FACULTAD DE DERECHO Y CIENCIAS POLÍTICAS

CRECIMIENTO DE LOS DELITOS INFORMÁTICOS EN LA MODALIDAD DE SUPLANTACIÓN DE IDENTIDAD, FACILITADOS POR LA VENTA AMBULATORIA DE CHIPS MÓVILES, LIMA 2020-2025

TRABAJO DE SUFICIENCIA PROFESIONAL

Para optar el título profesional de Abogado

AUTOR

Rodriguez Peña, Gonzalo

https://orcid.org/0009-0009-9092-7865

ASESOR

Mtro. Torero López, Gillmar Alejandro

https://orcid.org/0009-0000-1304-7092

Lima-Perú 2025

Visualizador de documentos

Turnitin Informe de Originalidad

Procesado el: 24-jul-2025 3:07 p. m. -05
Identificador: 2720044304
Número de palabras: 21185
Entregado: 1

CRECIMIENTO DE LOS DELITOS INFORMÁTICOS EN LA... Por - -

Índice de similitud	Similitud según fuente	
22%	Fuentes de Internet:	12%
	Publicaciones:	3%
	Trabajos del estudiante:	20%

excluir citas | incluir bibliografía | excluyendo las coincidencias < 12 de las palabras | modo:
ver informe en vista quickview (vista clásica) | imprimir | actualizar | descargar

Coincidencia del 13% (trabajos de los estudiantes desde 16-mar-2025)
Clase: Quick Submit
Ejercicio: Quick Submit
Nº del trabajo: 2615614938

Coincidencia del 3% (Internet desde 23-nov-2024)
https://lpderecho.pe/ley-delitos-informaticos-ley-30096/?f_link_type=f_linkinlinenote&need_sec_link=1&sec_link_scene=i

Coincidencia del 1% (Internet desde 04-jul-2025)
https://lpderecho.pe/ley-delitos-informaticos-ley-30096/

Coincidencia del 1% (Internet desde 07-mar-2024)
http://repositorio.uigv.edu.pe

Coincidencia del <1% (trabajos de los estudiantes desde 08-mar-2025)
Submitted to Universidad Inca Garcilaso de la Vega on 2025-03-08

Coincidencia del <1% (trabajos de los estudiantes desde 04-ene-2025)
Submitted to Universidad Inca Garcilaso de la Vega on 2025-01-04

Coincidencia del <1% (trabajos de los estudiantes desde 11-ene-2025)
Submitted to Universidad Inca Garcilaso de la Vega on 2025-01-11

Coincidencia del <1% (trabajos de los estudiantes desde 17-mar-2023)
Submitted to Universidad Inca Garcilaso de la Vega on 2023-03-17

Coincidencia del <1% (trabajos de los estudiantes desde 14-mar-2023)
Submitted to Universidad Inca Garcilaso de la Vega on 2023-03-14

Coincidencia del <1% (trabajos de los estudiantes desde 08-nov-2023)
Submitted to Universidad Inca Garcilaso de la Vega on 2023-11-08

Coincidencia del <1% (Internet desde 23-jun-2025)
https://lpderecho.pe/codigo-penal-peruano-actualizado/?utm=

Coincidencia del <1% (Internet desde 17-oct-2023)
http://repositorio.uigv.edu.pe

Coincidencia del <1% ()
Vasquez Ramos, David Francisco. "Regulación del "acoso" comercial en el Perú: en búsqueda de tentativas de solución", 'Baishideng Publishing Group Inc.', 2022

Coincidencia del <1% ()
Alejandro Flores, Lina Bertha. "El flasheo digital de equipos móviles como agravante en el delito de receptación, Lima, 2022", 'Universidad Cesar Vallejo', 2023

Coincidencia del <1% ()
Rimaicuna Torres, Mareli Fiorella. "Incorporación de las consecuencias nocivas del deepfake como agravantes del delito de suplantación de identidad en la Ley N° 30096", 'Universidad Cesar Vallejo', 2021

Coincidencia del <1% ()
Quispe Ayala, Victor Faustino, Quispe Saire, Laura Sofia. "Análisis jurídico de la ineficacia de la Ley N°30096 en el delito de suplantación de identidad por medios informáticos", 'Universidad Cesar Vallejo', 2023

Coincidencia del <1% (Internet desde 29-ene-2024)
http://intra.uigv.edu.pe

Coincidencia del <1% (Internet desde 15-mar-2024)
http://intra.uigv.edu.pe

Coincidencia del <1% (Internet desde 04-mar-2024)
http://intra.uigv.edu.pe

Coincidencia del <1% (Internet desde 05-sept-2023)
https://cdn.www.gob.pe/uploads/document/file/4797381/Nueva%20Compilaci%C3%B3n%20Normativa%20Migratoria.pdf

Coincidencia del <1% (Internet desde 26-jun-2022)
https://cdn.www.gob.pe/uploads/document/file/2941907/CYBERDELITO%20VOL%201%2017x24_compressed.pdf.pdf

Coincidencia del <1% (Internet desde 20-jun-2024)
http://tesis.unap.edu.pe

Coincidencia del <1% (Internet desde 13-sept-2023)

DEDICATORIA

A Dios, por ser mi guía, mi fuerza y mi fuente inagotable de sabiduría. Gracias por darme la perseverancia y la fe necesaria para alcanzar este momento tan significativo en mi vida.

A mi madre Felicita Peña Monzón y mi esposa, Luz Mezarina Castañeda, por su apoyo constante, amor incondicional y sus sacrificios, a mis hijos Karla y Jair, mis nietos Emilia y Thiago, que han sido mi inspiración, a mi abuela, tío Lucho y mi hermana Mari quien nos dejó en pleno proceso del proyecto, así como a toda mi familia; mis sueños no podrían haber sido construidos sin su apoyo. Debo este logro a ustedes tanto como a mí.

Con amor y la más profunda gratitud.

AGRADECIMIENTO

Agradezco a Dios, por la vida, salud y fuerza espiritual que me brinda durante todo este tiempo para poder salir adelante y culminar con éxito este trabajo.

Mi más sincero agradecimiento a la Universidad Inca Garcilaso de la Vega, por permitirme formar parte de un entorno académico notable. La universidad ha sido un lugar de desarrollo profesional para mí, brindando oportunidades de crecimiento y me ha equipado con las herramientas necesarias para afrontar los desafíos de mi carrera.

Asimismo, me gustaría expresar mi agradecimiento a mi asesor, el Maestro Gillmar Alejandro Torero López, por su extraordinaria asistencia, orientación y compromiso durante el desarrollo de la presente investigación. Su conocimiento, paciencia y compromiso han sido clave para el progreso de este proyecto. Gracias por sus comentarios constructivos, así como por su constante disposición para guiarme en cada etapa de este proceso.

Gracias por ser parte de este importante capítulo de mi vida académica.

RESUMEN

La presente investigación tiene como objetivo principal analizar cómo la venta informal de chips móviles influye legalmente en el aumento de los delitos informáticos, en particular en los casos de suplantación de identidad, y plantear reformas legales que refuercen la protección de los derechos de los ciudadanos en el Perú. Metodológicamente, se trata de una investigación de enfoque cualitativo, la cual utilizó la entrevista, análisis documental y el focus group (grupo focal) como técnicas de recolección de datos, además utilizó el software Atlas.ti para el procesamiento de la información proveniente de la aplicación de las entrevistas realizadas a cinco (05) especialistas en materia de delitos informáticos y en manejo y gestión de TICs. Como resultado se obtuvieron propuestas de solución desde un enfoque tripartito: social (concientización comunitaria y prevención), institucional (el rol de las empresas de servicios de telefonía móvil) y legislativo (principios jurídicos orientadores y mejora integral). Concluyendo que, existe la necesidad de sistemas avanzados de trazabilidad y control como *blockchain* y verificación de geolocalización en tiempo real para la distribución y monitoreo de activaciones de chips móviles. Tales sistemas permitirían a las autoridades prevenir y localizar actividades ilícitas de dispositivos móviles, manteniendo así la integridad durante el proceso de activación.

Palabras clave: Comercio ilícito, datos personales, delitos cibernéticos, dispositivos móviles, protección de información.

Growth in computer crimes in the modality of identity theft, facilitated by the ambulatory sale of mobile chips, Lima 2020-2025

ABSTRACT

The main objective of this research is to analyze how the informal sale of mobile chips legally influences the increase in cybercrimes, particularly in cases of identity theft, and to propose legal reforms that reinforce the protection of citizens' rights in Peru. Methodologically, it is a qualitative approach research, which used interviews, documentary analysis and focus groups as data collection techniques, and also used Atlas.ti software to process information from the application of interviews with five (05) specialists in cybercrimes and ICT management and management. As a result, solution proposals were obtained from a tripartite approach: social (community awareness and prevention), institutional (the role of mobile phone service companies) and legislative (guiding legal principles and comprehensive improvement). Concluding that there is a need for advanced traceability and control systems such as blockchain and real-time geolocation verification for the distribution and monitoring of mobile chip activations. Such systems would allow authorities to prevent and track illicit activity on mobile devices, thereby maintaining integrity during the activation process.

Keywords: Illicit trade, personal data, cybercrime, mobile devices, information protection.

ÍNDICE GENERAL

INTRODUCCIÓN

Hoy en día, el desarrollo de la tecnología digital está dejando oportunidades y riesgos para la protección de la información personal. En particular, los delitos informáticos, tales como la suplantación de identidad, han ido en aumento en los últimos años y han impactado tanto a individuos como a empresas. La suplantación de identidad se refiere al delito que utiliza datos personales de un individuo de manera fraudulenta con el fin de obtener ganancias ilícitas, tales como apertura de cuentas bancarias, compras, e incluso el acceso a diversos servicios. Este tipo de delitos ha cambiado rápidamente debido a la sobreexplotación de las vulnerabilidades digitales, así como la implementación de redes sociales y otros canales electrónicos que han vuelto difícil su prevención y control.

Algo que ha llevado la suplantación de identidad al extremo en Lima ha sido el comercio informal de chips de teléfono móvil. Esta clandestina actividad es la más reciente forma de venta llamada a la venta de datos personales. Los vendedores informales de chips móviles, o "munches" en la jerga de Lima, efectuaban estas transacciones sin cotejar las identidades de los compradores, con lo que se hacían propietarios de datos muy delicados. Delincuentes han comenzado a utilizar lo que inicialmente se consideraba una manera de conseguir una tarjeta SIM, que facilitaba el acceso a diferentes servicios de telefonía celular, para realizar estafas mucho más sofisticadas. Mediante estos chips se puede activar un aparato celular bajo una identidad falsa con la que se puede suplantar a otra persona y así realizar diversos tipos de fraudes: estafas virtuales, compras no autorizadas, o incluso acceder a cuentas bancarias.

La modalidad que abarca delitos informáticos ha experimentado un crecimiento acelerado durante los últimos años. Este fenómeno, a su vez, ha generado enormes problemas de control para las autoridades debido a la falta de regulación y supervisión adecuada en torno a este tipo de ventas informales. Asimismo, se suma el alto índice migratorio hacia Lima y la acumulación de sectores vulnerables en la zona periférica de la ciudad, lo que ayuda a la propagación de estas conductas delictivas. Este análisis pretende ilustrar los casos de venta informal de eclipses de números de identidad en chips telefónicos y cómo estos apuntan al aumento de delitos de suplantación de identidad entre 2020 y 2025, utilizando un enfoque cualitativo para el análisis de todos los elementos que se relacionan, como la infraestructura social y económica.

