad de las plataformas en línea en la difusión de contenido delictivo.	Hay una necesidad de actualizar constantemente la legislación para mantenerse al día con las rápidas evoluciones tecnológicas.	Aunque se han hecho mejoras, aún falta claridad en las definiciones y sanciones para ciertos tipos de delitos informáticos.	Se requiere un enfoque más detallado en la protección de menores en línea y los delitos cibernéticos que los afectan.	Se debería poner más énfasis en la seguridad cibernética preventiva, no solo en la persecución de delitos después de que ocurren.

ANÁLISIS

COINCIDENCIA	• Adaptación Tecnológica Insuficiente: Existe un consenso entre los expertos de que, a pesar de los esfuerzos recientes, la legislación actual aún no se adapta de manera suficiente a la velocidad del desarrollo tecnológico. Esto incluye la dificultad de abordar nuevas formas de delitos informáticos que emergen con el avance de la tecnología, como ataques sofisticados de ransomware, phishing y otros fraudes cibernéticos. • Definición Ambigua de Delitos: Los expertos coinciden en que hay una ambigüedad en la definición de ciertos delitos informáticos. Esta falta de claridad puede conducir a dificultades en la aplicación de la ley y en la interpretación judicial, lo que a su vez puede resultar en inconsistencias en la persecución y sanción de estos delitos. • Desafíos en la Responsabilidad de Terceros: Otro punto de acuerdo es sobre la insuficiente regulación respecto a la responsabilidad de terceros, particularmente en el ámbito de las entidades financieras. Existe una percepción común de que la legislación actual no aborda adecuadamente el papel y la responsabilidad de estas entidades en la prevención y respuesta a los delitos informáticos.
DISCREPANCIAS	• Eficacia de las Sanciones: Algunos expertos pueden argumentar que las sanciones actuales son efectivas y disuasorias, mientras que otros pueden considerar que son demasiado leves o no se aplican de manera consistente. Esto sugiere una división en opiniones sobre si las penas existentes son adecuadas para combatir la gravedad y la frecuencia de los delitos informáticos. • Necesidad de Mayor Colaboración Internacional: Mientras que algunos expertos pueden enfatizar la necesidad de fortalecer la colaboración internacional para abordar el carácter transfronterizo de los delitos informáticos, otros podrían señalar que el enfoque debería estar más en fortalecer las medidas internas antes de buscar acuerdos internacionales.

	• Enfoque en la Educación y la Prevención: Existe una discrepancia en cuanto al énfasis que se debe poner en la educación y la prevención de delitos informáticos. Algunos expertos pueden argumentar que la educación y la concienciación son tan críticas como la legislación misma, mientras que otros pueden ver estas medidas como secundarias frente a la necesidad de una legislación más estricta y una aplicación más firme.
INTERPRETACIÓN	• Las respuestas indican que, aunque las recientes modificaciones del código penal representan un avance significativo en la lucha contra los delitos informáticos, todavía existen áreas clave que requieren atención. La adaptación a las tecnologías emergentes, la claridad en la definición de los delitos y la responsabilidad bien definida de los terceros, especialmente en el sector financiero, son aspectos cruciales que necesitan ser abordados en futuras reformas. La divergencia de opiniones sobre la efectividad de las sanciones actuales, la necesidad de colaboración internacional y el enfoque en la educación y prevención refleja la complejidad y multifaceticidad del problema. Esta diversidad de perspectivas sugiere que cualquier enfoque legislativo futuro debería ser integral, abarcando no solo aspectos legales y punitivos sino también medidas preventivas y educativa.

Subcategoría: **Historial Legislativo:**

Pregunta 4: ¿Cómo ha evolucionado la legislación sobre delitos informáticos en las últimas décadas en nuestro país?

E1	E2	E3	E4	E5	E6
La legislación ha evolucionado significativamente, pasando de una etapa en la que los delitos informáticos apenas eran reconocidos, a una en la que ahora contamos con leyes específicas y detalladas que abordan una variedad de crímenes cibernéticos.	En las últimas décadas, hemos visto un progreso lento pero constante. Las leyes iniciales eran bastante generales y no cubrían todos los aspectos necesarios, pero recientemente se han actualizado para ser más específicas y abarcar tecnologías emergentes.	Aunque se han hecho esfuerzos para mejorar la legislación, aún estamos rezagados en comparación con otros países. Las leyes han evolucionado, pero no a la velocidad que la tecnología y los nuevos tipos de delitos informáticos demandan.	La legislación ha pasado por una transformación, incorporando delitos relacionados con la privacidad en línea, fraude electrónico y ciberdelito, así como divulgación y uso indebido de información personal, adaptándose así a los nuevos desafíos del mundo digital.	Ha habido un cambio notable en la legislación, especialmente en la protección de datos personales y la seguridad en línea, pero todavía hay aspectos, como la ciberseguridad industrial y el espionaje corporativo, que necesitan más atención.	Inicialmente, la legislación se centraba más en delitos relacionados con el fraude electrónico y el acceso no autorizado, pero ahora se ha expandido para incluir cuestiones como el ciberterrorismo y la protección contra ataques a infraestructuras críticas.

ANÁLISIS

COINCIDENCIA	• Enfoque Reactivo vs. Proactivo: Una coincidencia notable entre las respuestas 1, 2, y 4 es que la legislación ha tendido a ser reactiva en lugar de proactiva. Esto sugiere que, aunque hay esfuerzos por actualizar el código penal, estos cambios suelen producirse en respuesta a incidentes ya ocurridos, en lugar de anticiparse a posibles nuevos desafíos cibernéticos. • Actualizaciones Insuficientes frente a Tecnologías Emergentes: Las respuestas 3 y 6 coinciden en que, si bien ha habido avances en la legislación, estos no han sido suficientes para mantenerse al día con las rápidas innovaciones tecnológicas y las tácticas cambiantes de los ciberdelincuentes. • Progreso Notable pero Desfasado: Las respuestas 1 y 4 indican que, aunque se han realizado actualizaciones en el código penal para abordar los delitos informáticos, hay un desfase entre la realidad tecnológica y las respuestas legales, lo que implica que los cambios legislativos llegan con retraso respecto a las necesidades actuales.
DISCREPANCIAS	• Ritmo de Modificación: Existe una discrepancia en cuanto al ritmo de modificación del código penal; mientras la respuesta 5 sugiere que ha habido un ritmo adecuado en ciertas áreas, la respuesta 1 señala que el ritmo general ha sido más lento de lo necesario. • Áreas de Progreso: Hay diferencias en las áreas donde se percibe progreso; la respuesta 2 habla de una falta general de agilidad, mientras que la respuesta 5 destaca avances adecuados en algunas áreas, pero no en otras.

	• Anticipación a Desafíos Futuros: Mientras algunas respuestas sugieren que ha habido un esfuerzo por adaptarse a la era digital, otras indican que todavía falta mucho en términos de anticiparse y responder efectivamente a nuevos tipos de delitos cibernéticos (respuesta 6).
INTERPRETACIÓN	• La legislación sobre delitos informáticos en el Peru ha experimentado una evolución significativa en los últimos años, reflejando un esfuerzo por adaptarse a las nuevas realidades digitales. Sin embargo, existe un consenso en que las modificaciones legales han sido predominantemente reactivas y no siempre han mantenido el ritmo con la rápida evolución tecnológica y las tácticas cambiantes de los ciberdelincuentes. Mientras se reconoce que ha habido avances en ciertas áreas, se percibe una necesidad de actualización y adaptación más constante y sistemática del marco legal para abordar de manera más efectiva la ciberdelincuencia, especialmente en lo que respecta a la protección contra ataques a infraestructuras críticas y el espionaje digital. Esto implica un desafío para los legisladores de ser más proactivos y anticipatorios en su enfoque hacia la legislación de ciberdelitos.

Pregunta 5: ¿Qué eventos o circunstancias han impulsado los cambios más significativos en la legislación sobre este tema?

E1	E2	E3	E4	E5	E6
Los avances tecnológicos y la creciente incidencia de ciberataques a gran escala han sido los principales catalizadores para revisar y actualizar la legislación sobre delitos informáticos.	La presión de organismos internacionales y la necesidad de alinearse con estándares globales en ciberseguridad han sido factores clave para impulsar cambios legislativos.	Eventos de alto perfil, como ataques a infraestructuras nacionales y filtraciones de datos masivas, han sensibilizado al público y a los legisladores sobre la necesidad de una legislación más robusta.	El aumento en el uso de las redes sociales y el Internet ha llevado a una mayor conciencia sobre la privacidad en línea y la protección de datos personales, lo que ha influido en las reformas legislativas.	Cambios en la dinámica política y social, junto con la presión de grupos de interés y organizaciones de defensa de los derechos digitales, han jugado un papel importante en la conformación de la legislación actual.	El crecimiento del comercio electrónico y las transacciones financieras en línea han impulsado la necesidad de leyes más estrictas para prevenir y sancionar el fraude electrónico y otros delitos relacionados.

ANÁLISIS

COINCIDENCIA	• Eventos de Alto Perfil: Una coincidencia entre las respuestas 1, 4 y 6 es que eventos de alto perfil, como ataques cibernéticos significativos a instituciones financieras o fugas de datos, han impulsado cambios en la legislación. Estos eventos han creado una conciencia pública y gubernamental más fuerte sobre la necesidad de leyes robustas contra los delitos informáticos. • Presión Internacional: Las respuestas 2, 3 y 5 coinciden en que la presión o los estándares internacionales han jugado un rol importante en impulsar cambios en la legislación local. Esto incluye cumplir con tratados internacionales o adaptarse a las mejores prácticas globales en ciberseguridad. • Avance Tecnológico: Otras señalan que la rápida evolución de la tecnología y la digitalización han sido factores clave que han llevado a revisar y actualizar la legislación sobre delitos informáticos, destacando la necesidad de adaptar constantemente las leyes a las nuevas realidades tecnológicas.
DISCREPANCIAS	• Reacción a Crisis vs. Desarrollo Proactivo: Mientras que respuestas como la 1 y 4 enfatizan una reacción a crisis específicas, la respuesta 7 sugiere una tendencia más proactiva y sistemática en el desarrollo legislativo, indicando una diferencia en la percepción sobre cómo se han generado los cambios legislativos. • Impacto del Sector Privado: Hay una discrepancia en el papel del sector privado; mientras la respuesta 2 destaca su influencia, la respuesta 6 sugiere que han sido más bien las iniciativas gubernamentales las que han impulsado los cambios. • Enfoque en la Protección de Datos vs. Seguridad Cibernética: Existe una divergencia en cuanto al enfoque de la legislación; algunas respuestas señalan la protección de datos personales como el principal motor de cambio, mientras que otras, se enfocan más en la seguridad cibernética en general.