La investigación se sitúa dentro de un marco cualitativo ya que intenta explicar las percepciones, razones y otros elementos de la motivación detrás de este crimen en lugar

de testimonios de todos los participantes en los procesos, sean víctimas o delincuentes, así como especialistas en el campo. Se puede construir un entendimiento exhaustivo del tema a partir del problema a través de entrevistas y análisis de documentos, así como revisando estudios de casos previos.

La evidencia está compuesta de transcripciones de entrevistas, informes, expedientes de casos y otros documentos que se encuentran dentro de los límites establecidos por los objetivos de la investigación, incluidos la literatura relevante publicada y no publicada y las obras de medios.

Este trabajo se compone de cinco capítulos que se desarrolla progresivamente y expone los diversos aspectos del estudio en detalle. En el Capítulo I, "El Marco Teórico de la Investigación", se comienza con el relato del contexto histórico dentro del cual han surgido los delitos informáticos a lo largo de los años. A continuación, se presentan los principios fundamentales del estudio junto con el marco legal pertinente y el trasfondo de investigaciones previas sobre el tema, que también debe incluir las definiciones del marco conceptual necesario para formular el estudio.

En el Capítulo II único, "Planteamiento Del Problema", se narra la problemática circunscrita al fenómeno: venta ambulante de chips móviles en su conjunto, estudiando sus características y consecuencias, así como su alcance de crecimiento en delitos informáticos. También se plantea el problema general y los específicos, además de los objetivos de esta investigación.

En el Capítulo III "Justificación y Delimitación de la Investigación" se analiza el propósito de dicha investigación desde el punto de vista social, en especial, para el ámbito forense y los organismos de seguridad y protección de datos de carácter personal. Se precisan las delimitaciones del estudio, los alcances, límites geográficos y temporales de la investigación.

En el Capítulo IV "Formulación Del Diseño" se expone el diseño metodológico de la investigación. En él se aborda lo básico del diseño, la metodología del estudio, la estructura y los medios de recolección de datos.

Finalmente, en el Capítulo V, "Prueba del Diseño," se aplican las soluciones a los problemas que surgieron durante la investigación. La prueba del diseño evaluará la viabilidad de las medidas correctivas y preventivas propuestas para disminuir la venta ambulante de chips móviles y el robo de identidad vinculado a ello. El capítulo finalizará con conclusiones y recomendaciones basadas en los hallazgos.

CAPÍTULO I: MARCO TEÓRICO DE LA INVESTIGACIÓN

1.1. Marco histórico

La manera en la que los delitos informáticos han evolucionado, en especial la modalidad de suplantación de identidad, ha estado relacionada a los avances de la tecnología digital y la globalización de las comunicaciones. Este fenómeno que se moderniza en la era contemporánea, no solo abarca las formas comunes de fraudes, sino fraudes de nuevas formas que emplean las plataformas digitales y móviles para cometer los delitos. El fraude de suplantación de identidad ha sido llevado a cabo por delincuentes al aprovechar la falta de seguridad y educación digital que existe debido al acceso masivo a Internet y servicios de telecomunicaciones.

1.1.1. La primera fase de los delitos informáticos y cómo han evolucionado.

La historia de los delitos informáticos comienza en los años 60 y 70, cuando el uso de computadoras se expandió a instituciones académicas y gubernamentales. No obstante, la suplantación de identidad, por ejemplo, como modalidad de crimen absorbido por la tecnología, surgió a la par con la digitalización. Brenner, 2007, separa el surgimiento de los delitos informáticos en periodos, considerando el hacking, como el acceso no autorizado a sistemas y datos, el primero, ya desde los 90, con la inclusión de la web, el segundo, ocurriendo durante estos años la mayor diversificación de delitos, considerando el surgimiento de la usanza de hacer transacciones y compartir información en línea.

La suplantación de identidad, según Solms y Niekerk (2013), es un tipo de crimen cibernético donde una persona se hace pasar por otra para acceder a ciertos servicios o cometer actos ilegales. Fragmentos de este problema se unieron con el auge de las redes sociales y trucos más nuevos como el phishing, que ha permitido a los criminales obtener información sensible utilizando engaños electrónicos. Los viejos dispositivos de seguridad digital que los criminales utilizaban para atacar tuvieron que cambiar con el tiempo. Así, los delincuentes aprendieron a manipular y utilizar datos y brechas en la tecnología para eludir las protecciones.

1.1.2. El auge del uso de teléfonos móviles y la venta casual de tarjetas SIM móviles.

Uno de los factores principales que contribuyó al crecimiento del cibercrimen, particularmente la suplantación de identidad, fue el aumento de los teléfonos móviles, y posteriormente, los smartphones en la década de 2000. Con el auge de la globalización, los teléfonos móviles se convirtieron en una necesidad básica para la vida diaria, ya que los usuarios podían abrir sus cuentas bancarias, plataformas de pago, servicios gubernamentales y cuentas de redes sociales desde casi cualquier lugar del mundo en

cualquier momento. Como señala García y Ruiz (2020), cuando los chips móviles fueron vendidos sin regulaciones, se convirtió en una de las formas más importantes de ayudar al fraude porque los delincuentes pudieron obtener números de teléfono que no estaban emitidos o vinculados a ninguna cuenta autenticada. Esto se convirtió en una forma común de ejecutar fraude de identidad, particularmente en países con un control débil sobre la emisión de tarjetas SIM.

La venta no regulada de chips móviles o tarjetas SIM sin ninguna verificación es una práctica que gana popularidad con la disponibilidad de tecnologías de telecomunicaciones. Panadero et al. (2021) afirman que el mercado informal de chips no solo surge de la ausencia de regulación, sino también de la falta de educación pública sobre ciberseguridad que facilita la venta de tarjetas SIM sin ningún control. Una supervisión ineficaz de los mercados informales combinada con un registro de usuarios inadecuado facilitó el acceso de los delincuentes a sistemas financieros y bancarios usando números de teléfono fraudulentos y estándar.

1.1.3. La creciente proliferación de la suplantación de identidad.

A medida que la tecnología móvil se integró más en la vida cotidiana, los delincuentes encontraron nuevas formas de cometer crímenes. La suplantación de identidad se volvió más elaborada con el desarrollo de la banca móvil y otros servicios electrónicos en la década de 2010. El aumento en las transacciones financieras digitalizadas y el comercio electrónico permitió a los delincuentes encontrar nuevas formas de perpetrar fraude, y el uso de teléfonos móviles con chip se convirtió en uno de los métodos más destacados de la suplantación de identidad. Como señaló Schneier (2018), la capacidad de acceder a servicios financieros y plataformas de pago a través de un dispositivo móvil simplificó enormemente la realización de fraudes.

Rodríguez (2021) afirma que, en América Latina, países como Perú parecen estar en una crisis de seguridad en el ciberespacio debido a una relativa ausencia de regulación y control sobre la venta ambulante de chips móviles. El uso de chips no registrados permite a los criminales operar números de teléfono sin que estén vinculados a identidades reales, lo que facilita que un individuo asuma la identidad de alguien más y cometa fraudes electrónicos sin ser detectado. La mayor parte del tiempo, este tipo de fraude se lleva a cabo con la ayuda de la banca móvil o mediante la creación de cuentas bancarias falsas.

1.1.4. Contexto de Perú: La creciente proliferación de la venta de chips móviles y la falta de regulación adecuada.

En Perú, la venta informal de chips móviles y la proliferación de la suplantación de identidad son temas de preocupación creciente. Si bien existe la Ley N° 30096 de 2013, que crea un marco sancionador sobre el fraude mediante dispositivos móviles y la protección de datos personales, su ejecución ha sido precaria. Según Pérez y García (2020), la escasez de recursos y la falta de coordinación entre las autoridades de telecomunicaciones y los cuerpos de seguridad ha propiciado la impunidad de la venta ambulante de chips. En la mayoría de las regiones del país, los chips móviles se continúan vendiendo de manera informal, y sin la debida verificación de la identidad de los compradores, lo cual facilita la proliferación de fraudes financieros y muchos otros delitos de suplantación de identidad.

La falta de acceso a servicios educativos para áreas rurales y urbanas marginadas ha profundizado la vulnerabilidad de los usuarios debido a su ignorancia sobre los riesgos vinculados al uso de dispositivos móviles para la banca y otros servicios digitales. Para Schneier (2018), esto es una 'brecha digital', un vacío donde los criminales operan con impunidad. La negligencia en la educación sobre ciberseguridad ha resultado en una mayor dependencia del fraude habilitado digitalmente, cuyas víctimas no siempre reconocen a quiénes entre ellas tienen los criminales que suplantan a entidades gubernamentales (suplantación de identidad) y estafadores móviles (fraude con chips) como objetivos.

1.1.5. Implicaciones y la necesidad de un cambio legislativo.

A pesar de reconocer el problema del cibercrimen en Perú, especialmente en lo que respeta a la suplantación de identidad, hay muchos obstáculos que deben superarse para la implementación efectiva de la legislación. Las autoridades no han podido hacer cumplir adecuadamente la Ley N° 30096 y, como resultado, las ventas no reguladas de chips continúan siendo una de las mayores amenazas a la seguridad digital del país. Brenner (2007) sugiere que la legislación sobre cibercrimen necesita ser complementada con las reformas necesarias en tecnología y colaboración internacional, que Perú aún no ha implementado de manera efectiva.

1.2. Bases teóricas

El aumento de los ciberdelitos, en particular el fraude de identidad facilitado por la venta ambulante de tarjetas SIM móviles, involucra una combinación sofisticada de derecho penal, informática forense, protección de datos personales y seguridad de sistemas de información. Las tecnologías impulsadas por los clientes, junto con la facilidad con la que los criminales pueden obtener información personal a través de chips móviles no verificados, plantean desafíos reales para el control de los ciberdelitos. Se explica a continuación el desarrollo teórico del fenómeno construido en torno a las principales teorías y trabajos realizados por autores destacados en el campo, al tiempo que se modifica los enfoques previamente existentes mediante un examen elaborado de cada aproximación a las teorías interconectadas.

1.2.1. Teoría General del Ciberdelito.

La Teoría General Del Delito Informático precisa que existe un conjunto de delitos informáticos que se traducen a la utilización de herramientas tecnológicas y digitales. La delimitación de este nuevo campo ha sido mucho mayor con el avance de la tecnología de la información y la expansión de Internet. Para López (2017), estas definiciones de delitos informáticos incluyen no solo el uso de dispositivos electrónicos especializados para la comisión de un delito, sino que también incluyen atributos no materiales del daño causado. Esta teoría es fundamental porque la suplantación de identidad digital, que se facilita a través de la informalidad en la venta de chips móviles, es uno de los fraudes más atractivos que existen, y su naturaleza intangible hace que el daño sea mucho más agravante y casi imposible de cuantificar y reparar.

Brenner (2007) va más allá explicando que el ciberdelito incluye intrusiones electrónicas de hackeo en sistemas, defraudando sistemas y manipulando información a través de Internet. Tales crímenes pueden considerarse delitos transnacionales porque el perpetrador puede estar en cualquier parte del mundo y también pueden estarlo las víctimas. Esto se debe a que muchas fronteras nacionales no cubren la rapidez y facilidad con la que los criminales utilizan nuevas tecnologías para cometer robo de identidad.

En el caso de la venta ambulante de tarjetas SIM de teléfonos móviles, los delincuentes venden números de teléfono no verificados que pueden ser utilizados para suplantar a usuarios reales. Este es un caso claro de fraude que compromete la seguridad personal y financiera. Estos sistemas son vulnerables, expuestos además a brechas en la seguridad general del sistema cibernético, tal como señala Anderson et al. (2013), quienes

enfatizan que los ciberdelitos son posibles debido a las brechas existentes ya la falta de verificación adecuada de los sistemas de telecomunicaciones y digitales.

1.2.2. Teoría del Fraude de Identidad.

El robo de identidad es una forma de ciberdelito cada vez más dañina, especialmente porque se asocia con otros crímenes graves, como el fraude financiero y el robo de datos. Kumar y Mallick (2018) argumentan que el robo de identidad digital se refiere al delito en el cual un infractor, con la intención de cometer actos ilegales bajo la falsa identidad de una víctima, asume la personalidad de la víctima al participar en actividades como realizar compras, solicitar préstamos o transferir dinero desde cuentas bancarias. La venta de chips de teléfonos móviles sin la verificación suficiente de la identidad del comprador permite un nivel aún mayor de actividad fraudulenta.

Sullivan (2016) afirmó que el robo de identidad ha avanzado de contar mentiras por teléfono a utilizar métodos más complejos, como el acceso a sistemas bancarios o de pago electrónico, lo que puede ser extremadamente perjudicial para las víctimas. La venta de tarjetas SIM no verificadas es uno de los medios que utilizan los estafadores para ocultar el engaño debido a la posibilidad de usar el número de teléfono robado o falsificado para establecer perfiles de pagos bancarios y móviles, haciendo así que las estafas sean mucho más fáciles.

El análisis de González examina cómo el robo de identidad puede ser utilizado no solo para fraudes financieros, sino para suplantar a una víctima e infligir daño reputacional y emocional, quien puede pasar por experiencias de desilusión en relación con los sistemas digitales y las instituciones bancarias. El uso no regulado de tarjetas SIM móviles es uno de los medios más comunes para facilitar tales fraudes digitales, ya que las redes móviles y las plataformas electrónicas tienden a ser altamente vulnerables a intrusiones no autorizadas.

1.2.3. Teoría de la Ciberseguridad.

La ciberseguridad es un ámbito interdisciplinario destinado a proteger las redes de información, sistemas informáticos y datos personales de los usuarios contra accesos no autorizados, uso malicioso y otras formas de alteraciones. La teoría de la ciberseguridad define un ataque informático como una perpetración de daño a un sistema informático como consecuencia de debilidades no protegidas que no han sido suficientemente monitoreadas o controladas por las medidas de seguridad.

Schneier (2018) afirma que, en ciberseguridad, los protocolos destinados a

proteger la infraestructura digital y la información de un individuo deben ser integrales. En ese sentido, el robo de identidad puede ser uno de los delitos más graves de cometer debido a la ausencia de mecanismos de verificación en plataformas que permiten realizar transacciones, como en la venta informal de chips móviles.

Pfleeger y Pfleeger (2015) argumentan que la ciberseguridad no solo se ocupa de proteger los sistemas de hackers y otros criminales informáticos, sino también de salvar identidades digitales. Deben implementarse medidas de seguridad en el punto de venta de chips de teléfonos móviles para asegurar que los delincuentes no vendan las características de identidades falsas o no utilizadas para acceder a números de teléfono, ya que esto supone un riesgo para los sistemas financieros.

Para evitar el fraude por suplantación, los investigadores subrayan la necesidad de desarrollar tecnologías de autenticación de identidad en sistemas de pago móviles y electrónicos. García y Ruiz (2020) enfatizan que la verificación biométrica combinada con la autenticación multifactor tiene el potencial de mitigar el riesgo de fraude debido a la mayor dificultad para que los criminales accedan a plataformas de pago bajo identidades disfrazadas.

1.2.4. Teoría del Derecho Penal Informático.

Esta especialización se ocupa de la regulación de los delitos cometidos por medio de la tecnología de la información y surge del aumento de los delitos informáticos. La teoría del derecho penal informático argumenta que los delitos cibernéticos deben ser legislados en el contexto del fraude digital y la decepción de identidad. Como afirma González (2019), la falta de una legislación penal adecuada para abordar tales delitos se debe a que las leyes tradicionales son incapaces de lidiar con la velocidad y el alcance internacional de los delitos digitales.

En el caso del fraude de identidad a través de la venta de chips móviles, Código Penal Peruano (Art. 438) establece que las personas que acceden fraudulentamente a la información personal deben ser encarceladas. Brenner (2007) refuerza esta posición, enfatizando que no existía una única forma de fraude en el mundo digital que los legisladores estaban trabajando para abordar, lo cual era un requisito constante para todas las leyes. “Siempre hay cambios para asegurar que las leyes aborden cada una de las formas de delito, particularmente el fraude”.

Solms y Niekerk (2013) señalan que el principal problema es la velocidad a la que están cambiando las leyes sobre delitos cibernéticos en comparación con la tecnología. Generalmente hay una brecha entre las leyes nacionales y los avances en tecnología, y

esto conduce a vacíos legislativos que los criminales pueden utilizar, como la venta informal de chips móviles.

1.2.5. Teoría del Comercio Electrónico y el Mercado de Chips de Teléfonos Móviles.

El comercio electrónico ha cambiado la forma en que las personas compran, venden o realizan transacciones. Rodríguez (2021) señala que el mercado de chips de teléfonos móviles es uno de los más importantes en la intersección de las telecomunicaciones y las finanzas móviles, y su regulación sigue siendo un problema, particularmente en lo que respeta a la identificación del comprador.

Panadero y col. (2021) explican cómo el mercado informal de chips de teléfonos móviles permite a los criminales obtener números de teléfonos celulares en el extranjero, que luego se utilizan para fraudes a través de plataformas bancarias y redes sociales. La falta de control en la venta de estos dispositivos es un factor muy importante que permite y facilita el robo de identidad y el fraude.

1.2.6. Teoría de la Criminalidad Digital.

La criminalidad digital se ha desarrollado de una forma primaria de cibercriminalidad a una actividad sofisticada que se perpetra mediante el uso de la tecnología. Según Fuchs (2017), la criminalidad digital es una forma de crimen transfronterizo que no se limita al hacking, sino que se extiende para incluir el fraude cibernético, el robo de identidad, el phishing y la suplantación. Fuchs argumenta que, dentro del proceso de digitalización social, el delito se desplaza del espacio físico a un ámbito virtual, lo que permite que se lleve a cabo sin restricciones geográficas.

Los delincuentes ahora operan de manera global, y suplantar la identidad se ha convertido en un delito que aumenta día con día, todo debido a la falta de verificación sistemática para comprar tarjetas SIM. Como se menciona en Wall (2007), los delincuentes informáticos utilizan los sistemas electrónicos y las plataformas de comercio en línea para generar fraude digital y estafas. En cuanto al contexto peruano, Brenner (2007) ilícitamente ha marcado esta forma de fraude como criminalidad digital. No solo se trata de la falta de control, sino también de falta de orden al poder vender chips móviles. La falta de control permite relativamente fácil generar fraudes y tener acceso a datos personales sin consentimiento de las víctimas. Debido a la gran falta de orden en la venta ambulante de chips móviles, Perú se ha convertido en un foco de criminalidad digital.

En cuanto a fomentar la prevención, se necesita primero desarrollar un marco sistemático que se acople a los avances de la tecnología. Las leyes tradicionales van a

quedar obsoletas con el avance de los sistemas de justicia y la política pública. Al no tener un orden establecido, brinda la oportunidad a los sistemas de seguridad de ser constantemente vulnerables al ser usados para llevar a cabo delitos de suplantación de identidad.

La psicología del cibercrimen proporciona una visión que examina los motivos y factores psicológicos subyacentes que llevan a las personas a cometer delitos, especialmente aquellos que involucran fraude como el robo de identidad. Cohen y Felson (1979) presentaron la teoría de oportunidades en criminología que establece que los delitos se cometen cuando hay circunstancias favorables para los perpetradores, que se perciben como de bajo riesgo y alta ganancia. Este principio es muy cierto para el cibercrimen porque la facilidad de acceso a la información personal, así como las mínimas restricciones sobre la venta de chips móviles, crean oportunidades para que el robo de identidad prospere.

Gibbs (2019) argumenta que la psicología de un hacker informático se basa en sentimientos de anonimato y falta de consecuencias inmediatas, lo que a veces puede disminuir el sentido de culpa de los infractores. Este sentimiento de anonimato se acentúa aún más en las ventas informales de chips de teléfonos móviles donde los criminales obtienen números de teléfonos no verificados y los utilizan para defraudar a otros sin ser fácilmente identificables. La ignorancia percibida, junto con poco control sobre los sistemas de telecomunicaciones, facilita y hace más tentador cometer fraude de identidad. La psicología social también juega un gran papel en la aceptación de cuentos fraudes en culturas particulares. Young (2014) observa que los participantes del cibercrimen a menudo experimentan una desconexión moral y, por lo tanto, no aprecian el daño infligido a las víctimas. Este fenómeno ayuda a explicar la persistencia de los
ladrones de identidad que sienten poca o ninguna culpa.

Una de las cosas que facilitan cometer fraude de identidad en línea es la venta ilegal de información personal. El mercado negro de información personal, especialmente en la web oscura, se ha diversificado. Números de tarjetas de crédito, números de teléfono, contraseñas y otra información sensible se están vendiendo en bases de datos por buenas sumas de dinero. Según Mann (2014), la falta de control en la recolección de datos es responsable de este tipo de comercio ilegal, así como la facilidad con la que los criminales pueden obtener información personal a través de phishing, hacking y compra de tarjetas de teléfono prepagadas no verificadas.

El uso de chips móviles no registrados o robados con el propósito de cometer fraude es común en el negocio del fraude de identidad. La compra de tarjetas SIM en

mercados informales con números de teléfonos falsos permite a los estafadores suplantar a otra persona y realizar transacciones bancarias o comprar bienes o prestar dinero. Este tipo de uso indebido de la información personal debido al anonimato en Internet destruye la confianza en el ciberespacio. Estos tipos de mercados tienen un impacto muy negativo en la banca móvil y las industrias de comercio electrónico.

1.2.7. Teoría de la Protección de Datos Personales.

La protección de datos personales es uno de los temas más importantes respecto al robo de identidad. Warren y Brandeis (1890) fueron los primeros en desarrollar el concepto del derecho a la privacidad, que ha sido incorporado con mucha flexibilidad en la legislación contemporánea que protege los datos personales de los ciudadanos. Como afirma Solove (2021), la protección de los datos personales va más allá de la seguridad de la recolección y su almacenamiento; También significa asegurar que las personas controlen cómo se utiliza su información.

Con vendedores ambulantes que venden chips móviles, la falta de verificación de identidad para adquirir una tarjeta SIM viola directamente la privacidad del usuario. González (2019) señala que la Ley de Protección de Datos en Perú (Ley N° 29.198) estipula que las empresas de telecomunicaciones deben registrar de manera segura la información personal del usuario, sin embargo, la venta no controlada e ilegal de tarjetas SIM representa una amenaza de seguridad por robo de identidad y fraude. Según Schneier (2018), la protección de los datos de información personal es ineficaz sin sistemas de autenticación y verificación de identidad robustos que deben implementarse a lo largo de toda la cadena de valor de los servicios tecnológicos y de telecomunicaciones.