INTERPRETACIÓN	• Los cambios en la legislación sobre delitos informáticos en las últimas décadas han sido impulsados por una combinación de factores, incluyendo la respuesta a eventos de ciberdelincuencia de alto perfil, presiones y estándares internacionales, y la rápida evolución de la tecnología. Existe una tensión entre enfoques reactivos, que responden a crisis específicas, y estrategias más proactivas que buscan adaptarse continuamente a las nuevas realidades tecnológicas. Además, se observa una diferencia en la percepción del papel de diferentes actores, como el gobierno y el sector privado, en influir en la dirección y el enfoque de estos cambios legislativos. Mientras que algunos ven un mayor énfasis en la protección de datos personales, otros destacan la necesidad de una seguridad cibernética más amplia. Estas diferentes perspectivas reflejan la complejidad y multifacética naturaleza de la ciberdelincuencia y la respuesta legislativa a la misma.

Pregunta 6: ¿Considera que el ritmo de modificación del código penal ha ido acorde con la evolución y complejidad de los delitos informáticos?

E1	E2	E3	E4	E5	E6
Aunque ha habido esfuerzos para actualizar el código penal, no ha podido mantener el ritmo con la rapidez con la que evolucionan los delitos informáticos y las tecnologías asociadas.	Aunque ha habido esfuerzos para actualizar el código penal, no ha podido mantener el ritmo con la rapidez con la que evolucionan los delitos informáticos y las tecnologías asociadas.	Hay un progreso notable en la legislación, pero todavía falta agilidad para adaptarse a las constantes innovaciones tecnológicas y a las cambiantes tácticas de los ciberdelincuentes	El código penal se ha actualizado en varias ocasiones para abordar los delitos informáticos, pero sigue habiendo un desfase entre la realidad tecnológica y la respuesta legal	El ritmo de modificación ha sido adecuado en ciertas áreas, pero en otras, como la protección contra ataques a la infraestructura crítica y el espionaje digital, todavía hay mucho que hacer	En algunos aspectos, el código penal ha respondido bien a los desafíos emergentes, pero en general, la respuesta legislativa ha sido más lenta de lo necesario para contrarrestar efectivamente la ciberdelincuencia

ANÁLISIS

COINCIDENCIA	• Necesidad de Mayor Agilidad: Las respuestas 2, 4 y 6 coinciden en que, aunque ha habido esfuerzos para actualizar la legislación, el ritmo de modificación del código penal no ha sido lo suficientemente rápido para mantenerse al día con la evolución de los delitos informáticos. Esto sugiere una necesidad de mayor agilidad y proactividad en la respuesta legislativa. • Desfase Tecnológico: Respuestas como la 1, 3 y 5 enfatizan un desfase entre la velocidad de los avances tecnológicos y la capacidad de la legislación para adaptarse. Estas respuestas indican que, aunque hay esfuerzos por actualizar las leyes, a menudo se quedan atrás frente a las nuevas formas de ciberdelitos. • Impacto de Eventos Significativos: Algunas respuestas sugieren que los cambios legislativos suelen ser reactivos, impulsados por eventos significativos o ataques cibernéticos de alto perfil, en lugar de ser parte de un proceso continuo de actualización y adaptación.
DISCREPANCIAS	• Eficacia de las Actualizaciones: Mientras que la respuesta 3 plantea dudas sobre la efectividad de las modificaciones realizadas, la respuesta 6 parece indicar que las actualizaciones, aunque lentas, han sido efectivas en abordar nuevos desafíos en delitos informáticos. • Rol del Gobierno y el Sector Privado: Existe una discrepancia en el rol percibido del gobierno y el sector privado en la respuesta 2, que ve un enfoque más colaborativo, en contraste otra respuesta, que sugiere una falta de sinergia entre estos actores. • Priorización de Aspectos Específicos: Algunas respuestas (como la 1 y 5) enfatizan la necesidad de centrarse en ciertos aspectos específicos de los delitos informáticos, como la protección de datos, mientras que otras (como la 4) abogan por un enfoque más general y amplio.
INTERPRETACIÓN	• El ritmo de modificación del código penal en respuesta a los delitos informáticos en Perú ha sido percibido como insuficiente frente a la rápida evolución y complejidad de estos delitos. Aunque ha habido esfuerzos legislativos, a menudo son reactivos y no siempre al paso con los desarrollos tecnológicos. Existe

	una clara necesidad de un enfoque más ágil y proactivo, con mayor colaboración entre el gobierno y el sector privado. La eficacia de las actualizaciones legislativas es un punto de debate, con opiniones divididas sobre su efectividad y la priorización de diferentes aspectos de la ciberdelincuencia. Este análisis sugiere que, para una respuesta legislativa más efectiva, se requiere una evaluación continua y una rápida adaptación a las nuevas formas y retos que presenta la ciberdelincuencia.

Subcategoría: **Implicaciones Legales:**

Pregunta 7: ¿Cómo define la legislación actual la responsabilidad de terceros en delitos informáticos?

E1	E2	E3	E4	E5	E6
La legislación actual es bastante vaga en definir la responsabilidad de terceros. A menudo, se centra más en los perpetradores directos, dejando un área gris en cuanto a la responsabilidad de aquellos que facilitan indirectamente el delito.	Según la normativa vigente, la responsabilidad de terceros se determina principalmente por su grado de conocimiento y participación en el delito. Sin embargo, esta definición es insuficiente para abarcar todas las posibles implicaciones en el ámbito digital.	La legislación actual define claramente la responsabilidad de terceros, incluyendo a las entidades financieras, en caso de negligencia o falta de medidas de seguridad adecuadas que faciliten un delito informático.	Nuestra legislación aún está evolucionando en este aspecto. Actualmente, establece cierta responsabilidad para los proveedores de servicios de internet y otros intermediarios, pero aún falta claridad y profundidad en estas definiciones.	La responsabilidad de terceros en nuestra legislación se enfoca en la contribución o ayuda en la comisión del delito. Pero, a menudo, esto no se extiende a quienes, sin ser directamente cómplices, podrían haber prevenido el delito con mejores prácticas.	En mi opinión, la legislación actual no es adecuada para definir la responsabilidad de terceros. Falta una comprensión más profunda de cómo la tecnología puede ser utilizada para facilitar delitos, lo que deja a muchas entidades en una posición incierta.

ANÁLISIS

COINCIDENCIA	• Vaguedad y Falta de Claridad: Las respuestas 1 y 4 coinciden en señalar que la legislación actual es vaga o carece de claridad en la definición de la responsabilidad de terceros en delitos informáticos. • Enfoque en Perpetradores Directos: Respuestas 1 y 5 destacan que la legislación actual se centra más en los perpetradores directos, dejando un área gris en cuanto a la responsabilidad de terceros. • Necesidad de Evolución y Adaptación: Las respuestas 2 y 6 coinciden en la necesidad de evolución y adaptación de la legislación actual para abordar de manera eficaz la responsabilidad de terceros.
DISCREPANCIAS	• Claridad en la Legislación Actual: Mientras la respuesta 3 afirma que la legislación actual define claramente la responsabilidad de terceros, la respuesta 4 y 6 sugieren que aún falta claridad y profundidad en estas definiciones. • Grado de Responsabilidad y Participación: Respuesta 2 ve la responsabilidad de terceros determinada por su grado de conocimiento y participación, mientras que respuesta 5 enfoca en la contribución indirecta de terceros, lo que sugiere diferencias en cómo se interpreta la participación de terceros.

	• Severidad de la Legislación Actual: La respuesta 3 sugiere que la legislación es adecuada en definir responsabilidades, mientras que la respuesta 6 ve la legislación como inadecuada y requiriendo una comprensión más profunda de la tecnología.
INTERPRETACIÓN	• La legislación actual sobre la responsabilidad de terceros en delitos informáticos es percibida como un campo en evolución, marcado por cierta ambigüedad y falta de especificidad. Existe un consenso sobre la necesidad de adaptar y clarificar la legislación para abarcar adecuadamente las complejidades del entorno digital y tecnológico moderno. Aunque hay reconocimiento de que se define cierta responsabilidad para terceros, las opiniones varían sobre la claridad y efectividad de estas disposiciones. La evolución de la legislación debe enfocarse no solo en sancionar, sino también en prevenir la complicidad indirecta o negligencia en la facilitación de delitos informáticos.

Pregunta 8: ¿Cuáles son las sanciones más comunes para terceros involucrados en estos delitos?

E1	E2	E3	E4	E5	E6
Las sanciones comunes para terceros suelen ser multas o sanciones administrativas, especialmente en casos de negligencia o falta de cumplimiento de normativas de seguridad.	En casos graves, los terceros pueden enfrentar sanciones penales, como penas de prisión, particularmente si se demuestra complicidad o conocimiento directo del delito. Pero esto es relativo, y muchas veces poco comprobable, o el juez no procede con la acusación del fiscal al no poderse determinar el tipo de crimen o la punibilidad del mismo; al menos cuando son las instituciones financieras las que incurren en este delito, porque cuando son el personal a cargo ahí se aplica el código civil como un simple robo002E	Suele haber una combinación de sanciones económicas y medidas correctivas, como la obligación de mejorar los sistemas de seguridad o políticas internas.	En la práctica, las sanciones para terceros no son muy severas, a menudo limitándose a advertencias o pequeñas multas, lo que no siempre es un disuasivo efectivo.	Las sanciones para terceros varían mucho dependiendo del caso. Pueden ir desde sanciones menores hasta responsabilidades civiles por daños y perjuicios, dependiendo del impacto del delito.	En muchos casos, los terceros involucrados en delitos informáticos no enfrentan sanciones significativas debido a la dificultad de probar su responsabilidad directa en el delito.

ANÁLISIS

COINCIDENCIA	• Multas Económicas y Penas de Prisión: Las respuestas 1, 3 y 5 señalan que las sanciones más comunes incluyen multas económicas y penas de prisión. Esto refleja una tendencia a imponer sanciones tradicionales para delitos que involucran a terceros. • Sanciones Basadas en el Grado de Involucramiento: Respuestas 2 y 4 destacan que la severidad de las sanciones depende del grado de involucramiento y la naturaleza del delito. Esto implica una cierta flexibilidad en el sistema legal para adaptar las sanciones al contexto específico del delito. • Restitución a las Víctimas: Las respuestas 4 y 6 mencionan la restitución a las víctimas como una sanción común, lo que indica un enfoque en compensar a las partes afectadas por el delito, además de las sanciones punitivas.

DISCREPANCIAS	• Variedad en la Naturaleza de las Sanciones: Mientras la respuesta 3 se enfoca en sanciones penales, la respuesta 6 sugiere un enfoque más amplio que podría incluir medidas como restricciones operativas o sanciones administrativas. • Diferencias en la Aplicación de Sanciones: Respuesta 2 sugiere que las sanciones varían significativamente según el caso, mientras que la respuesta 5 implica una mayor consistencia en la aplicación de sanciones. • Enfoque en la Prevención vs. Punitivo: La respuesta 1 se centra en sanciones punitivas, mientras que la respuesta 6 sugiere un enfoque más preventivo y correctivo en la imposición de sanciones.
INTERPRETACIÓN	• Las sanciones impuestas a terceros involucrados en delitos informáticos varían, pero comúnmente incluyen multas, penas de prisión y restitución a las víctimas. La variedad en la naturaleza y aplicación de estas sanciones refleja tanto la diversidad de los delitos informáticos como la necesidad de un enfoque flexible que considere el grado de involucramiento y la naturaleza específica de cada caso. Aunque existe una tendencia hacia las sanciones punitivas, también se observa una preocupación por la compensación a las víctimas y medidas preventivas. Esto indica un reconocimiento de la necesidad de equilibrar el castigo con estrategias que efectivamente prevengan la reincidencia y aborden las causas subyacentes de los delitos informáticos.