1.2.8. Teoría del Crimen Transnacional.

La criminalidad transnacional es un fenómeno que permite a un delincuente informático operar en varios países al mismo tiempo. Shelley (2005) menciona que ciertos delitos, tales como el abuso de identidad, son difíciles de perseguir debido a que las fronteras geográficas no son un límite para el uso de tecnologías digitales. Delitos informáticos, tales como el uso fraudulento de números telefónicos por medio de la venta ambulante de chips móviles, permiten a los criminalistas estafadores el uso de identificaciones telefónicas ficticias sin ser localizados. Esto facilita el fraude y complica su persecución a nivel internacional.

Panadero y col. (2021) advierten que un amenazante nivel de fraude puede ser llevado a cabo por computadoras que utilizan móviles sin registrarse porque se pueden usar sin limitación geográfica, junto con la tecnología de chips inscriptores que no requieren de un documento de identidad. Esos informáticos gozan de libertad total, siempre y cuando trabajan a través de plataformas digitales que no requieren geolocalización. La lucha contra la criminalidad transnacional exige que todas las instancias colaboren entre sí, como sugieren Baker y colaboradores.

1.3. Marco legal

El marco legal que cubre el delito informático, especialmente el robo de identidad facilitado por la explotación y venta de chips de teléfonos móviles, incorpora una multitud de regulaciones nacionales e internacionales que buscan salvar la información privada del individuo, controlar la industria de las telecomunicaciones y castigar el cibercrimen. La adecuada aplicación de este marco legal es fundamental para garantizar la seguridad en la prestación de servicios digitales y proteger a los usuarios del fraude en un entorno altamente susceptible como la venta informal o casual de chips móviles.

1.3.1. Constitución Política del Perú.

La versión de la Constitución Política del Perú de 1993, que fue actualizada por última vez en 2005, incluye una sección sobre la violación de la privacidad de una persona y se relaciona con la tecnología y las comunicaciones electrónicas. El artículo 2 se refiere a los Derechos Fundamentales de los individuos, en el párrafo 5, menciona que:

Toda persona tiene derecho a la inviolabilidad de su domicilio, a la privacidad de sus comunicaciones, así como a la protección de sus datos personales.

Este derecho crea las condiciones para la protección de datos personales y las comunicaciones a través de Internet y dispositivos electrónicos. Solo, en el caso de identidades asumidas, la constitución garantiza a la persona cuya identidad se utiliza que sus datos personales serán respetados y protegidos. Esta garantía se fusiona con todas las plataformas y servicios en línea, incluidos los servicios de telefonía móvil y banca electrónica, donde la identidad del usuario puede ser fácilmente abusada. La ausencia de control en la venta en la calle de chips móviles es un ejemplo flagrante de la deficiencia de estos derechos fundamentales de protección de la privacidad.

1.3.2. Ley N° 30096 – Ley sobre delitos informáticos.

La Ley N° 30096 es la pieza legislativa más importante en Perú en relación con los delitos informáticos. Se aprobó el 21 octubre de 2013. Su propósito es:

Definir procedimientos legales y penales para calificar y sancionar delitos informáticos.

Esta ley aborda una variedad de delitos informáticos, incluidos fraudes electrónicos, piratería informática, robo de datos y robo de identidad. El robo de identidad, siendo uno de los delitos informáticos más comunes, se aborda de manera directa en esta legislación.

La Ley N° 30096 establece que se puede infraccionar a los autores por delitos cometidos en el ciberespacio; sin embargo, se les pueden imponer sanciones privativas de libertad y multas privativas de libertad. Este tipo de leyes son condenatorias, debido al abuso que ocurre con el uso indebido de datos personales. (García y Ruiz, 2020).

Artículo 2. Acceso ilícito*

El que deliberada e ilegítimamente accede a todo o en parte de un sistema informático, o se excede en lo autorizado, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días-multa.

Si el agente accede deliberada e ilegítimamente, en todo o en parte, al sistema informático vulnerando las medidas de seguridad establecidas para impedirlo, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días-multa.

* Artículo modificado por el artículo 2 del DL 1614, publicado el 21 de diciembre de 2023.

Artículo 8. Fraude informático*

El que deliberada e ilegítimamente procura para sí o para otro un provecho ilícito en perjuicio de tercero mediante el diseño, introducción, alteración, borrado, supresión, clonación de datos informáticos, suplantación de interfaces o páginas web o cualquier interferencia o manipulación en el funcionamiento de un sistema informático, será reprimido con una pena privativa de libertad no menor de cuatro ni mayor de ocho años y con sesenta a ciento veinte días-multa.

La pena será privativa de libertad no menor de cinco ni mayor de diez años y de ochenta a ciento cuarenta días multa cuando se afecte el patrimonio del Estado destinado a fines asistenciales o a programas de apoyo social.

La misma pena se aplica al que intencionalmente colabora con la comisión de alguno de los supuestos de los párrafos precedentes, facilitando la transferencia de activos.

* Artículo modificado por el artículo 2 del DL 1614, publicado el 21 de diciembre de 2023.

Artículo 9. Suplantación de identidad*

El que, mediante las tecnologías digitales suplanta la identidad de una persona natural o jurídica, siempre que de dicha conducta resulte algún perjuicio, material, moral o de cualquier otra índole, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años.

La pena privativa de libertad es no menor de seis ni mayor de nueve años cuando se suplante la identidad de una persona menor de 18 años de edad y resulte algún perjuicio, material, moral o de cualquier otra índole.

* Artículo modificado por el artículo 2 del DL 1591, publicado el 13 de diciembre de 2023.

Artículo 10. Abuso de mecanismos y dispositivos informáticos*

El que deliberada e ilegítimamente fabrica, diseña, desarrolla, vende, facilita, distribuye, importa u obtiene para su utilización, uno o más mecanismos, programas informáticos, dispositivos, contraseñas, códigos de acceso o cualquier otro dato informático, específicamente diseñados para la comisión de los delitos previstos en la presente Ley, o el que ofrece o presta servicio que contribuya a ese propósito, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días-multa.

* Artículo modificado por el artículo 1 de la Ley 30171, publicada el 10 de marzo de 2014.

Artículo 11. Agravantes

El juez aumenta la pena privativa de libertad hasta en un tercio por encima del máximo legal fijado para cualquiera de los delitos previstos en la presente Ley cuando:

1. *El agente comete el delito en calidad de integrante de una organización criminal.*
2. *El agente comete el delito mediante el abuso de una posición especial de acceso a la data o información reservada o al conocimiento de esta información en razón del ejercicio de un cargo o función.*
3. *El agente comete el delito con el fin de obtener un beneficio económico, salvo en los delitos que prevén dicha circunstancia.*
4. *El delito compromete fines asistenciales, la defensa, la seguridad y la soberanía nacionales.*

1.3.3. Ley N° 29733 - Ley de Protección de Datos Personales.

Esta ley fue promulgada el 11 de julio de 2011 y establece la Ley N° 29733 de Protección de Datos Personales. Esta ley contiene normas para la obligación de proteger la información personal. Previendo el posible fraude, los datos personales deben ser procesados por personas que estén debidamente autorizadas. Esta ley fue creada para evitar que los comerciantes de chips móviles recopilen y abusen de la información personal de los consumidores sin consentimiento.

El artículo 3 de esta ley establece que los datos de una persona incluyen cualquier información que pueda ser utilizada para identificarla, como su nombre, dirección, número de teléfono y cualquier otra información vinculada a la identidad de esa persona. El artículo 13 numeral 5 de la ley indica que se requiere un consentimiento explícito del titular para procesar los datos, y establece que la empresa que recopila los datos debe asegurarse de que los datos recopilados solo se usarán para el propósito para el cual fueron recopilados.

Artículo 13. Alcances sobre el tratamiento de datos personales

13.5. Los datos personales solo pueden ser objeto de tratamiento con consentimiento de su titular, salvo ley autoritativa al respecto. El consentimiento debe ser previo, informado, expreso e inequívoco.

Con respecto a la venta de chips de teléfonos móviles, esta ley estipula que los compradores deben ser notificados de manera clara y en un lenguaje inequívoco sobre lo que sucederá con sus datos personales. Estos autores señalan que la verificación de identidad (o comprobación de identidad) es deficiente al vender chips móviles, lo que lleva a una pobre aplicación de la ley que permite el fraude de identidad.

Artículo 14.- Consentimiento y datos sensibles.

Tratándose de datos sensibles, el consentimiento debe ser otorgado por escrito, a través de su firma manuscrita, firma digital o cualquier otro mecanismo de autenticación que garantice la voluntad inequívoca del titular.

Artículo 28. Obligaciones

4. No utilizar los datos personales objeto de tratamiento para finalidades distintas de aquellas que motivaron su recopilación, salvo que medie procedimiento de anonimización o disociación.

1.3.4. Código Penal Peruano.

En el artículo 438-A del código penal peruano, relativo a la falsedad genérica agravada por la emisión de títulos académicos o profesionales ficticios, tiene una conexión, aunque indirecta, sustantiva con la problemática de suplantación de la identidad en el entorno digital. La venta no controlada de tarjetas de chips telefónicas permite la creación

de líneas anónimas o falsas por parte de personas que no tienen que someterse a un control estricto identificativo. Tales líneas pueden ser utilizadas en la organización y ejecución de diversas actividades delictivas, tales como la expedición y distribución de documentos fraudulentos, constancias académicas o profesionales.

Por lo tanto, queda claro que la desatención de las reglas de orden y control en la oferta y venta de los chips telefónicos se constituye en una estufa que alimenta la expansión de delitos como la suplantación de identidad, la falsedad documental, y otros delitos informáticos, los cuales conjuntamente la venta informal de SIM y la venta de títulos profesionales adquieren un carácter ostensible de criminalidad en el entorno digital, académico, y profesional.

Artículo 438-A.- Falsedad genérica agravada*

El que otorgue, expida u oferte certificados, diplomas u otras constancias que atribuyan grado académico, título profesional, título de segunda especialidad profesional, nivel de especialización u otra capacidad análoga, sin que el beneficiario haya llevado efectivamente los estudios correspondientes, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años y sesenta a ciento cincuenta días-multa.

* Artículo incorporado por el DL 1351, publicado el 7 de enero de 2017.

1.3.5. El Contexto Internacional: La Convención de Budapest.

A nivel internacional, la Convención de Budapest sobre Cibercrimen, que Perú firmó en 2007, proporciona un marco para la cooperación internacional para combatir el cibercrimen. El tratado busca alinear las leyes nacionales, facilitar la colaboración judicial y fortalecer la prevención del cibercrimen. La Convención trata sobre el robo de identidad y el fraude electrónico y establece reglas básicas para la privacidad y las brechas de seguridad de datos.

1.4. Antecedentes del estudio

El aumento de los delitos informáticos se ha convertido en uno de los desafíos más serios de la era digital. Desde accesos no autorizados a sistemas hasta la suplantación de identidad, este tipo de crímenes ha crecido de forma acelerada en los últimos veinte años, impulsado por la expansión de Internet, la masificación de los dispositivos móviles y el acceso generalizado a plataformas digitales.

De Romaña (2022), en su investigación titulada “Análisis del sistema regulatorio en los servicios de telefonía e internet fijo y móvil y su necesidad de permanente revisión y cambio, Perú 2021”, planteó como objetivo determinar si el mercado de las telecomunicaciones puede producir vacíos o lagunas normativas que afecten negativamente a los usuarios, sugiriendo una revisión periódica y constante de la

regulación. Con base en una metodología que combinó la recopilación de información de expertos del sector con la experiencia de 50 usuarios de estos servicios, la investigación dejó en evidencia que existen casos de vulneración de derechos, tanto por malas prácticas de los operadores como por la insuficiencia de la normativa vigente. El estudio reveló deficiencias en la comprensión y aplicación de las regulaciones, lo que puso de manifiesto la necesidad de contar con un marco legal más sólido y actualizado. Finalmente, se concluyó que la protección efectiva del usuario requiere una vigilancia permanente y un perfeccionamiento constante del marco regulatorio, con el fin de evitar vacíos legales y garantizar la calidad de los servicios de telecomunicaciones.

Villar (2024), en su investigación titulada "Tráfico ilegal de datos: necesidad de reforma del Código Penal peruano", se propuso evaluar cuán efectivas son las normas penales actuales frente al uso indebido de datos personales en entornos digitales. Para ello, empleó un enfoque cualitativo que incluyó el análisis de leyes nacionales, jurisprudencia y entrevistas con especialistas en derecho informático. Los hallazgos revelaron que el marco legal vigente resulta insuficiente para prevenir y sancionar de forma adecuada este tipo de delitos. Ante ello, el estudio planteó la necesidad de modificar el Código Penal para incluir de forma clara el delito de tráfico ilegal de datos personales y así reforzar la protección de la privacidad ciudadana. Como cierre, se sugirió capacitar a los operadores del sistema judicial y aplicar sanciones más estrictas, alineadas con los avances tecnológicos, con el fin de desalentar este tipo de conductas.

Lupaca (2024), en su investigación titulada "Rol de los intermediarios de Internet en la lucha contra el delito de suplantación de identidad en Perú, 2020", propuso analizar cómo los intermediarios de Internet pueden ser aliados clave en la lucha contra el robo de identidad en el país durante ese año. Para ello, empleó una metodología cualitativa, basada en entrevistas a ocho especialistas en Derecho relacionados con la temática. A partir de estas entrevistas, se evidenció que en Perú no existe un marco legal específico que regule claramente las responsabilidades y funciones de los intermediarios de Internet frente a casos de suplantación de identidad. La investigación concluye que estos actores juegan un papel fundamental, ya que son responsables de implementar medidas de seguridad que resguarden derechos como la privacidad, la dignidad y la protección de la identidad. Además, tienen el deber de colaborar con las autoridades para identificar a los usuarios involucrados en delitos informáticos. No obstante, también se identificó que este rol aún no es completamente eficaz. Esto se debe, por un lado, a la falta de herramientas digitales avanzadas —como sistemas de verificación biométrica— y, por otro, a la ausencia de una normativa clara que delimite sus responsabilidades penales y civiles. Por ello, se

recomienda la creación de una ley o una reforma legal que aborde estas situaciones y se adecúe a las demandas actuales en materia de ciberdelitos.

Por otro lado, en el contexto internacional, Fernández (2023), en su investigación titulada "La Suplantación de la Identidad Cibernética en el Ecuador", se planteó como un objetivo principal determinar si la sociedad ecuatoriana está preparada para dar respuesta a los peligros que se presentan en la era tecnológica, así como evaluar la idoneidad de la legislación interna para la protección de los derechos de los usuarios. Se aplicó una metodología de enfoque mixto, que incluía la revisión de literatura especializada y la aplicación de cuestionarios a *focal groups*, con el propósito de obtener datos sobre el grado de conocimiento y percepciones de la población en cuanto a seguridad en línea. Entre los resultados más destacados, se evidenció un gran desconocimiento de herramientas digitales de protección y de las acciones legales disponibles para denunciar casos de suplantación de identidad; además, se encontró la necesidad de fortalecer los marcos regulatorios con el propósito de adaptarlos a la creciente complejidad de las amenazas cibernéticas. Como conclusión, el autor planteó el fortalecimiento de campañas de conciencia dirigidas a ciudadanos, posibilitando la capacitación especializada de los operadores de justicia y actualizando la legislación vigente para cubrir amplia y efectivamente las nuevas modalidades de delitos informáticos que comprometen la privacidad y seguridad de los ecuatorianos.

Nugra et al. (2023), en su artículo titulado "*Sim swapping* como variante del delito de la violación a la intimidad e integrante de otras infracciones penales", que tuvo como objetivo señalar al *SIM Swapping* como una modalidad delictiva que, a su vez, atenta contra la privacidad y, al mismo tiempo, integra otras infracciones penales establecidas dentro del Código Orgánico Integral Penal del Ecuador. La metodología que se propuso fue de tipo cualitativa, con un alcance analítico y descriptivo, fundamentada en el análisis de obras y documentos de referencia que abordan la problemática. Los resultados reflejaron la violación de la seguridad jurídica de los ciudadanos en virtud de la falta de una figura delictiva del *SIM Swapping*, dejando a las víctimas de estos delitos informáticos el uso indebido de sus datos personales. Como conclusión y recomendación, se propone sustituir el marco negativo y defensivo del derecho ecuatoriano por un enfoque proactivo que, al mismo tiempo, proteja los derechos de los usuarios y les brinde mecanismos útiles para defender su información ante esta creciente amenaza.

1.5. Marco conceptual

1.5.1. Delitos Informáticos.

Un crimen u ofensa ilícita que implica el uso de tecnología de la información y la comunicación, comparado como cibercrimen, incluye delitos como el acceso no autorizado a dispositivos o sistemas de información, modificación o destrucción de datos, robo de información sensible y otros tipos de engaño electrónico. McQuade (2006) enfatiza que el cibercrimen, como la mayoría de las otras formas de delito, se ha desarrollado con la llegada de Internet y la globalización de la vida diaria, proporcionando más opciones para los delincuentes. Tales crímenes son una amenaza porque no solo van dirigidos a individuos particulares, sino también a instituciones, naciones e incluso grandes empresas cuya infraestructura digital está en riesgo.

1.5.2. Suplantación de Identidad.

El robo de identidad ocurre cuando alguien utiliza la información privada de otra persona para llevar a cabo actos fraudulentos, incluyendo, pero no limitándose a, acceder ilegalmente a cuentas bancarias, crear cuentas falsas en redes sociales o realizar compras a nombre de la víctima. Estos crímenes han aumentado tremendamente debido a la facilidad con la que se puede obtener información privada en internet y en las redes sociales. Como cita Suso (2017), el robo de identidad digital no solo pone en peligro las finanzas de la víctima, sino que también puede causar daños severos a su imagen personal o profesional. Esto se ha convertido en uno de los tipos más comunes de cibercrimen que defrauda a millones de personas en todo el mundo.

1.5.3. Venta Ambulatoria de Chips Móviles.

La venta de chips de teléfonos móviles se refiere al comercio de tarjetas SIM fuera de los canales oficiales o autorizados, y sin autenticar la identidad del comprador. Esto permite a los criminales adquirir tarjetas SIM sin tener que proporcionar verdaderas formas de identificación, lo que les permite cometer delitos como el robo de identidad. En este sentido, Álvarez (2019) indica que este tipo de comercio no solo carece de los controles adecuados, sino que tampoco proporciona un seguimiento suficiente sobre la actividad del comprador, lo que dificulta mucho que las autoridades puedan identificar a alguien responsable de actos ilegales como el fraude financiero y el robo de identidad.

1.5.4. Ciberseguridad.

La ciberseguridad implica el enfoque estratégico que una persona adopta con las prácticas de seguridad, políticas y tecnologías utilizadas para defender a los usuarios, la información y los dispositivos informáticos del acceso no autorizado, daño o destrucción.

Anderson (2014) destaca no solo la protección de datos personales y organizacionales, sino también el punto crítico de protección para la infraestructura, como hospitales, bancos y

servicios gubernamentales, que dependen en gran medida de la tecnología para funcionar como entidad. La ciberseguridad está amenazada por virus, ransomware, ataques de phishing y mucho más; por lo tanto, siempre se deben tomar medidas drásticas para minimizar tales riesgos.

1.5.5. Fraude Electrónico.

El fraude electrónico se define como el uso de internet y otras herramientas digitales para llevar a cabos, que pueden incluir robo de identidad, fraude bancario y fraude con tarjetas de crédito. Según Holt, Bossler y May (2016), este tipo de fraude se puede llevar a cabo mediante el uso de phishing, implementando malware e incluso creando sitios web falsos diseñados para robar información sensible de las víctimas objetivo. Al igual que con otras formas de cibercriminalidad, esto se ha agravado por la relativa facilidad con la que los cibercriminales pueden acceder a sistemas débiles y engañar a las personas para que proporcionen sus datos personales o financieros.

1.5.6. Phishing.

El phishing es una técnica que utiliza el engaño para espiar el comportamiento de alguien con la esperanza de obtener información personal valiosa – como contraseñas y números de tarjeta de crédito – de una víctima que supone que está siendo abordada por una institución legítima, como un banco o tienda de confianza. Según Böhme (2010), el fraude phishing es parte de una gran variedad de cibercrimen que se establece y mantiene por su confiabilidad y bajo costo de ejecución. Por medio del uso de correos electrónicos, mensajes de texto y páginas web fraudulentas, el phishing se da con el claro objetivo de recoger datos delicados de las víctimas desprevenidas.

1.5.7. TIC (Tecnologías de la Información y la Comunicación).

Las TIC constituyen una combinación de tecnologías que permiten el procesamiento, almacenamiento y difusión de la información en redes de comunicación como: internet, sistemas computacionales o dispositivos móviles. Según Castells (2000) la transformación que han sufrido las sociedades modernas es a tal escala, que el uso de la tecnología de la información y la comunicación se ha vuelto fundamental para el acceso a la información, sin embargo, este mal uso también acarrea riesgos, como lo son: el incremento de los delitos informáticos.

1.5.8. Redes Sociales

Las redes sociales son plataformas digitales mediante las cuales los usuarios pueden crear perfiles, interactuar con otros usuarios y compartir contenido en forma de texto, imágenes y videos. Boyd, 2014 explica que las redes sociales han tenido un impacto

automático tremendo en la forma en que las personas se interconectan y comunican, porque hay un espacio en forma de un sitio web donde las personas establecen y también mantienen relaciones sociales. Por otro lado, también han abierto nuevas ventanas para la suplantación de identidad, el ciberacoso y otros crímenes informáticos, ya que estos espacios son mal utilizados por delincuentes para recopilar información personal de manera engañosa.

1.5.9. Acceso no autorizado.

El acceso no autorizado se refiere a la intrusión en el uso de sistemas informáticos, bases de datos o redes sin permiso de los propietarios o administradores adecuados. Van der Velde, 2018 señala que este tipo de acceso ilegal tiene consecuencias directas, como el robo de información confidencial, espionaje industrial y manipulación de datos. Generalmente, los cibercriminales explotan un sistema de seguridad o un sistema de datos utilizando técnicas de hacking o la instalación de programas maliciosos para obtener información destinada a otros usuarios.

1.5.10. Delincuencia Cibernética.

Los delitos cibernéticos hacen referencia a los crímenes que se cometen a través de internet o de alguna tecnología digital, incluyendo el fraude especial, el hackeo, el robo de datos y malware. Según Wall (2007), el fenómeno de la cibercriminalidad ha aumentado a la par con la creciente publicidad del uso de internet y la digitalización de la información rica en nuevo contenido; lo que origina nuevos tipos de crímenes que son muy complejos de localizar y controlar por el anonimato del entorno cibernético.

1.5.11. Robo de identidad.

El robo de identidad es cuando le roban a alguien su información personal para obtener beneficios económicos de cierto tipo, como acceder a cuentas bancarias o contratar algunos servicios a nombre de otra persona. Whitfield (2013) explica distintas formas en que el "phishing", el hackeo de la base de datos o el uso de información personal proveniente de redes sociales puede producir un delito como el robo de identidad. Este tipo de ciberdelito se ha vuelto de suma importancia por el simple hecho de que la información se puede obtener tan sencillamente de internet.