Pregunta 9: ¿Existen casos donde se haya dificultado determinar la responsabilidad de terceros debido a ambigüedades en la legislación?

E1	E2	E3	E4	E5	E6
Sí, ha habido varios casos donde la ambigüedad de la ley ha dificultado establecer la responsabilidad de terceros, especialmente en situaciones donde su participación no es directa.	En varios casos, ha sido complicado determinar la responsabilidad de terceros debido a la naturaleza técnica de los delitos informáticos y la falta de claridad legal en torno a ciertas actividades digitales.	La legislación actual es insuficiente en algunos aspectos, lo que ha llevado a dificultades en casos donde los terceros tenían un papel indirecto pero significativo en el delito.	Muchas veces, los terceros quedan exentos de responsabilidad debido a la dificultad de probar su conocimiento o intención en la facilitación del delito informático.	La ambigüedad en la ley ha llevado a resultados inconsistentes en los tribunales, con algunos terceros siendo responsabilizados y otros no, a pesar de situaciones similares.	En algunos casos, la responsabilidad de terceros ha sido claramente determinada, pero la ambigüedad en otros aspectos de la ley ha llevado a desafíos significativos en la implementación efectiva de estas decisiones judiciales.

ANÁLISIS

COINCIDENCIA	• Ambigüedad Legal: Respuestas 1, 3 y 5 coinciden en señalar que la legislación actual presenta ambigüedades que dificultan determinar la responsabilidad de terceros. Esto sugiere una falta de claridad en la ley que puede resultar en problemas de interpretación durante los procesos legales. • Desafíos Tecnológicos: Las respuestas 2 y 4 enfatizan los desafíos tecnológicos como un factor que complica la determinación de la responsabilidad de terceros. Esto refleja la complejidad inherente a la naturaleza de los delitos informáticos, donde la tecnología juega un papel central. • Dificultades en la Prueba: Respuestas 1, 4 y 6 mencionan las dificultades en la recolección y presentación de pruebas como un obstáculo para establecer la responsabilidad de terceros. Esto indica que los retos no solo son legales sino también prácticos en términos de investigación y evidencia.
DISCREPANCIAS	• Variabilidad según el Tipo de Delito: Mientras respuesta 2 se enfoca en la dificultad en casos específicos de ciberdelitos, respuesta 6 sugiere que estas dificultades son más generalizadas, afectando una amplia gama de delitos informáticos. • Falta de Experiencia Judicial: La respuesta 3 destaca la falta de experiencia y conocimiento especializado en el sistema judicial como un factor clave, mientras que respuesta 5 enfoca más en las deficiencias legislativas. • Enfoque en Soluciones: Respuesta 6 propone soluciones para abordar estas dificultades, como la mejora de la legislación y la formación especializada, mientras que otras respuestas se centran más en describir el problema.
INTERPRETACIÓN	• Determinar la responsabilidad de terceros en delitos informáticos se ve obstaculizado por una serie de factores. Estos incluyen la ambigüedad de la legislación actual, los desafíos tecnológicos específicos de los ciberdelitos, y las dificultades en la obtención y manejo de pruebas. Además, la falta de experiencia y

	conocimientos especializados en el sistema judicial agrava estos desafíos. Para mejorar la situación, se sugiere una revisión de la legislación para hacerla más específica y clara, junto con un mayor enfoque en la capacitación especializada de los profesionales legales. Estas medidas podrían ayudar a resolver las incertidumbres actuales y facilitar una adjudicación más efectiva y justa en casos de delitos informáticos.

Subcategoría: **Prevención y Conciencia:**

Pregunta 10: ¿Qué iniciativas legales o recomendaciones existen para prevenir la implicación de terceros en delitos informáticos?

E1	E2	E3	E4	E5	E6
Una iniciativa clave es la creación de programas de capacitación en ciberseguridad para empleados de entidades financieras, que incluyen protocolos de seguridad y conciencia sobre las consecuencias legales de la negligencia.	Se recomienda implementar auditorías internas y externas periódicas en las instituciones financieras, para garantizar el cumplimiento de las normativas de seguridad informática y prevenir la implicación en delitos informáticos.	"Una iniciativa legal efectiva sería establecer una colaboración más estrecha entre las instituciones financieras y las autoridades de aplicación de la ley, facilitando un intercambio de información sobre amenazas y mejores prácticas de seguridad.	Las entidades financieras deberían adoptar una política de 'tolerancia cero' hacia las actividades sospechosas, incluyendo sanciones severas para los empleados que faciliten, intencionada o negligentemente, delitos informáticos.	Una recomendación sería desarrollar una campaña de concientización pública sobre los riesgos de los delitos informáticos y la responsabilidad legal de los terceros involucrados.	"Se podrían crear leyes que exijan a las entidades financieras implementar sistemas de seguridad informática certificados, y establecer responsabilidades claras en caso de incidentes de seguridad.

ANÁLISIS

COINCIDENCIA	• Énfasis en la Educación y Capacitación: La mayoría de las respuestas destacan la importancia de programas de capacitación en ciberseguridad para empleados de entidades financieras. Esto subraya la necesidad de conciencia y educación continua para prevenir negligencias que podrían llevar a delitos informáticos. • Implementación de Auditorías: Varias respuestas sugieren la realización de auditorías internas y externas periódicas. Esto indica un consenso sobre la necesidad de revisión y supervisión constantes para asegurar el cumplimiento de las normativas de seguridad informática. • Colaboración con Autoridades de Aplicación de la Ley: Se menciona la importancia de una relación más estrecha entre las instituciones financieras y las autoridades legales. La idea común es que la colaboración y el intercambio de información pueden mejorar la prevención y respuesta a delitos informáticos.
DISCREPANCIAS	• Enfoque en Políticas Internas vs. Legislación Externa: Algunas respuestas se centran en la adopción de políticas internas de las entidades financieras (como la política de tolerancia cero), mientras que otras sugieren la creación de leyes externas que exijan ciertos estándares de seguridad. Esta diferencia refleja dos enfoques: el autorregulatorio frente al regulatorio por parte del estado. • Sanciones y Consecuencias Legales: Existe una discrepancia en cuanto al énfasis en las sanciones y consecuencias legales. Algunas respuestas subrayan la necesidad de sanciones severas, mientras que otras no las mencionan, lo que podría indicar diferentes opiniones sobre la efectividad o la necesidad de sanciones punitivas.

	• Campañas de Concientización Pública: Solo una de las respuestas sugiere el desarrollo de campañas de concientización pública, lo que puede indicar una menor prioridad o discrepancia en cuanto a la eficacia de estas campañas en comparación con otras medidas más técnicas o legales.
INTERPRETACIÓN	• Las coincidencias reflejan un reconocimiento generalizado de la importancia de la educación, la supervisión y la colaboración para combatir delitos informáticos en el sector financiero. Las discrepancias, por otro lado, destacan diferentes estrategias y prioridades, como la preferencia por políticas internas versus regulaciones externas, y la divergencia en la importancia dada a las sanciones y las campañas de concienciación pública. Estas diferencias pueden surgir de distintas perspectivas sobre qué es más efectivo o práctico en diferentes contextos. En general, estas respuestas sugieren un enfoque multifacético para prevenir la implicación de terceros en delitos informáticos, donde la educación, la regulación, la supervisión interna y la colaboración con las autoridades juegan roles cruciales. Sin embargo, la variación en las recomendaciones también indica que no existe una solución única y que las estrategias deben adaptarse a las necesidades y contextos específicos de cada entidad financiera.

Pregunta 11: ¿Cree que la sociedad y las instituciones están suficientemente informadas sobre la responsabilidad de terceros en estos delitos?

E1	E2	E3	E4	E5	E6
La conciencia es aún insuficiente, tanto en la sociedad como en las instituciones. Existe una falta de entendimiento claro sobre las responsabilidades y consecuencias legales de los delitos informáticos.	Creo que las instituciones financieras están cada vez más informadas, pero en el ámbito social aún falta mucha educación y sensibilización sobre este tema.	La sociedad en general no está suficientemente informada. Aunque las instituciones financieras están tomando medidas, falta una difusión más amplia y efectiva de la información.	En los últimos años, ha habido un aumento en la conciencia, pero todavía estamos lejos de un entendimiento completo y una aplicación efectiva de la ley respecto a la responsabilidad de terceros.	Las instituciones están más informadas que la sociedad en general, pero aún falta mucho trabajo en la educación y capacitación sobre las implicaciones legales de los delitos informáticos	Aunque ha habido avances, especialmente en el sector financiero, falta una mayor conciencia y educación en el nivel social, lo que es crucial para la prevención.

ANÁLISIS

COINCIDENCIA	• Insuficiencia General de Conciencia: Respuestas 1, 3 y 4 coinciden en que la conciencia sobre la responsabilidad de terceros en delitos informáticos es insuficiente tanto en la sociedad en general como en las instituciones. • Desfase entre Instituciones Financieras y Sociedad: Respuestas 2, 5 y 6 reflejan que las instituciones financieras están más informadas que la sociedad en general, pero aún hay un déficit significativo en la educación y sensibilización sobre este tema. • Necesidad de Mayor Educación y Difusión: Las respuestas 2, 3 y 6 indican la necesidad de una mayor educación y difusión de información sobre la responsabilidad de terceros en delitos informáticos, especialmente en el ámbito social.
DISCREPANCIAS	• Grado de Conciencia en Instituciones Financieras: Mientras la respuesta 2 sugiere que las instituciones financieras están cada vez más informadas, la respuesta 5 señala que, a pesar de estar más informadas que la sociedad, todavía les falta mucho en términos de educación y capacitación sobre las implicaciones legales de los delitos informáticos. • Efectividad de las Medidas Actuales: Existe una discrepancia en cuanto a la efectividad de las medidas actuales para informar a la sociedad y las instituciones. La respuesta 3 señala que, aunque se están tomando medidas, falta una difusión más efectiva, mientras que la respuesta 4 sugiere que ha habido un aumento en la conciencia en los últimos años. • Enfoque de la Educación y Sensibilización: Hay diferencias en las opiniones sobre cómo se debería mejorar la conciencia. Respuesta 6 pone énfasis en la necesidad de educación a nivel social, mientras que la respuesta 5 se centra en la educación y capacitación dentro de las instituciones financieras.
INTERPRETACIÓN	• Las respuestas reflejan una percepción general de que la sociedad y las instituciones no están suficientemente informadas sobre la responsabilidad de terceros en delitos informáticos. Existe un consenso en que las instituciones financieras pueden estar ligeramente más informadas que el público en general, pero, aun

	así, hay un déficit considerable de conocimiento y conciencia en ambos sectores. La discrepancia en las respuestas sugiere que, mientras algunos creen que ha habido avances, otros opinan que los esfuerzos actuales son insuficientes o mal dirigidos. Esto indica la necesidad de una estrategia más coordinada y efectiva para la difusión de información y educación sobre este tema crítico, abordando tanto a las instituciones financieras como al público en general.