1.5.12. Crimen Digital.

El crimen digital incluye cualquier acto ilegal que se lleve a cabo utilizando una tecnología digital. Finn y Longo (2018) describen sus casos como incluyendo fraude electrónico, robo de identidad, difusión de malware y hackeo. El crimen digital ha aumentado significativamente con el crecimiento de Internet y las tecnologías móviles, ya que ha facilitado y hecho más eficiente la operación de los delincuentes.

1.5.13. Ciberacoso.

El ciberacoso es un tipo de acoso que se perpetúa a través de medios digitales, como plataformas de redes sociales, correos electrónicos o mensajes de texto. Kowalski et al. (2014) se centran en particular en el hecho de que esta forma de acoso está tan fácilmente disponible para muchas personas que el objetivo puede ser acosado muchas veces en cualquier instancia posible. El ciberacoso puede tener repercusiones graves en el bienestar emocional y psicológico de las víctimas, más aún si el acoso se realiza de forma anónima.

1.5.14. Virus informático.

Se entiende por malware el diseño de software que es capaz de crear daños a dispositivos o sistemas electrónicos. Según Symantec (2017), el malware es más común conocido como: virus, gusanos, troyanos o ransomware, cada uno teniendo sus propios objetivos como controlar dispositivos, herir información o chantajear a las víctimas. El funcionamiento del malware es bastante veloz y es capaz de causar estragos en un gran número de dispositivos a la vez.

1.5.15. Delincuencia Cibernética.

Se define la cibercriminalidad como la realización de actividades ilícitas a través del uso de internet y tecnologías de la información, tales como fraude, daño de datos o contrabando de información. Según Weimann (2016), no es fácil el control y el castigo, puesto que es un delito que se realiza por un conjunto de personas a nivel internacional. Es una de las principales amenazas al sistema de seguridad internacional porque, por lógica, son operaciones que integran gobiernos y empresas multinacionales.

CAPÍTULO II: PLANTEAMIENTO DEL PROBLEMA

2.1. Descripción de la realidad problemática

La publicación de una identidad falsa es algo que se torna cada vez más común y que afecta a las personas en forma más seria a medida que pasan los años, esto gracias al progreso de la tecnología y al uso de ordenadores y móviles. Con la venta ilegal de chips de teléfonos móviles que se ha facilitado por la falta de control de muchas naciones, este tipo delito cibernético se ha vuelto más fácil de realizar. Los defraudadores utilizan este descontrol para hacer estafas e identidades falsas, que afecta no solo a las víctimas primarias, sino que también financia las pérdidas empresariales y de telecomunicaciones. Por lo que se le debe dar suma importancia a conocer la evolución de esta problemática, global y local, incluyendo los pasos que se están implementando para remediar los peligros que vienen a raudales.

A escala mundial, el fenómeno delictivo de la venta y explotación no autorizada de una identidad en particular ha crecido en preocupantes fronteras en las diferentes partes del mundo. Como menciona el reporte de las naciones unidas, el incremento de casos identificados en la venta y tráfico de identidad a través de recursos electrónicos ha subido exponencialmente en los últimos cinco años, configurándose entre los delitos más consumidos en el medio digital.

En los EE.UU. UU., Canadá y otras partes de Europa, los criminales cibernéticos recurren a comprar números de teléfono y cambiarlos utilizando aplicaciones de mensajería para acceder fácilmente a información sensible. La simplicidad con la que se pueden obtener ilegalmente chips móviles ha hecho posible este tipo de fraudes. Estos dilemas han causado que las autoridades internacionales tomen medidas más severas en la vigilancia de las transacciones digitales y automaticen la venta de dispositivos de telecomunicaciones.

La informalidad en la venta de chips móviles ha provocado que Perú sea víctima del delito de robo de identidad. Desde el 2022, La Policía Nacional del Perú ha informado un aumento constante en casos de fraude y estafa debido a lazos con delitos utilizando chips de teléfonos obtenidos en involucrados en la venta informal. Esto se explica por la falta completa de control y regulación para este tipo de ventas que permite a los delincuentes tener líneas telefónicas sin registrador, lo que imposibilita el rastreo. Esta ausencia de norma es grave tanto para las autoridades como para las personas comunes debido a que afecta la seguridad y confianza en la economía digital.

El robo de identidad ha sido un crimen existente desde tiempos inmemoriales, y su versión digital está aún más agravada debido a los avances en telecomunicaciones,

información y otras tecnologías en las últimas décadas. Tradicionalmente, este crimen se llevaba a cabo principalmente en el mundo offline e implicaba suplantar a personas utilizando documentos falsos para obtener servicios o bienes. Pero a medida que la información se digitalizaba, los métodos se volvían preferidos. La sofisticación dio lugar al uso de la tecnología para cometer fraudes más grandes y fáciles que nunca. El uso desenfrenado de teléfonos móviles y la facilidad de acceder a servicios bancarios en línea no han hecho más que facilitar esta mala práctica. Estos avances han hecho que falsificar información sea un proceso fluido y han suscitado interrogantes sobre la protección de datos y la seguridad del mundo cibernético.

El informe de Martínez de 2019 sobre la venta ilegal de chips móviles y su conexión con el aumento de delitos cibernéticos en América Latina, hace una mención notable. Sus hallazgos han demostrado que la ausencia de regulación en el mercado de los dispositivos es un contribuyente importante a los intentos de falsificación de identidad por parte de los ciberdelincuentes.

Otro tema que debe incorporarse es el estudio hecho por Rodríguez y Pérez (2021), quienes abordan la fragilidad de los sistemas de telecomunicaciones por el aumento de fraudes digitales en Perú. Ellos mencionan con énfasis la necesidad de mejorar las políticas de control sobre la venta de dispositivos móviles, así como la digitalización de la educación para evitar estos delitos.

La finalidad de la presente investigación es tratar de explicar con profundidad y claridad cómo la venta informal de chips telefónicos ha ayudado a incrementar el número de casos de suplantación de identidad por medio de fraude en el Perú. La meta es lograr entender más los elementos que permiten la comisión de este delito, así como brindar alternativas que sean útiles para detener su avance. También, se pretende generar un mayor nivel de sensibilidad de los ciudadanos no solo en torno a la protección de datos personales, sino también en torno a la legislación que rige la venta de dispositivos de telecomunicaciones. Se intenta plantear a través del examen de la legislación existente en el país y su vinculación con la cibercriminalidad, buscar las lagunas que se encuentran en la legislación vigente, y desarrollar normas legales que neutralicen esas brechas y aseguren un intercambio controlado de chips móviles.

2.2. Formulación del problema general y específicos

2.2.1 Problema general

¿Qué consecuencias legales tiene la venta informal de chips móviles en el aumento de los delitos informáticos, especialmente en casos de suplantación de identidad, y cómo afecta esto a la protección de los derechos de los ciudadanos en el Perú?

2.2.2 Problemas específicos

1) ¿Qué vacíos legales y regulatorios existen en la legislación peruana respecto a la venta informal de chips móviles, y de qué manera estos vacíos facilitan la comisión de delitos informáticos como la suplantación de identidad?
2) ¿Cómo se podría reforzar el marco legal en el Perú para regular adecuadamente la venta de dispositivos móviles y evitar su uso fraudulento en casos de suplantación de identidad?
3) ¿Cómo abordan las leyes actuales sobre delitos informáticos en el Perú los casos de suplantación de identidad vinculados a la venta ilegal de chips móviles, y qué mejoras podrían implementarse desde el ámbito legislativo?
4) ¿Qué grado de responsabilidad tienen las empresas de telecomunicaciones y los proveedores de servicios móviles en la prevención de delitos informáticos originados por la venta no regulada de chips móviles?
5) ¿Qué consecuencias legales tiene la suplantación de identidad a través de la compra ilegal de chips móviles en relación con los derechos fundamentales de las personas afectadas, como el derecho a la privacidad y la protección de datos personales?

2.3. Objetivo general y específicos

2.3.1 Objetivo general

Analizar cómo la venta informal de chips móviles influye legalmente en el aumento de los delitos informáticos, en particular en los casos de suplantación de identidad, y plantear reformas legales que refuercen la protección de los derechos de los ciudadanos en el Perú.

2.3.2 Objetivos específicos

1) Analizar los vacíos legales y regulatorios que existen en la legislación peruana sobre la venta informal de chips móviles, y cómo estos vacíos contribuyen a que se cometan delitos informáticos como la suplantación de identidad.

2) Evaluar el marco legal vigente en el Perú sobre la comercialización de dispositivos móviles y proponer cambios normativos que ayuden a prevenir su uso fraudulento en casos de suplantación de identidad.
3) Estudiar cómo las leyes peruanas en materia de delitos informáticos enfrentan la suplantación de identidad facilitada por la venta ilegal de chips móviles, e identificar aspectos que podrían mejorarse para garantizar una mayor protección de los derechos ciudadanos.
4) Determinar cuál es la responsabilidad legal de las empresas de telecomunicaciones y los proveedores de servicios móviles en la prevención de delitos informáticos relacionados con la venta no regulada de chips.
5) Analizar las consecuencias jurídicas de la suplantación de identidad a través de la compra ilegal de chips móviles, en relación con los derechos fundamentales de las personas afectadas, como la privacidad y la protección de datos personales, y proponer soluciones legales viables.

CAPÍTULO III: JUSTIFICACIÓN Y DELIMITACIÓN DE LA INVESTIGACIÓN

3.1. Justificación e importancia del estudio

3.1.1. Justificación del estudio.

3.1.1.1. Justificación teórica. Existen varias teorías que explican la suplantación de identidad junto con la venta ambulante de chips móviles como un delito de tecnología de la información. El uso indebido de chips móviles constituye un crimen social y tecnológico como lo describe activamente Ericson (2007), quien ofrece explicaciones sobre cómo los avances tecnológicos han proporcionado nuevos caminos para que los violadores de la ley eviten los mecanismos de control social y penal y

3.1.1.2. obtengan acceso no autorizado

a datos a través de manipulaciones negatorias tecnológicas como los chips móviles. Apoyando esta afirmación, la teoría del control social deja un vacío para que los vendedores de accesorios para teléfonos celulares operen sin responsabilidad civil y legal. Además, favorece la suplantación, ya que Lyon (2003), en su estudio sobre la sociedad de control, no solo analiza la expansión tecnológica de la vigilancia, sino que también examina la oportunidad añadida para eludir dicha vigilancia y cometer delitos. Esta circunstancia crea condiciones favorables para llevar a cabo la venta informal de chips móviles. La teoría de oportunidades de Cohen y Felson (1979) afirma que el crimen es más probable que aumente donde hay demasiada laxitud en la supervisión de oportunidades criminales. Por último, Foucault (1995) discute que no hay supervisión ni protección de los datos, presentando así una oportunidad para que los criminales tomen el control de las identidades ajenas sin ser notados abiertamente. En otras palabras, se centra en el poder de vigilancia de la tecnología.

3.1.1.2. Justificación práctica. Desde una perspectiva práctica, el análisis del aumento de la actividad criminal como la suplantación de identidad debe ser considerado primordial para la formulación de políticas públicas que se ocupan de prevenir que los

misma es ilegal y, por lo tanto, representa una amenaza considerable a la seguridad de la información personal de los usuarios, ya que alimenta este tipo de fraudes. Esta investigación intenta resaltar medidas que sean de fácil aplicación dentro de los planos de las entidades que regulan el uso de dispositivos móviles en la ciudad. También se pueden obtener resultados sobre cómo reestructurar las estrategias de prevención, detección, y en su caso, represión de delitos informáticos mediante el diseño de programas educativos y

campañas de concientización sobre los peligros que rodean la adquisición de tarjetas SIM en vuelos no oficiales. Se espera que con las evidencias recolectadas se logren establecer condiciones más rígidas en la comercialización de los dispositivos móviles y los accesorios.