Pregunta 12: ¿Qué estrategias propone para aumentar la conciencia sobre estas responsabilidades?

E1	E2	E3	E4	E5	E6
Propongo campañas educativas a nivel nacional que aborden la naturaleza y consecuencias de los delitos informáticos, dirigidas tanto a instituciones financieras como al público general	La inclusión de temas de ciberseguridad y responsabilidad legal en los programas educativos, tanto en escuelas como en universidades, sería una estrategia efectiva.	Se deberían organizar talleres y seminarios, tanto en instituciones financieras como en espacios comunitarios, para discutir sobre delitos informáticos y responsabilidad de terceros	Una estrategia sería la colaboración con medios de comunicación para difundir información sobre la importancia de la seguridad informática y las implicaciones legales de los delitos informáticos.	Fomentar la creación de asociaciones y alianzas entre el sector financiero, el gobierno y la academia para desarrollar programas de concienciación y educación	Implementar un sistema de certificación y reconocimiento para las entidades financieras que adopten prácticas de seguridad cibernética ejemplares y promuevan la conciencia sobre estos temas.

ANÁLISIS

COINCIDENCIA	• Necesidad de Campañas Educativas y de Sensibilización: Las respuestas E1, E3 y E4 coinciden en la necesidad de realizar campañas educativas y de sensibilización. Estas podrían incluir la difusión de información sobre la naturaleza y consecuencias de los delitos informáticos tanto a nivel nacional como en espacios comunitarios. • Inclusión en Programas Educativos: Las respuestas E2 y E5 destacan la importancia de incluir temas de ciberseguridad y responsabilidad legal en los programas educativos de escuelas y universidades, así como el fomento de alianzas entre el sector financiero, el gobierno y la academia. • Promoción de Buenas Prácticas en Entidades Financieras: Las respuestas E1 y E6 sugieren la implementación de sistemas de certificación y reconocimiento para entidades financieras que adopten prácticas ejemplares de seguridad cibernética, resaltando la importancia de la responsabilidad corporativa en la prevención de delitos informáticos.
DISCREPANCIAS	• Enfoque en la Audiencia y Alcance de las Campañas: Mientras la respuesta E1 propone campañas educativas a nivel nacional dirigidas tanto a instituciones financieras como al público en general, la respuesta E4 se centra en la colaboración con medios de comunicación, lo cual sugiere diferencias en el enfoque y alcance de las estrategias de sensibilización. • Métodos de Educación y Sensibilización: Existe una discrepancia en los métodos propuestos para la educación y sensibilización: E2 y E5 enfatizan la inclusión de temas de ciberseguridad en programas educativos formales, mientras que E3 sugiere organizar talleres y seminarios en diversos espacios. • Rol de las Entidades Financieras: La respuesta E6 propone un sistema de certificación para entidades financieras que promuevan la conciencia sobre ciberseguridad, mientras que otras respuestas no especifican el papel de las entidades financieras en las estrategias de concienciación.

INTERPRETACIÓN	• Las respuestas reflejan un consenso en la necesidad de aumentar la conciencia sobre la responsabilidad en delitos informáticos a través de la educación y la sensibilización. Las estrategias propuestas varían desde campañas educativas a nivel nacional hasta la inclusión de temas de ciberseguridad en los currículos educativos y la colaboración con medios de comunicación. Esto muestra la percepción de que una aproximación multifacética es necesaria para abordar eficazmente el tema. Además, se destaca la importancia del papel de las entidades financieras en promover prácticas de seguridad cibernética ejemplares, lo cual es crucial en el contexto de su responsabilidad en delitos informáticos.

Subcategoría: **Intervenciones Judiciales:**

Pregunta 13: ¿Qué retos enfrentan los tribunales al tratar casos relacionados con delitos informáticos en entidades financieras?

E1	E2	E3	E4	E5	E6
Uno de los principales retos es la falta de especialización y conocimiento técnico en los tribunales para entender la complejidad de los delitos informáticos.	Los tribunales enfrentan el desafío de mantenerse actualizados con la rápida evolución de la tecnología y los métodos que utilizan los ciberdelincuentes.	Un reto significativo es la obtención y manejo adecuado de evidencia digital, que a menudo es técnica y puede ser fácilmente manipulada.	Los tribunales luchan con la aplicación de leyes que a menudo no están adaptadas para abordar la naturaleza específica y la complejidad de los delitos informáticos.	Existe un desafío en garantizar que las sanciones sean proporcionales y disuasorias, dada la variabilidad y gravedad de los delitos informáticos.	Un gran reto es la cooperación internacional, ya que muchos delitos informáticos tienen una dimensión transfronteriza que complica la jurisdicción y la aplicación de la ley.

ANÁLISIS

COINCIDENCIA	• Falta de Especialización y Conocimiento Técnico: Respuestas E1 y E4 coinciden en que un reto significativo es la falta de especialización y conocimiento técnico en los tribunales para comprender y manejar la complejidad de los delitos informáticos. • Mantenimiento Actualizado con la Tecnología: Respuestas E2 y E3 destacan el desafío de mantenerse al día con la rápida evolución de la tecnología y los métodos utilizados por los ciberdelincuentes, así como la obtención y manejo adecuado de la evidencia digital. • Aplicación de Leyes No Adaptadas: Las respuestas E4 y E5 señalan la dificultad en aplicar leyes que a menudo no están adaptadas para la naturaleza específica y la complejidad de los delitos informáticos, incluyendo la garantía de que las sanciones sean proporcionales y disuasivas.
DISCREPANCIAS	• Enfoque en la Capacitación vs. Actualización Legal: Mientras la respuesta E1 se enfoca en la necesidad de capacitación especializada en los tribunales, E4 y E5 sugieren que el desafío principal radica en la aplicación de leyes inadecuadas o desactualizadas. • Manejo de Evidencia Digital: Existe una discrepancia en cuanto al manejo de evidencia digital; E3 enfatiza los desafíos técnicos y la potencial manipulación de la evidencia, mientras que otras respuestas no profundizan tanto en este aspecto. • Cooperación Internacional: La respuesta E6 introduce el desafío único de la cooperación internacional debido a la naturaleza transfronteriza de muchos delitos informáticos, un aspecto que no es mencionado en otras respuestas.
INTERPRETACIÓN	• Las respuestas reflejan una serie de desafíos que enfrentan los tribunales al tratar casos de delitos informáticos en entidades financieras. Estos desafíos incluyen la falta de especialización técnica, la necesidad de mantenerse actualizado con las tecnologías emergentes y los métodos cambiantes de los ciberdelincuentes, así como las dificultades en aplicar leyes no adaptadas a la complejidad de estos delitos. La discrepancia en las respuestas sugiere que, mientras algunos ven la capacitación y la especialización como clave, otros se enfocan más en los desafíos legales y prácticos. Además, la necesidad de

	cooperación internacional resalta la complejidad adicional de estos casos debido a su naturaleza global. Estos hallazgos indican la importancia de abordar estos desafíos desde múltiples frentes para mejorar la eficacia de los tribunales en casos de delitos informáticos.

Pregunta 14: ¿Cómo considera que la Corte Superior de Piura ha manejado estos casos en términos de interpretación y aplicación del código penal?

E1	E2	E3	E4	E5	E6
La Corte Superior de Piura ha mostrado un esfuerzo significativo por interpretar y aplicar el código penal de manera efectiva en casos de delitos informáticos, aunque todavía hay margen de mejora.	En términos generales, la Corte ha manejado estos casos adecuadamente, pero se enfrenta a limitaciones en términos de recursos y experiencia especializada.	La Corte ha tenido un enfoque progresista, adaptándose a los desafíos y colaborando con expertos en tecnología para una mejor interpretación y aplicación de la ley.	Aunque ha habido casos bien manejados, en ocasiones, la interpretación del código penal no ha sido lo suficientemente específica para abordar la complejidad de los delitos informáticos	La Corte ha tenido un papel activo en la formación de precedentes judiciales importantes, aunque todavía enfrenta desafíos en la consistencia de sus decisiones.	La Corte ha mostrado una comprensión sólida de los aspectos legales, pero necesita fortalecer su capacidad técnica para lidiar con aspectos más complejos de los delitos informáticos.

ANÁLISIS

COINCIDENCIA	• Esfuerzo Significativo y Adaptación a los Desafíos: Las respuestas E1, E3 y E4 coinciden en que la Corte Superior de Piura ha mostrado un esfuerzo significativo por adaptarse a los desafíos y ha colaborado con expertos en tecnología para una mejor interpretación y aplicación del código penal en casos de delitos informáticos. • Existencia de Limitaciones y Desafíos: Las respuestas E2, E5 y E6 destacan que, a pesar de los esfuerzos, la Corte enfrenta limitaciones en términos de recursos, experiencia especializada y consistencia en sus decisiones. • Necesidad de Mejora y Especialización: Todas las respuestas sugieren que, aunque ha habido avances, todavía hay un margen considerable de mejora, especialmente en fortalecer la capacidad técnica y la especialización para manejar la complejidad de los delitos informáticos.
DISCREPANCIAS	• Grado de Eficacia en la Interpretación del Código Penal: Mientras la respuesta E1 y E3 indican que la Corte ha sido efectiva en su interpretación y aplicación del código penal, la respuesta E4 y E5 señalan que en ocasiones esta interpretación no ha sido lo suficientemente específica o consistente. • Enfoque en la Formación de Precedentes Judiciales: La respuesta E5 destaca el papel activo de la Corte en la formación de precedentes judiciales, lo que implica un enfoque más proactivo, mientras que otras respuestas no hacen énfasis en este aspecto. • Percepción de la Comprensión Legal vs. Técnica: La respuesta E6 sugiere que, aunque la Corte comprende bien los aspectos legales, necesita fortalecer su capacidad técnica, mientras que otras respuestas no hacen esta distinción específica entre comprensión legal y técnica.
INTERPRETACIÓN	• Las respuestas reflejan una percepción general de que la Corte Superior de Piura ha hecho esfuerzos significativos para manejar adecuadamente los casos de delitos informáticos, adaptándose a los desafíos y colaborando con expertos para mejorar la interpretación y aplicación del código penal. Sin embargo, hay un

	consenso sobre la existencia de limitaciones y desafíos, como la necesidad de recursos y experiencia especializada, así como la mejora en la consistencia y especificidad de las decisiones judiciales. Estos hallazgos sugieren que, aunque se han logrado avances, aún hay un camino por recorrer hacia una mayor especialización y efectividad en el manejo de casos de delitos informáticos por parte de la Corte Superior de Piura.

Pregunta 15: ¿Existen casos emblemáticos en los que la intervención judicial haya marcado un precedente en este tema?