3.1.1.3. Justificación metodológica. El estudio adopta un enfoque cualitativo debido a la necesidad de explicar en detalle el fenómeno y las dinámicas socioculturales de la clonación de identidad a través de la venta de chips móviles. Esto es apropiado ya que permite capturar las percepciones, experiencias y significados de los participantes, algo que no es posible con un enfoque cuantitativo. Se utilizarán tres herramientas metodológicas para adaptar y complementar el análisis: entrevistas, grupos focales y análisis de documentos. Las entrevistas proporcionarán información de primera mano de expertos, autoridades y actores sociales relevantes sobre las políticas y desafíos hacia la prevención de este crimen. El análisis de documentos será crucial para marcar la investigación dentro de los límites legales y normativos relevantes a través de la revisión de legislaciones, regulaciones y estudios previos sobre delitos cibernéticos. Por último, el grupo focal estará por personas que han experimentado engaño de identidad o que han participado en el mercado informal de chips móviles, lo que mejorará la comprensión de las experiencias narradas y las percepciones generales del público sobre las víctimas. Esta combinación de herramientas metodológicas garantizará una visión más clara del fenómeno, lo que a su vez conducirá a una mejor propuesta de políticas y estrategias públicas.

3.1.2. Importancia del estudio.

El presente estudio de la suplantación de identidad, mediante la venta ambulatoria de chips móviles, adquiere interés crítico dentro de los derechos fundamentales y el desarrollo del Estado Social y Democrático de Derecho. Esto lo hacemos al analizar no solo las dimensiones técnicas y económicas del delito, sino también la consecuencia de la ausencia de legislación o la existencia de leyes que dejan la materia en blanco suficiente para que estos hechos se perpetran con relativa impunidad. En este sentido, el análisis jurídico resulta fundamental para lograr avanzar en la revisión y actualización de leyes, en la elaboración de mayor legislación protectora, y en el planteamiento de leyes que fortalecen la seguridad jurídica en Internet.

Por otro lado, el enfoque del Derecho tiene la particularidad de analizar las repercusiones que estos delitos producen en el ámbito de la protección de la identidad y la privacidad de los ciudadanos, las cuales están consagradas en la Constitución y en diversos instrumentos internacionales de derechos humanos. La suplantación de identidad se da a

nivel individual, pero también afecta la confianza en las instituciones y en el funcionamiento de los sistemas de control judicial y administrativo. Este trabajo, por consiguiente, resulta ser un instrumento de fundamental importancia para orientar a aquellos que participan en la elaboración de las políticas y estrategias legislativas, así como también a los y fiscales, defensores públicos y otros operadores jurídicos responsables de la cibercriminalidad.

Además, la investigación toma un carácter prospectivo al incluir un contexto como el previsto en Lima para el año 2025, el cual se caracteriza por avances tecnológicos y digitalización de servicios que requieren respuestas legales creativas y proactivas. La evolución de escenarios y la identificación de nuevos riesgos suponen cambios legislativos y en la práctica jurídica, en donde las respuestas legales aseguran evolucionar acorde al incremento de la delincuencia cibernética. Así, esta investigación aporta al desarrollo académico en la ciencia del Derecho, así como también a la construcción de una sociedad más segura y confiable.

3.2. Delimitación del estudio

3.2.1. Delimitación espacial.

Este estudio de investigación está limitado a la ciudad de Lima, la capital de Perú. Esta decisión se justifica en que Lima tiene un alto nivel de comercio informal y una creciente demanda de servicios de telecomunicaciones, lo que contribuye a la proliferación de la venta de chips móviles. Además, la alta densidad poblacional de la ciudad, junto con las actividades económicas, da lugar a una situación en la que estos cibercriminales pueden tener un campo de acción considerable en la localización de potenciales víctimas y formas de operar. Por lo tanto, el alcance del trabajo de campo, la recopilación de datos y el análisis del tema se llevará a cabo en diversos distritos de Lima, que tienen altas tasas de venta informal de chips y reportes de robo de identidad y suplantación.

3.2.2. Delimitación poblacional.

La población foco está compuesta, en primera instancia, por los usuarios o las posibles víctimas de delitos informáticos, quienes adquirieron chips móviles y pueden ser víctimas de identidad falsificada. En segunda, se tomará en cuenta a los vendedores informales y formales de chips móviles por su importancia respecto a la perpetración de estos delitos. Finalmente, se incluirá para comprender las telecomunicaciones en Perú, junto con los representantes de las empresas de telecomunicaciones, a las entidades

gubernamentales que atienden los asuntos de control y supervisión de las telecomunicaciones del país, con el fin de entender qué legales y/o vacíos existen en los procesos de control y fiscalización.

3.2.3. Delimitación temporal.

La presente investigación abarcará el período de tiempo comprendido por los años 2020 al 2025 (enero – abril) con el fin de analizar cómo el paso del tiempo ha influido en el aumento de los delitos informáticos por suplantación de identidad. De esta manera, se espera poder adelantarse a los posibles escenarios futuros y formular posibles acciones para la prevención y control que sean efectivas y factibles para aplicar en Lima en el año 2025.

CAPÍTULO IV: FORMULACIÓN DEL DISEÑO

4.1. Diseño esquemático

Esta sección describe las herramientas de diseño utilizadas en el desarrollo de la investigación, basadas en el marco teórico actual. También se proporciona un breve resumen del diseño. Las siguientes técnicas e instrumentos se utilizaron en este estudio de investigación cualitativa:

Tabla 1

Técnicas e instrumentos para el desarrollo de la investigación

Técnica	Instrumento
Entrevista	Guía de entrevista
Análisis documental	Ficha de análisis documental
Focus group online (grupo focal en línea)	Guía de entrevista grupal

Para llevar a cabo esta investigación cualitativa sobre el incremento de los delitos informáticos de suplantación de identidad mediante la venta de chips móviles en Lima durante los años 2020 a 2025, se emplearon entrevistas, análisis documental y *focus groups online* como técnicas de recolección de información. Para ello, se elaboraron la guía de entrevista, la ficha de análisis documental y la guía de entrevista grupal con el propósito de obtener información representativa y exhaustiva sobre la problemática estudiada. El uso de estas técnicas, debido a su combinación, resulta en una gran cantidad de datos, lo que justifica el uso de Atlas.ti como software para el procesamiento de la información, ya que permite una organización, codificación y análisis sistemático de los datos cualitativos obtenidos a partir de los testimonios y documentos recolectados. El software permite la inclusión ordenada y precisa de cada fragmento de información dentro de las categorías analíticas que se han creado, esto fortalece la trazabilidad y transparencia del sistema, además de facilitar la organización, clasificación y reconocimiento de patrones dentro de los conceptos.

Igualmente, la flexibilidad de Atlas.ti ayuda en la triangulación de datos al incorporar sistemáticamente las perspectivas de entrevistas individuales, la evidencia documental y las contribuciones de grupos focales en línea, lo que culmina en un análisis integral y confiable de la suplantación de identidad y su relación con la venta ambulatoria de chips móviles.

4.2. Descripción de los aspectos básicos del diseño

4.2.1. Entrevista.

La entrevista es una forma de recolección de datos cualitativos que requiere la interacción de un investigador y un participante que buscan entender sus experiencias, percepciones y actitudes (Kvale y Brinkmann, 2009). Inferir a través de preguntas abiertas o semiestructuradas, se intenta desarrollar una comprensión de la visión del mundo del encuestado para capturar un rico significado contextual que a menudo está más allá del alcance de los métodos cuantitativos.

Dentro del ámbito de estudio del creciente crimen informático de suplantación de identidad facilitado por la venta ambulatoria de chips móviles en Lima durante los años 2020-2025, las entrevistas ayudan a capturar los puntos de vista de expertos en seguridad digital y reguladores de políticas digitales. De esta manera, se captura una comprensión integral de las estrategias de suplantación de identidad, así como las brechas legales y procesales que potencialmente existen y contribuyen a la comisión de estos crímenes.

4.2.2. Análisis documental.

El análisis documental se establece como el análisis metódico de fuentes escritas o de otros soportes como textos legales, informes institucionales, informes periodísticos, bases de datos, etc. para extraer, clasificar y evaluar información relevante para un objeto de estudio específico (Bowen, 2009). Esta técnica permite la triangulación de datos recopilados por otros medios y brindar un contexto apropiado que sustente las conclusiones del investigador.

En esta investigación, el análisis documental se justifica por la necesidad de estudiar disposiciones legales, denuncias, estadísticas oficiales y estudios previos relevantes al comercio ambulante de chips móviles y los crímenes de suplantación de identidad. Con esto, el estudio pretende definir arquetipos de fraude, identificar brechas dentro de la legislación y encontrar tendencias en el uso de identidades falsas para obtener líneas móviles, lo que proporciona pruebas sólidas que complementan la información recopilada a través de entrevistas y otros métodos cualitativos.

4.2.3. Focus group online (grupo focal en línea).

El *focus group*, como lo define Ñaupas et al. (2018), es una técnica cualitativa que consiste en reunir un grupo de personas para que discutan sobre un tema

determinado, siendo guiados por un moderador que sabe escuchar y saber hacer preguntas fundamentales. En entornos virtuales, se realiza a través de videoconferencias o salas de chat que permiten la interacción sin necesidad de presencia física, ampliando así la convocatoria para incluir participantes de diversas ubicaciones geográficas.

Para este estudio, el uso de *focus group* en línea permite acceder a una visión colectiva de las percepciones, experiencias y propuestas por un conjunto de actores clave: usuarios de servicios móviles, soluciones profesionales de ciberseguridad y representantes de la industria de telecomunicaciones. Al fomentar la discusión y el diálogo, es posible llegar a acuerdos e identificar diversas opiniones que profundicen en la comprensión de los factores que facilitan la suplantación de identidad y la venta ambulatoria desenfrenada de chips de teléfonos móviles.

4.2.4. Atlas.ti

Atlas.ti es un programa informático utilizado para el análisis de datos cualitativos. Permite a los usuarios organizar, codificar y explorar sistemáticamente los datos, incluidas transcripciones de entrevistas, documentos, notas de campo y discusiones de focus group (Friese, 2019). Atlas.ti facilita la separación de la información en unidades de significado, codificándolas y construyendo redes conceptuales que representan las relaciones entre categorías analíticas, por lo tanto, acelera la interpretación y fomenta la confiabilidad de los hallazgos.

En esta investigación, la aplicación de Atlas.ti dentro del estudio es indispensable para organizar sistemáticamente y gestionar meticulosamente los grandes volúmenes de datos recopilados a través de entrevistas, análisis documental y discusiones de focus group en línea. El software permite la coherencia e integración de los resultados a través de informes sin problemas, lo que facilita la identificación de patrones, la triangulación de datos y la síntesis de resultados en relación con la suplantación de identidad y su relación con la venta ambulatoria de chips de teléfonos móviles en Lima (2020-2025). Además, la solidez metodológica y la credibilidad de los resultados de la investigación se ven mejoradas por la transparencia y la trazabilidad del software.