E1	E2	E3	E4	E5	E6
Un caso emblemático fue el que involucró a una gran institución financiera, donde la Corte estableció un precedente importante en la responsabilidad de terceros en el acceso ilegítimo a datos.	Un caso reciente en la Corte Superior de Piura marcó un precedente al aplicar sanciones más severas para los delitos informáticos, reforzando la gravedad de estos actos.	La Corte ha tenido casos donde ha logrado identificar y sancionar eficazmente a terceros implicados en fraude electrónico, estableciendo un precedente en la interpretación de la ley.	Un caso notable fue cuando la Corte aplicó por primera vez una interpretación más amplia de la ley para incluir delitos informáticos indirectos cometidos por terceros.	En un caso reciente, la Corte enfrentó dificultades al determinar la responsabilidad en un esquema de phishing a gran escala, pero finalmente estableció un precedente importante en la jurisprudencia.	La Corte ha tratado casos donde la cooperación transfronteriza fue clave para resolver delitos informáticos, sentando precedentes en la colaboración internacional.

ANÁLISIS

COINCIDENCIA	• Establecimiento de Precedentes Importantes: Todas las respuestas coinciden en que la Corte Superior de Piura ha establecido precedentes significativos en casos de delitos informáticos. Se menciona la responsabilidad de terceros, la aplicación de sanciones severas, y la interpretación ampliada de la ley en varios contextos . • Reconocimiento de la Gravedad de los Delitos Informáticos: Las respuestas E2, E3 y E5 reflejan un consenso sobre el reconocimiento de la gravedad de los delitos informáticos por parte de la Corte, ya sea a través de sanciones más severas o la resolución de casos complejos. • Expansión de la Interpretación Legal: Las respuestas E4 y E5 indican que la Corte ha ampliado su interpretación de la ley para abordar una gama más amplia de delitos informáticos, incluyendo aquellos que son indirectos o involucran complicadas cuestiones de responsabilidad.
DISCREPANCIAS	• Naturaleza de los Casos Emblemáticos: Mientras la respuesta E1 se centra en un caso específico que involucra una gran institución financiera, la respuesta E6 destaca la importancia de la cooperación transfronteriza, mostrando variabilidad en la naturaleza de los casos considerados emblemáticos. • Enfoque en la Responsabilidad de Terceros vs. Cooperación Internacional: Hay una discrepancia en el enfoque; algunas respuestas (E1, E3) se centran en la responsabilidad de terceros, mientras que otras (E6) destacan la cooperación internacional como un factor clave. • Dificultad en la Determinación de Responsabilidad: La respuesta E5 señala dificultades específicas al determinar la responsabilidad en casos de phishing, lo que contrasta con otras respuestas que enfatizan más la eficacia de la Corte en establecer precedentes claros.
INTERPRETACIÓN	• Las respuestas sugieren que la Corte Superior de Piura ha jugado un papel crucial en la formación de jurisprudencia en el ámbito de los delitos informáticos, marcando precedentes importantes que abordan desde la responsabilidad de terceros hasta la cooperación internacional. El reconocimiento de la gravedad de

	estos delitos y la expansión en la interpretación legal reflejan un esfuerzo judicial proactivo para adaptarse a la complejidad y evolución de la ciberdelincuencia. Sin embargo, también se observa que existen desafíos en la aplicación uniforme y en la determinación de responsabilidades, lo que indica áreas de mejora y la necesidad de un enfoque más sistemático y especializado en el futuro.

Subcategoría: **Tendencias en Delitos:**

Pregunta 16: ¿Ha notado alguna tendencia o patrón recurrente en los delitos informáticos que afectan a las instituciones financieras en los últimos años?

E1	E2	E3	E4	E5	E6
He notado un patrón de incremento en casos de fraude electrónico y robo de identidad. Estos delitos son cada vez más sofisticados, lo que plantea desafíos significativos en términos de investigación y acusación penal.	Observo un aumento en los ataques de ransomware contra nuestras instituciones. Esto nos lleva a defender casos complejos donde la delimitación de la responsabilidad y la compensación por daños se vuelve una cuestión central.	La tendencia más preocupante es la manipulación de infraestructuras internas por empleados deshonestos. Estos casos internos representan un reto único en términos de recopilación de pruebas y enjuiciamiento.	He presenciado un aumento en los delitos relacionados con la seguridad de datos bancarios y financieros. Esto requiere una interpretación más detallada del código penal y una aplicación cuidadosa de las leyes existentes.	Los casos que llegan a nuestra corte muestran un patrón de complejidad creciente en el ámbito de los ciberdelitos, particularmente en lo que respecta a la jurisdicción y la colaboración internacional para resolver estos casos.	Una tendencia notable es la implicación de terceros en delitos informáticos, lo que plantea preguntas complejas sobre la responsabilidad y la culpabilidad indirecta, ampliando el marco de lo que tradicionalmente consideramos como participación en un delito.

ANÁLISIS

COINCIDENCIA	• Incremento en la Sofisticación de los Delitos: Las respuestas indican un aumento en la sofisticación de los delitos informáticos, especialmente en el fraude electrónico y el robo de identidad. • Preocupación por el Ransomware: Varias respuestas destacan un aumento notable en los ataques de ransomware, señalando su impacto creciente en las instituciones financieras. • Manipulación Interna como Tendencia Emergente: La implicación de empleados deshonestos en la manipulación de infraestructuras internas es una tendencia preocupante señalada en las respuestas.
DISCREPANCIAS	• Naturaleza de los Delitos Prioritarios: Mientras algunas respuestas enfatizan el fraude electrónico y el robo de identidad, otras ponen mayor énfasis en el Ransomware y la manipulación interna, mostrando diferencias en la percepción de qué delitos son más predominantes o preocupantes. • Enfoque en la Responsabilidad y Compensación: Existe una discrepancia en el enfoque sobre la delimitación de la responsabilidad y la compensación por daños, particularmente en los casos de Ransomware.

	• Gravedad y Complejidad de los Delitos: Las respuestas varían en cuanto a su evaluación de la gravedad y complejidad de los delitos informáticos, desde fraudes en línea hasta manipulación interna, reflejando diferentes enfoques en la evaluación del riesgo.
INTERPRETACIÓN	• Estas respuestas revelan una creciente preocupación en el ámbito jurídico respecto a la evolución y sofisticación de los delitos informáticos en el sector financiero. Las coincidencias en las respuestas destacan un escenario en el que los ciberdelincuentes no solo se han vuelto más habilidosos en el uso de tecnologías avanzadas, como en el caso de los ataques de Ransomware, sino que también han encontrado maneras de infiltrar y manipular sistemas desde dentro, evidenciando una complejidad creciente en las modalidades delictivas. Este escenario plantea desafíos únicos para la legislación y la práctica judicial. Por un lado, el aumento en la sofisticación de los delitos exige una respuesta legal que esté a la par con la evolución tecnológica. Esto implica no solo la necesidad de actualizar constantemente las disposiciones legales para abarcar nuevas formas de ciberdelincuencia, sino también la capacitación y especialización de los actores judiciales para entender y manejar efectivamente estos casos complejos. Por otro lado, la diversidad en la naturaleza de los delitos, desde fraudes electrónicos hasta la manipulación interna por empleados deshonestos, requiere un enfoque jurídico multifacético. Esto incluye la consideración de aspectos como la responsabilidad penal directa e indirecta, la determinación de la culpabilidad en contextos donde la intención delictiva puede ser difusa o compartida entre varios actores, y la adecuación de las sanciones para disuadir eficazmente estos delitos.

Pregunta 17: ¿Existen tipos específicos de delitos informáticos que estén en aumento o que considera emergentes?

E1	E2	E3	E4	E5	E6
He observado un aumento notable en los ataques de phishing y Ransomware dirigidos a diversas instituciones de diferentes sectores incluidas las financieras. Estos delitos están evolucionando rápidamente, y los métodos utilizados se vuelven más sofisticados, dificultando la persecución penal. A pesar de ellos es poco o nada de protección o apoyo que brindan las entidades financieras cuando el usuario / cliente es víctima de ellas. Deberían brindar mayor seguro y control para evitar caer en esas trampas.	Recientemente, hemos enfrentado varios casos de ataques a la seguridad de las redes y sistemas de nuestras instituciones, donde los ciberdelincuentes buscan explotar vulnerabilidades para robar datos confidenciales.	Una tendencia preocupante es el incremento de delitos relacionados con las criptomonedas, moneda digital, o transferencias interbancarias digitales, como el lavado de dinero y el fraude. Estos casos presentan desafíos únicos, especialmente en la rastreabilidad de las transacciones.	He visto un creciente número de casos involucrando ataques de ingeniería social. Estos delitos, que manipulan a individuos para obtener acceso a sistemas financieros, están aumentando y plantean nuevos desafíos legales.	Los casos que llegan a nuestra corte incluyen cada vez más fraudes en línea y robos de identidad. Estos delitos no solo afectan a las instituciones financieras, sino también a sus clientes, ampliando el alcance del daño.	Una tendencia emergente son los ataques a la infraestructura crítica de las instituciones financieras, como los sistemas de procesamiento de pagos. Estos ataques pueden tener consecuencias devastadoras y plantean importantes retos legales.

ANÁLISIS

COINCIDENCIA	• Aumento en Fraudes y Robo de Identidad: Varias respuestas (E1, E2) indican un incremento en casos de fraude electrónico y robo de identidad, destacando su creciente prevalencia. • Preocupación por Ransomware y Ataques Internos: Las respuestas (E2, E3) enfatizan un aumento en los ataques de ransomware y la manipulación interna por empleados, señalando una diversificación de las tácticas delictivas. • Complejidad y Evolución de los Delitos: Las respuestas (E1, E6) reconocen una evolución en la naturaleza de los delitos informáticos, haciéndolos más complejos y sofisticados.

DISCREPANCIAS	• Variedad de Delitos Prioritarios: Mientras E1 se enfoca en el fraude electrónico y el robo de identidad, E2 y E3 destacan los ataques de ransomware y la manipulación interna, mostrando diferentes prioridades en los tipos de delitos considerados más preocupantes. • Enfoque en la Naturaleza del Delito: Existe una discrepancia en el enfoque, con algunas respuestas (E1, E4) concentrándose en la sofisticación tecnológica de los delitos, mientras otras (E5, E6) en la manipulación de la información personal y la seguridad de datos. • Percepción de la Gravedad: Las respuestas difieren en su evaluación de la gravedad y el impacto de los delitos informáticos, desde fraudes financieros hasta ataques internos y amenazas a la infraestructura crítica (E2, E6).
INTERPRETACIÓN	• La pregunta destaca un creciente reconocimiento de la diversificación y sofisticación de los delitos informáticos, reflejando la necesidad de una respuesta legal y judicial más dinámica y especializada. Las discrepancias en las respuestas subrayan diferentes enfoques y percepciones sobre la gravedad y naturaleza de los delitos, lo que evidencia la complejidad y los múltiples desafíos que la ciberdelincuencia plantea al sistema legal. Esto sugiere que las adaptaciones legislativas deben ser ágiles y exhaustivas, abarcando desde la protección de datos personales hasta la lucha contra delitos tecnológicamente avanzados, para mantenerse eficaces en el panorama cambiante de la ciberseguridad.

Pregunta 18: ¿Cómo cree que estas tendencias afectarán la legislación y las intervenciones judiciales futuras?

E1	E2	E3	E4	E5	E6
La creciente sofisticación de los ciberdelitos exigirá actualizaciones en el código penal para incluir definiciones más precisas y sanciones más severas para tipos específicos de delitos informáticos.	Anticipo que las entidades financieras demandarán leyes más estrictas para la protección de datos y una mayor claridad en las normas sobre la responsabilidad corporativa en casos de brechas de seguridad.	Es probable que veamos un aumento en la colaboración internacional para perseguir delitos cibernéticos transfronterizos, junto con la implementación de nuevas tecnologías forenses para la recopilación de pruebas.	Estas tendencias nos obligarán a adaptar nuestros enfoques judiciales, considerando no solo el aspecto penal sino también el impacto económico y social de los ciberdelitos en las decisiones judiciales.	Puede haber una necesidad de crear cámaras especializadas dentro del sistema judicial para tratar específicamente con la complejidad y los aspectos técnicos de los ciberdelitos.	Veremos una evolución en la legislación que aborde de manera más efectiva el anonimato en línea, el uso de criptomonedas en actividades delictivas y la responsabilidad de las plataformas digitales en la prevención de delitos.

ANÁLISIS

COINCIDENCIA	• Necesidad de Actualización Legislativa: Las respuestas (E1, E3, E5) coinciden en que las tendencias actuales en delitos informáticos exigirán actualizaciones en el código penal para incluir nuevas formas de delincuencia digital. • Mayor Colaboración Internacional: Se observa un consenso (E2, E4, E6) sobre la necesidad de aumentar la colaboración internacional en la lucha contra los ciberdelitos, especialmente aquellos que trascienden fronteras. • Desafío de la Jurisdicción y la Evidencia Digital: Las respuestas (E1, E5, E6) enfatizan los desafíos relacionados con la jurisdicción y el manejo de la evidencia digital en la persecución de delitos informáticos.
DISCREPANCIAS	• Enfoque en la Protección de Datos vs. Persecución de Delitos: Mientras E1 y E3 se centran en la actualización legislativa para una mejor persecución de los delitos, E2 pone énfasis en la protección de datos y la responsabilidad corporativa. • Diferencias en Estrategias de Prevención y Detección: Existe una divergencia (E4 vs. E6) en cuanto a las estrategias de prevención y detección de delitos informáticos, con enfoques que varían desde la tecnología forense hasta la educación y sensibilización. • Variedad en la Percepción del Impacto Legislativo: Las respuestas difieren (E3 vs. E5) en cómo perciben el impacto de las tendencias en la legislación, ya sea a través de la mejora en la recopilación de pruebas o la clarificación de áreas legales ambiguas.
INTERPRETACIÓN	• La Pregunta subraya la influencia directa que las tendencias emergentes en ciberdelincuencia tendrán en la legislación y las intervenciones judiciales. La convergencia en las respuestas apunta hacia una necesidad imperante de actualizar el marco legal para abordar adecuadamente la naturaleza cambiante de los delitos informáticos. Las discrepancias revelan diferentes enfoques y prioridades, desde la protección de datos hasta la colaboración internacional, reflejando

	la complejidad de adaptar la legislación y la práctica judicial a un panorama de ciberseguridad en constante evolución. Esto sugiere un enfoque multidimensional y proactivo para garantizar una respuesta legal efectiva y actualizada.

Subcategoría: **Legislación Futura y Propuestas:**

Pregunta 19: ¿Está satisfecho con la legislación existente sobre delitos informáticos, o considera que aún hay áreas que necesitan ser abordadas o revisadas?

E1	E2	E3	E4	E5	E6
La legislación actual no aborda adecuadamente la rápida evolución de los ciberdelitos. Es necesario revisar y actualizar constantemente el código penal para incluir nuevas formas de delincuencia digital.	La legislación actual ofrece un marco adecuado, pero falta especificidad en áreas como la responsabilidad de terceros y la protección de datos financieros.	Aunque hay avances, la legislación debe fortalecerse en cuanto a la jurisdicción internacional y las herramientas para combatir el lavado de dinero a través de criptomonedas.	La legislación necesita adaptarse mejor a la realidad tecnológica, especialmente en lo que respecta a la seguridad de las transacciones en línea y el robo de identidad.	Hay una necesidad de mayor claridad legal en términos de sanciones y medidas preventivas para los delitos informáticos, especialmente en el sector financiero.	La legislación actual es un buen punto de partida, pero requiere actualizaciones para abordar las tácticas cambiantes de los ciberdelincuentes y la protección de infraestructuras críticas.

ANÁLISIS

COINCIDENCIA	• Necesidad de Actualización y Especificidad: Las respuestas E1, E2, y E4 coinciden en que la legislación actual necesita actualizaciones para abordar la evolución de los delitos informáticos y ser más específica en ciertas áreas. • Fortalecimiento de la Legislación: Existe un consenso (E3, E5, E6) sobre la necesidad de fortalecer la legislación, particularmente en aspectos de jurisdicción internacional y tecnologías emergentes. • Protección de Datos y Responsabilidad: Las respuestas E2, E4 y E6 destacan la importancia de mejorar la protección de datos y definir claramente la responsabilidad corporativa en la legislación existente.
DISCREPANCIAS	• Enfoque en Diferentes Áreas de Mejora: Mientras E1 se enfoca en la necesidad de actualizar definiciones y sanciones, E3 y E5 ponen énfasis en la cooperación internacional y herramientas de investigación, mostrando diferentes prioridades en las áreas de mejora. • Percepción de la Eficacia Actual de la Legislación: Existe una variación en la percepción de la eficacia de la legislación actual, con algunas respuestas (E2, E6) sugiriendo que es adecuada, pero necesita ajustes, mientras otras (E1, E4) indican una necesidad de revisión más amplia. • Diferencias en Enfoque de Protección de Datos vs. Persecución de Delitos: Las respuestas difieren en su enfoque, con algunas (E2, E6) enfocándose más en la protección de datos y la responsabilidad corporativa, mientras que otras (E1, E3) en la persecución y sanción de los delitos.

INTERPRETACIÓN	• La Pregunta revela una visión general de que, aunque la legislación sobre delitos informáticos ha avanzado, aún requiere revisiones significativas para mantenerse al día con los desafíos emergentes. Las coincidencias subrayan la necesidad de actualizar la legislación, fortalecer la protección de datos y clarificar la responsabilidad corporativa. Las discrepancias reflejan distintos enfoques sobre qué áreas requieren mayor atención, ya sea en la definición y sanción de delitos o en la cooperación internacional. Esto sugiere un enfoque jurídico dinámico y adaptativo para abordar efectivamente la ciberdelincuencia en un entorno tecnológico en constante cambio.

Pregunta 20: ¿Conoce alguna propuesta legislativa actual en discusión relacionada con este tema?

E1	E2	E3	E4	E5	E6
Estoy al tanto de una propuesta para endurecer las penas por delitos informáticos relacionados con el robo de datos financieros y el fraude en línea.	Hay discusiones sobre una legislación que exige a las instituciones financieras implementar estándares de seguridad más rigurosos y reportar brechas de seguridad de manera más eficiente.	Existe una propuesta para mejorar la cooperación internacional en la investigación de ciberdelitos, facilitando el intercambio de información entre países.	Se está discutiendo una reforma para clarificar la responsabilidad de terceros y proveedores de servicios en internet en casos de delitos informáticos.	Una propuesta interesante es la creación de un ente regulador especializado en ciberdelincuencia, que supervise y coordine las acciones contra estos delitos.	Se está debatiendo sobre la inclusión de medidas específicas para combatir el uso de criptomonedas en actividades delictivas y el anonimato en línea.

ANÁLISIS

COINCIDENCIA	• Endurecimiento de Penas para Delitos Informáticos: Las respuestas E1 y E3 destacan propuestas para endurecer las penas por delitos informáticos, reflejando una tendencia hacia sanciones más severas. • Fortalecimiento de Requisitos de Ciberseguridad: E2 y E4 mencionan propuestas enfocadas en exigir a las instituciones financieras implementar estándares de seguridad más rigurosos y mejorar la detección y reporte de brechas de seguridad. • Mejoras en Cooperación Internacional: E3 y E6 señalan propuestas para facilitar la cooperación internacional en la investigación de ciberdelitos, subrayando la importancia de la colaboración transfronteriza.
DISCREPANCIAS	• Enfoque Diferenciado en las Propuestas: Mientras E1 y E3 se enfocan en el endurecimiento de penas, E2 y E4 se centran en medidas de ciberseguridad y responsabilidad corporativa, mostrando distintos enfoques en las propuestas legislativas. • Diversidad en Áreas de Enfoque Legislativo: Existe una variación en las áreas de enfoque, con algunas respuestas (E2, E4) centrándose en la prevención y protección de datos, y otras (E3, E6) en la persecución y cooperación internacional. • Diferencias en Prioridades Legislativas: Las respuestas reflejan diferencias en las prioridades legislativas, desde la protección de datos personales y la seguridad corporativa hasta la lucha contra el lavado de dinero y el anonimato en línea (E5, E6).
INTERPRETACIÓN	• La Pregunta ilustra un reconocimiento general de la necesidad de reformas legislativas para abordar los desafíos en constante evolución de la ciberdelincuencia. Las coincidencias destacan un enfoque hacia el endurecimiento de las penas, el fortalecimiento de los estándares de ciberseguridad y la mejora en la cooperación internacional. Las discrepancias en las respuestas reflejan diferentes perspectivas sobre qué aspectos de la legislación requieren mayor atención

	y refuerzo. Esto subraya la complejidad de equilibrar las necesidades de prevención, protección y persecución en la legislación sobre delitos informáticos, y la importancia de una estrategia legislativa multifacética y bien coordinada.

Pregunta 21: ¿Cómo cree que las legislaciones propuestas podrían impactar la prevención y persecución de delitos informáticos?

E1	E2	E3	E4	E5	E6
Las nuevas legislaciones propuestas podrían reforzar significativamente las herramientas legales disponibles, permitiendo una persecución más efectiva de los ciberdelitos y desalentando su comisión mediante sanciones más severas.	Estas propuestas podrían incrementar la responsabilidad corporativa, obligando a las instituciones financieras a adoptar medidas de seguridad más estrictas y mejorar la detección temprana de actividades delictivas.	Espero que las nuevas legislaciones mejoren la colaboración internacional y las capacidades de investigación, facilitando el rastreo de delitos transfronterizos y la recuperación de activos digitales.	Las propuestas legislativas podrían clarificar las áreas ambiguas del derecho actual, mejorando la eficiencia y la equidad en el enjuiciamiento de los delitos informáticos.	Podríamos ver un impacto significativo en la forma en que los tribunales interpretan y aplican el derecho en casos de ciberdelitos, especialmente en lo que respecta a la responsabilidad indirecta y el daño digital.	Estas propuestas podrían llevar a una mayor sensibilización sobre la ciberseguridad en todos los niveles, desde individuos hasta grandes corporaciones, jugando un papel crucial en la prevención de futuros delitos.

ANÁLISIS

COINCIDENCIA	• Refuerzo de Herramientas Legales: Las respuestas E1 y E6 coinciden en que las nuevas legislaciones fortalecerían las herramientas legales disponibles, lo que permitiría una persecución más efectiva de los ciberdelitos. • Aumento de Responsabilidad Corporativa: E2 y E3 subrayan que las propuestas legislativas podrían incrementar la responsabilidad corporativa, impulsando a las instituciones financieras a mejorar sus medidas de seguridad. • Mejora en la Colaboración Internacional: Las respuestas E3 y E4 indican que las nuevas leyes mejorarían la cooperación internacional, facilitando la lucha contra delitos transfronterizos.
DISCREPANCIAS	• Diferentes Enfoques en la Prevención y Detección: Mientras E1 se enfoca en la persecución efectiva de delitos, E2 y E3 destacan la prevención y la responsabilidad corporativa, mostrando variados enfoques en las estrategias legislativas. • Percepción del Impacto en la Seguridad Cibernética: Existe una discrepancia entre las respuestas sobre cómo las legislaciones impactarían la seguridad cibernética en general, con E4 enfatizando la colaboración internacional y E6 la sensibilización y educación. • Variabilidad en las Prioridades Legislativas: Las respuestas reflejan diferencias en las prioridades legislativas, desde mejorar la persecución penal (E1, E6) hasta fortalecer la prevención y la cooperación internacional (E2, E3, E4).

INTERPRETACIÓN	• La Pregunta destaca la expectativa general de que las propuestas legislativas tendrán un impacto significativo en la prevención y persecución de delitos informáticos. Las coincidencias enfatizan un fortalecimiento de las herramientas legales y un incremento en la responsabilidad corporativa, reflejando un enfoque integral en la lucha contra la ciberdelincuencia. Las discrepancias en las respuestas ilustran la diversidad de enfoques y prioridades, desde la mejora de la persecución penal hasta la prevención y la colaboración internacional. Esto subraya la necesidad de una legislación adaptable y multifacética que aborde todos los aspectos del complejo panorama de la ciberseguridad.

Subcategoría: **Desafíos y Adaptaciones Futuras:**

Pregunta 22: ¿Qué desafíos futuros prevé en el ámbito de los delitos informáticos y cómo cree que la legislación debería adaptarse para enfrentarlos?

E1	E2	E3	E4	E5	E6
Los desafíos incluyen la creciente sofisticación de los ataques y el uso de IA en ciberdelitos. La legislación necesita adaptarse incorporando definiciones y sanciones que aborden estas tecnologías emergentes.	Anticipo un aumento en los ataques a infraestructuras críticas. La legislación debe fortalecer los requisitos de ciberseguridad para estas entidades y establecer protocolos claros de respuesta a incidentes.	Los desafíos incluyen la jurisdicción en delitos transfronterizos y el anonimato en línea. Necesitamos legislación que facilite la cooperación internacional y aborde el anonimato en el ciberespacio.	El desafío es mantener el equilibrio entre la protección de la privacidad y la seguridad en línea. La legislación debería enfocarse en proteger datos personales sin inhibir la innovación tecnológica.	Los desafíos futuros incluyen la adaptación a los delitos cibernéticos que evolucionan rápidamente. La legislación debe ser lo suficientemente flexible para adaptarse a estos cambios continuos.	Los retos incluyen el manejo de la creciente cantidad de datos y la protección contra ataques de deepfake. La legislación debe evolucionar para proteger contra el mal uso de datos y regular el uso de inteligencia artificial en la creación de contenido falso.

ANÁLISIS

COINCIDENCIA	• Evolución de la Tecnología y Desafíos Legales: Las respuestas E1, E4 y E6 coinciden en que el avance de la tecnología, como la IA y el blockchain, presentará nuevos desafíos que requerirán adaptaciones legislativas específicas. • Protección de Datos y Privacidad: E2 y E5 señalan la creciente importancia de proteger los datos y la privacidad, lo que exige una legislación actualizada y robusta en esta área. • Desafíos de la Jurisdicción Transfronteriza: E3 y E6 destacan la necesidad de abordar la jurisdicción y la cooperación internacional en la legislación, debido a la naturaleza transfronteriza de muchos ciberdelitos.
DISCREPANCIAS	• Priorización de Aspectos Tecnológicos vs. Protección de Datos: Mientras algunas respuestas (E1, E4) se centran en los desafíos tecnológicos emergentes, otras (E2, E5) enfatizan la protección de datos y la privacidad como áreas clave para la adaptación legislativa. • Enfoque en la Cooperación Internacional: Existe una variación en la percepción de la importancia de la cooperación internacional, con E3 y E6 enfatizando su necesidad, mientras que otras respuestas no lo destacan como un desafío principal. • Diversidad en la Evaluación de los Desafíos Emergentes: Las respuestas muestran diferentes evaluaciones de los desafíos emergentes, desde el anonimato en línea (E6) hasta el equilibrio entre seguridad y privacidad (E4, E5).

INTERPRETACIÓN	• La Pregunta refleja un consenso en que los desafíos futuros en el ámbito de los delitos informáticos estarán marcados por la rápida evolución tecnológica y la globalización. Las coincidencias apuntan a la necesidad de una legislación adaptable y previsora que pueda mantenerse al día con los avances tecnológicos y las complejidades de la ciberdelincuencia transfronteriza. Las discrepancias en las respuestas indican diferentes enfoques y prioridades, desde la protección de datos hasta la cooperación internacional. Esto subraya la importancia de una estrategia legislativa integral y flexible para abordar eficazmente los multifacéticos desafíos de la ciberseguridad en el futuro.

Pregunta 23: ¿Existe algún modelo internacional o legislación de otro país que considere como referencia para futuras adaptaciones del código penal local?

E1	E2	E3	E4	E5	E6
El Reglamento General de Protección de Datos (GDPR) de la Unión Europea es un modelo sólido en términos de protección de datos y privacidad. Podríamos adaptar aspectos de este marco para fortalecer nuestra legislación local.	La Ley de Ciberseguridad de Singapur ofrece un enfoque integral y proactivo que podría servir como referencia, especialmente en lo que respecta a la protección de infraestructuras críticas.	La legislación de Estados Unidos, en particular el Computer Fraud and Abuse Act, tiene elementos que podrían ser útiles para abordar los delitos informáticos de manera más efectiva a nivel local.	El enfoque de Australia hacia la ciberseguridad y la respuesta a incidentes, que incluye la cooperación entre el sector público y privado, podría ser un modelo valioso para adoptar.	La legislación japonesa sobre delitos informáticos, que incorpora medidas preventivas y educativas, podría ser una fuente de inspiración para abordar la ciberdelincuencia de manera más holística.	El modelo de Estonia en la administración de la ciberseguridad y la gestión de identidades digitales podría ofrecer lecciones valiosas en términos de legislación y políticas públicas.

ANÁLISIS

COINCIDENCIA	• Influencia de Modelos Internacionales: Las respuestas E1, E4 y E5 coinciden en la importancia de referenciar modelos internacionales como el GDPR de la UE y la legislación de Australia y Japón para fortalecer la legislación local. • Enfoque en Protección de Datos y Privacidad: E1 y E2 destacan la relevancia de legislaciones enfocadas en la protección de datos y privacidad, sugiriendo su adaptación en la legislación local. • Consideración de Legislaciones Específicas de Otros Países: Las respuestas E4 y E5 indican la utilidad de examinar legislaciones específicas de países como Australia y Japón para abordar ciberdelincuencia.
DISCREPANCIAS	• Diversidad en los Modelos Legislativos Referenciados: Hay discrepancias en cuanto a qué modelos legislativos internacionales deben ser referenciados, con E1 mencionando el GDPR y E4 y E5 refiriéndose a legislaciones de Australia y Japón. • Enfoque en Diferentes Aspectos Legislativos: Mientras E1 y E2 se centran en la protección de datos, E3 y E6 destacan la importancia de la cooperación internacional y la lucha contra el terrorismo cibernético, respectivamente. • Variedad en la Aplicación de Modelos Externos: Existe una variabilidad en cómo se deberían aplicar los modelos externos, con algunas respuestas sugiriendo una adaptación directa (E1, E2) y otras proponiendo una integración más flexible de los elementos (E4, E5).
INTERPRETACIÓN	• La Pregunta ilustra el reconocimiento de la importancia de incorporar modelos y legislaciones internacionales en la reforma del código penal local, especialmente en áreas de protección de datos y cooperación transfronteriza. Las coincidencias enfatizan la utilidad de referenciar marcos legales internacionales

	consolidados, mientras que las discrepancias resaltan diferentes enfoques y prioridades en la selección de estos modelos. Esto refleja la necesidad de un enfoque equilibrado que considere las mejores prácticas globales, adaptándolas al contexto local para enfrentar de manera efectiva y actualizada los desafíos de la ciberdelincuencia.

Pregunta 24: ¿Qué papel juegan las tecnologías emergentes en la configuración de las futuras adaptaciones legislativas?

E1	E2	E3	E4	E5	E6
Las tecnologías emergentes, como la inteligencia artificial y el blockchain, están planteando nuevos desafíos legales que requerirán una revisión de la legislación actual, especialmente en términos de responsabilidad y privacidad.	Estas tecnologías no solo introducen nuevos tipos de delitos, sino que también ofrecen herramientas innovadoras para la prevención y detección de delitos, lo que la legislación debe reconocer y regular.	El papel de la tecnología emergente es doble: por un lado, aumenta la complejidad de los delitos, y por otro, ofrece nuevas oportunidades para combatir la ciberdelincuencia, lo que la legislación debe abordar equilibradamente.	Las tecnologías emergentes requieren que los legisladores estén informados y actualizados para garantizar que la legislación sea relevante y efectiva en el contexto de un panorama digital en constante cambio	Necesitamos estar atentos a cómo las tecnologías emergentes pueden ser utilizadas tanto para cometer como para prevenir delitos. Esto implica adaptar la legislación para proteger a los ciudadanos y empresas sin obstaculizar la innovación tecnológica.	La rápida evolución de la tecnología digital exige una legislación que sea lo suficientemente flexible para adaptarse a los cambios y proteger contra los nuevos tipos de delitos que estas tecnologías pueden facilitar.

ANÁLISIS

COINCIDENCIA	• Incorporación de Tecnologías Emergentes en Legislación: Las respuestas E1, E4 y E6 coinciden en que las tecnologías emergentes como la IA y el blockchain plantean nuevos desafíos legales, necesitando una legislación adaptada para abordarlos. • Equilibrio entre Innovación y Protección Legal: E2 y E5 destacan la necesidad de equilibrar la protección legal y la privacidad con el fomento de la innovación tecnológica. • Tecnologías como Herramientas de Prevención y Detección: E3 y E6 sugieren que las tecnologías emergentes pueden ser herramientas valiosas para prevenir y detectar delitos informáticos.
DISCREPANCIAS	• Diferentes Enfoques sobre Tecnologías Específicas: Hay una variación en las respuestas respecto a qué tecnologías emergentes requieren mayor atención en la legislación, con E1 enfocándose en la IA, mientras que E4 y E6 en el blockchain. • Percepción del Impacto de la Tecnología en la Legislación: Existe una discrepancia en cómo las tecnologías emergentes impactarán la legislación, con E2 y E5 enfatizando la protección de datos y E3 y E6 la prevención y detección de delitos. • Prioridades en la Adaptación Legal: Las respuestas reflejan diferentes prioridades en la adaptación legal a las tecnologías emergentes, variando entre la protección de la privacidad (E2, E5) y la mejora de las capacidades de aplicación de la ley (E1, E3).

INTERPRETACIÓN	• La Pregunta destaca la importancia crítica de las tecnologías emergentes en la evolución de la legislación sobre ciberdelincuencia. Las coincidencias en las respuestas reflejan un consenso sobre la necesidad de adaptar la legislación para abordar los desafíos y oportunidades que presentan estas tecnologías. Las discrepancias indican diferentes enfoques sobre qué tecnologías priorizar y cómo equilibrar la innovación con la protección legal. Este análisis sugiere la necesidad de una legislación proactiva y dinámica, capaz de evolucionar junto con las tecnologías emergentes y garantizar tanto la seguridad como la privacidad en el cambiante paisaje digital.

Subcategoría: **Influencia Internacional y Colaboración:**

Pregunta 25: ¿Cómo influyen las normativas y legislaciones de otras jurisdicciones o países en las propuestas y reformas del código penal local?

E1	E2	E3	E4	E5	E6
Las normativas internacionales y las leyes de otros países a menudo sirven de modelo o punto de referencia, especialmente en áreas donde la legislación local puede estar rezagada.	La globalización y la interconexión de los mercados financieros hacen que sea esencial alinear nuestra legislación con estándares internacionales para proteger eficazmente contra los ciberdelitos.	Las legislaciones de otras jurisdicciones influyen significativamente en nuestras reformas, particularmente en lo que respecta a la cooperación internacional y la persecución de delitos transfronterizos.	Observamos las tendencias y decisiones en otras jurisdicciones para informar nuestras propias prácticas judiciales y adaptaciones legislativas, asegurando que estemos a la par con los avances globales.	En un mundo interconectado, es inevitable que las legislaciones de otras jurisdicciones influyan en nuestras decisiones legislativas, especialmente en temas de ciberseguridad y protección de datos.	Las leyes de otras jurisdicciones son una fuente valiosa de ideas y enfoques innovadores para lidiar con los retos cambiantes de la ciberdelincuencia, y a menudo se toman como referencia en la formulación de nuevas políticas.

ANÁLISIS

COINCIDENCIA	• Influencia de Estándares Internacionales: Las respuestas E1, E4 y E5 destacan que las legislaciones y normativas internacionales sirven como modelos o puntos de referencia importantes, influenciando las reformas locales. • Necesidad de Armonización con Estándares Globales: E2 y E3 subrayan la importancia de alinear la legislación local con estándares internacionales, especialmente en el contexto de la globalización de los mercados financieros. • Uso de Legislación Externa para Informar Prácticas Locales: E4 y E6 sugieren que las leyes de otras jurisdicciones son fundamentales para informar y mejorar las prácticas judiciales y legislativas locales.
DISCREPANCIAS	• Diversidad en Modelos de Referencia: Hay una variación en las respuestas sobre qué modelos legislativos internacionales deben ser referenciados, con E1 mirando hacia el Convenio de Budapest y E2 y E3 hacia la protección de datos y estándares de ciberseguridad. • Enfoque en Diferentes Aspectos de la Legislación: Mientras E1 y E4 se centran en la adaptación de modelos legales específicos, E2 y E3 enfatizan la alineación con estándares globales de protección de datos y ciberseguridad.

	• Prioridades en la Adaptación Legal: Existe una variabilidad en las prioridades de adaptación legal, con algunas respuestas (E1, E4) sugiriendo la incorporación de elementos específicos de legislaciones extranjeras, mientras que otras (E2, E3) destacan la importancia de la armonización general con estándares internacionales.
INTERPRETACIÓN	• La Pregunta revela que las normativas y legislaciones de otras jurisdicciones tienen un impacto significativo en la configuración del derecho local sobre ciberdelincuencia. Las coincidencias indican un reconocimiento general de la importancia de referenciar y armonizar con estándares y modelos internacionales. Las discrepancias, sin embargo, reflejan diferentes enfoques sobre qué aspectos de la legislación extranjera deben ser adaptados y cómo. Esto sugiere la necesidad de un enfoque legislativo que equilibre la adaptación de prácticas internacionales probadas con la consideración de las particularidades y necesidades locales, asegurando así una respuesta legal efectiva y contextualizada a los desafíos de la ciberdelincuencia.

Pregunta 26: ¿Existen acuerdos internacionales o convenios que afecten o guíen la legislación nacional sobre delitos informáticos?

E1	E2	E3	E4	E5	E6
Los acuerdos como el Convenio sobre Ciberdelincuencia de Budapest influyen significativamente en nuestra legislación, proporcionando un marco para la cooperación internacional y la persecución de delitos informáticos.	Acuerdos internacionales de protección de datos, como el Escudo de Privacidad UE-EE. UU., juegan un papel crucial en la forma en que nuestra legislación aborda la transferencia y protección de datos personales.	Las resoluciones de la ONU y otros tratados internacionales sobre ciberseguridad y delitos informáticos sirven como guía para nuestras políticas y prácticas legales en esta área.	Los tratados internacionales son fundamentales en la formación de nuestra legislación, especialmente para asegurar la compatibilidad y cooperación en la persecución de delitos transfronterizos.	Iniciativas como la Estrategia Global de Ciberseguridad de la ONU influyen en nuestra legislación, orientando el enfoque hacia una respuesta más integral a los desafíos de la ciberdelincuencia.	Los acuerdos internacionales establecen estándares que nuestra legislación local busca cumplir o superar, especialmente en áreas como la lucha contra el terrorismo cibernético y la protección de infraestructuras críticas.

ANÁLISIS

COINCIDENCIA	• Relevancia del Convenio sobre Ciberdelincuencia de Budapest: Las respuestas E1 y E3 señalan la influencia significativa del Convenio de Budapest en la formación de la legislación local, destacando su papel como un marco para la cooperación internacional. • Influencia de Tratados Internacionales: E2 y E4 coinciden en que tratados internacionales y resoluciones de la ONU guían y afectan la legislación local, especialmente en lo que respecta a la ciberseguridad y la lucha contra los ciberdelitos. • Estándares Globales en la Legislación Local: E5 y E6 sugieren que los estándares establecidos por acuerdos internacionales sirven como puntos de referencia para la legislación local, garantizando la compatibilidad y cooperación global.
DISCREPANCIAS	• Diferencia en Acuerdos Específicos Referenciados: Mientras E1 y E3 destacan el Convenio de Budapest, E2 y E4 se enfocan en la influencia de tratados y resoluciones más generales de la ONU, mostrando diferencias en los acuerdos internacionales considerados más relevantes.

	• Enfoque en Protección de Datos vs. Cooperación en la Persecución de Delitos: Existe una variación en el enfoque de los acuerdos, con algunas respuestas (E2, E4) enfocándose en la protección de datos y otras (E1, E3) en la cooperación para la persecución de delitos. • Variedad en la Interpretación del Impacto de los Acuerdos: Las respuestas reflejan diferentes interpretaciones del impacto de estos acuerdos en la legislación local, desde la adaptación directa de normativas (E1, E3) hasta la influencia más general en la formación de políticas (E5, E6).
INTERPRETACIÓN	• La Pregunta destaca la importancia crítica de los acuerdos internacionales en la formación de la legislación nacional sobre delitos informáticos. Las coincidencias revelan un consenso en que estos acuerdos proporcionan marcos esenciales para la cooperación y la armonización legislativa. Las discrepancias, sin embargo, indican diferentes perspectivas sobre qué acuerdos son más influyentes y cómo se integran en la legislación local. Esto sugiere la necesidad de un enfoque legislativo que considere tanto la cooperación internacional como la protección de datos, equilibrando la adopción de estándares globales con las necesidades y realidades locales en la lucha contra la ciberdelincuencia.

Pregunta 27: ¿Considera necesario establecer más colaboraciones internacionales para fortalecer la legislación local en este ámbito?

E1	E2	E3	E4	E5	E6
Dada la naturaleza transfronteriza de muchos ciberdelitos, es imperativo establecer más colaboraciones internacionales para desarrollar una legislación más efectiva y coherente a nivel local.	Las colaboraciones internacionales son esenciales para entender las tendencias globales en ciberdelincuencia y adaptar nuestra legislación para proteger mejor nuestras instituciones financieras.	Más colaboración internacional facilitaría el intercambio de información y mejores prácticas, lo que es crucial para formular una legislación local más robusta y preparada para enfrentar los retos del ciberespacio.	La colaboración internacional no solo es necesaria, sino vital para garantizar que nuestra legislación sea efectiva y relevante en el contexto global de la ciberdelincuencia.	Fomentar la colaboración internacional podría ayudar a cerrar las brechas en nuestra legislación, especialmente en términos de jurisdicción y persecución de delitos informáticos complejos.	La colaboración internacional es clave para enfrentar los ciberdelitos modernos. Nos permite aprender de otros países y adaptar soluciones innovadoras a nuestro contexto legal.

ANÁLISIS

COINCIDENCIA	• Importancia de la Colaboración Internacional: Las respuestas E1, E4, y E6 coinciden en la necesidad crítica de aumentar la colaboración internacional para enfrentar eficazmente los delitos informáticos, subrayando su naturaleza transfronteriza. • Colaboraciones para Abordar Desafíos Globales: E2 y E3 destacan que las colaboraciones internacionales son esenciales para comprender y adaptarse a las tendencias globales en ciberdelincuencia. • Influencia en la Legislación Local: E3 y E5 sugieren que la colaboración internacional podría ayudar a cerrar brechas en la legislación local, mejorando la eficacia en la lucha contra los ciberdelitos.
DISCREPANCIAS	• Enfoque en Aspectos Específicos de la Colaboración: Hay diferencias en el enfoque de las colaboraciones, con E1 enfocándose en la persecución de delitos, mientras que E2 y E3 en la comprensión y adaptación a las tendencias globales. • Diversidad en la Percepción de la Necesidad de Colaboración: Mientras algunas respuestas (E4, E6) ven la colaboración internacional como fundamental, otras (E1, E3) sugieren que es importante, pero no la única solución. • Variabilidad en la Implementación de Colaboraciones: Las respuestas reflejan diferentes opiniones sobre cómo se deberían implementar las colaboraciones internacionales, con E5 y E6 sugiriendo una integración más directa en la legislación local, mientras que E2 y E3 enfatizan la importancia de la adaptación y el intercambio de conocimientos.
INTERPRETACIÓN	• La Pregunta resalta un consenso general sobre la importancia de fortalecer las colaboraciones internacionales para mejorar la legislación local en el ámbito de los delitos informáticos. Estas colaboraciones son vistas como esenciales para abordar la naturaleza global de la ciberdelincuencia y para adaptar eficazmente las leyes locales a los desafíos emergentes. Las discrepancias en las respuestas indican variadas perspectivas sobre cómo se deben implementar estas

	colaboraciones, reflejando un equilibrio entre la adopción de mejores prácticas internacionales y la adaptación a las realidades y necesidades específicas de cada jurisdicción. Esto sugiere la importancia de un enfoque colaborativo y adaptativo en la legislación sobre ciberdelincuencia.