CAPITULO V: PRUEBA DE DISEÑO

5.1. Aplicación de la propuesta de solución

5.1.1. Enfoque Social: Concientización comunitaria y prevención

Para mitigar los problemas asociados con la venta ambulatoria y las activaciones ilegales de líneas móviles, es necesario un enfoque social fuerte que incorpore a los miembros de la comunidad, las escuelas y los medios de comunicación. La idea central es generar una fuerte conciencia pública sobre los riesgos involucrados en estas actividades ilegales, como la suplantación de identidad y otros crímenes cibernéticos.

A. Campañas educativas y de concientización

1) **Objetivo:** Informar y educar a la gente sobre el peligro inherente asociado con la compra ilegal de tarjetas SIM y líneas móviles, y las consecuencias que estas suponen para la seguridad colectiva y personal.

2) **Acciones:**

- Realizar campañas de concienciación en redes sociales y sitios web gubernamentales utilizando testimonios reales de víctimas de casos de suplantación de identidad.

- Desarrollar materiales visuales interactivos que ilustren cómo los criminales defraudan y estafan a sus víctimas utilizando líneas móviles adquiridas ilegalmente. Estas campañas de concientización deben incluir videos, infografías y publicaciones en blogs, y deben adaptarse a personas de todas las edades.

- Charla comunitaria en plazas y en los centros comunitarios sobre los efectos negativos de la venta ambulatoria ilegal de SIM cards y cómo no convertirse en una víctima de fraude.

B. Impulsar la colaboración y denuncia comunitaria

1) **Objetivos:** Incentivar la denuncia de venta de SIM cards ilegales, así como la participación activa de la comunidad para frenar la venta ilegal de chips.

2) **Acciones:**

- Producir y comercializar de forma masiva una campaña publicitaria para el funcionamiento de una línea telefónica de denuncias anónimas, así como una aplicación móvil que facilite a los ciudadanos y a los ostensibles la denuncia de presuntas actividades ilícitas relacionadas con la venta de chips y líneas de

telefonía móvil.

- Trabajar junto con los líderes comunitarios y asociaciones de vecinos que pueden realizar un control social al pasar la información sobre la presencia de los vendedores ambulantes ilegales a las autoridades competentes.

C. Educación en la escuela

1) **Objetivo:** Incluir en los programas curriculares de educación primaria y secundaria la importancia de la seguridad digital y de la protección de la identidad.
2) **Acciones:**

- Implementar módulos de educación sobre la cibercriminalidad y la protección de la identidad que se imparta en informática, ética y ciudadanía en las escuelas.
- Estos módulos deben capacitar a los estudiantes sobre la identificación del fraude cibernético así como las ramificaciones legales de participar en actividades ilegales.
- Talleres en universidades e instituciones de educación superior dedicados a la seguridad digital y aspectos legales de los crímenes cibernéticos, particularmente el robo de identidad.

5.1.2. Enfoque Institucional: El rol de las empresas de servicios de telefonía móvil

Los proveedores de servicios de telefonía móvil son protagonistas del problema respecto a la venta ilegal de líneas móviles. Es crucial que asuman más responsabilidad en la detección y prevención de estos delitos, no solo cumpliendo con la legislación existente, sino trabajando proactivamente contra las operaciones ilegales.

A. Innovación en procedimientos de venta y activación de SIM cards

1) **Objetivo:** Agilizar los procesos de venta y activación de chips móviles mediante la aplicación de tecnología más sofisticada y métodos adicionales para mejorar la legitimidad de las transacciones y prevenir fraudes relacionados de suplantación de identidad.
2) **Acciones:**

Desarrollar un sistema de activación inteligente utilizando IA.

- **Innovación:** En lugar de utilizar métodos tradicionales como la biometría y la verificación de datos, se puede establecer un sistema que involucre inteligencia artificial (IA) con la capacidad de analizar patrones en tiempo real respecto a las características del usuario (por ejemplo, frecuencia de gasto, ubicación y

historial de activación). Esto ayudaría a identificar comportamientos anormales o posibles fraudes.

- **Acción:** Implementar algoritmos de IA que, durante la activación de una línea telefónica, realicen automáticamente un chequeo cruzado de datos a través de múltiples bases de datos (documentos de identidad, redes sociales y registros de compra de chips) para posibles fraudes activos. Este sistema debería tener el potencial de marcar discrepancias que permitirían generar alertas automáticas en los bordes de los datos proporcionados por el usuario y sus datos de confirmación de identidad.

Autenticación Multifactor (MFA) para el proceso de activación de líneas

- **Innovación:** Ampliar las fronteras de la autenticación más allá de la biometría. Se utilizará un método más sofisticado conocido como autenticación multifactor (MFA) que se centra en datos biométricos (huellas dactilares o rostro) junto con otro factor que podría ser una segunda factor a través del teléfono o correo electrónico del usuario utilizando códigos únicos.
- **Acción:** La activación del chip debe requerir un mínimo de dos mecanismos de validación, que incluyen biometría abarcadora y la confirmación de un identificador único temporal. Esto garantizará que solo el portador de la identidad pueda activar la línea, y será particularmente útil en caso de que la primera autenticación no pueda asegurar suficientemente la autenticidad del usuario.

Blockchain para el registro y la trazabilidad de activaciones

- **Innovación:** Implementar tecnología *blockchain* para proporcionar la trazabilidad e inmutabilidad requeridas en las transacciones de activación de líneas móviles.
- **Acción:** Desarrollar un sistema de *blockchain* seguro que registre cada activación de línea junto con la verificación de identidad correspondiente. Este registro en blockchain solo estaría disponible para las autoridades autorizadas y los operadores, lo que garantizaría la integridad de la información y facilitaría la auditoría en caso de actividades fraudulentas o problemas legales. Además, el sistema permitiría la verificación de la autenticidad de las líneas activadas de manera instantánea durante el período.

Validación proactiva por geolocalización

- **Innovación:** El proceso de venta y activación de una línea móvil incorporará tecnología de geolocalización para verificar la ubicación del comprador y contrastarla con su identidad.

- **Acción:** En el momento de la compra, el operador puede confirmar la ubicación del comprador utilizando su dispositivo móvil y cruzarla con las direcciones registradas en el documento de identidad. Cuando se esté realizando el paso de activación en un área geográfica inusual o fuera de una zona conocida, el sistema puede requerir un paso de verificación adicional antes de continuar con la activación.

Integración de tecnología de análisis de comportamiento en el punto de venta

- **Innovación:** El uso de tecnología de análisis de comportamiento en tiendas físicas y en línea debe aplicarse con la inclusión de cámaras de reconocimiento facial y otros dispositivos motivados por el comportamiento para identificar posibles actividades fraudulentas.

- **Acción:** Los operadores pueden colocar cámaras que detectan emociones y comportamientos en lugares estratégicos del punto de venta. Estos sistemas podrán reconocer ciertas actividades inusuales y sospechosas, como intentos repetidos de usar identidades robadas, y alertar a los vendedores o a las fuerzas del orden para que tomen acción.

B. Sistema de trazabilidad de chips móviles

1) **Objetivo:** Desarrollar un sistema descentralizado que permita el seguimiento del ciclo de vida del chip móvil desde su distribución hasta su activación final.
2) **Acción:**

- Diseñar un registro de base de datos interconectado que rastree cada SIM card de teléfono móvil (unidad) vendido y lo vincule con el código de identificación único del usuario móvil.

- Desarrollar un marco de monitoreo y evaluación para evaluar el rendimiento y resultado del sistema de alerta automática configurado para notificar a las autoridades cuando se detecten actividades sospechosas de chips SIM, como detalles de activación sospechosos.

- Los operadores de telecomunicaciones deben controlar la distribución de chips

listos para usar (por ejemplo, preactivados) (poseyendo el estado activado, listos para usar sin la confirmación previa del usuario). Cada chip (unidad) debe estar asociado con una identificación legítima en cada nivel antes de llegar al usuario del servicio.

C. Trabajando junto con las autoridades pertinentes para desmantelar redes ilegales de distribuidores conocidos

1) **Objetivo:** Identificar y apoyar activamente a las agencias de orden público en el tratamiento de afiliaciones de distribuidores ilegales.

2) **Acciones:**

- Los operadores móviles necesitan establecer acuerdos de políticas colaborativas con la Policía Nacional y la Fiscalía para proporcionar documentos útiles sobre distribución y activación de líneas móviles consideradas sospechosas.

- Fomentar la colaboración entre los operadores para desarrollar una portabilidad de numeración móvil (MNP) que marque los números de teléfono que se considere que están activos ilegalmente.

5.1.3. Enfoque Legislativo: Principios jurídicos orientadores y mejora integral

A. Aumento de las sanciones penales en relación con el comercio informal de tarjetas SIM y la activación de líneas móviles

1) **Objetivo:** Reforzar la pena de prisión para aquellos que se dediquen a la venta informal y al alquiler ilegal de líneas móviles para un número particular, asegurándose de que los infractores sean juzgados por la gravedad de sus acciones.

2) **Acciones:**

Cambio en las penas descritas en el Artículo 9-A de la Ley Nº 30096 (Ley de Delitos Informáticos):

- **Propuesta de innovación:** Se puede incluir la posibilidad de imponer una pena adicional de inhabilitación para participar en la activación ilegal de líneas móviles, esta inhabilitación podría ser de más de cinco años y también podría aplicarse a aquellos que trabajen en la industria de telecomunicaciones ilegalmente al no contar con el certificado o autorización requerida para hacerlo.

- **Nuevo enfoque:** Establecer un tipo de delito para comercializadores informales de tarjetas SIM que incluya la confiscación de cualquier equipo móvil o accesorio utilizado en la activación ilegal de líneas y la imposición de la sanción económica destinada a maximizar la efectividad disuasoria.

Introducción de sanciones para compradores de tarjetas SIM ilegales (Art. 222-B del Código Penal):

- **Propuesta de innovación:** Introducir una pena específica para el kit adquirido

que contenga una tarjeta SIM ilegal. Si se puede demostrar que una persona adquirió una tarjeta SIM de manera delictiva y, posteriormente, la utilizó para el robo de identidad o fraude, esa persona debe incurrir en responsabilidad penal, aunque menos severa, que sea suficiente para detener tal comportamiento en el futuro.

- **Nuevo punto de vista:** La pena de prisión debería oscilar entre uno y tres años, junto con la adición de sanciones administrativas que prohíban a la persona contratar con compañías de telefonía móvil por un período determinado de tiempo, restringiéndolos de entrar en futuros acuerdos.

B. Implementación de un sistema nacional de control y trazabilidad para tarjetas SIM

1) **Objetivo:** Crear un sistema de monitoreo que permita a las autoridades localizar más fácilmente los puntos de venta y activación de tarjetas SIM ilegales.

2) **Acciones:**

Crear un sistema de control integral interinstitucional:

- **Propuesta de innovación:** Construir una plataforma digital operada por el Ministerio del Interior, el Ministerio de Transportes y Comunicaciones (MTC), y OSIPTEL, que registre cada SIM distribuida y la vincule a un sistema de verificación biométrica o digital que muestre al comprador. Este registro debería estar abierto para los operadores móviles y autoridades para la emisión de legitimidad de transacciones.

- **Nuevo enfoque:** Idear un sistema de alertas preventivas para operadores y autoridades desencadenadas por la venta sospechosa de tarjetas SIM en áreas prohibidas o marcadas en rojo. Asimismo, se tendría que incluir la posibilidad de suspender líneas móviles de manera instantánea, en tiempo real, para mejorar la respuesta ante los intentos de fraude.

Sistema de verificación de identidad para compra y activación.

- **Propuesta innovadora:** Aparte de los métodos biométricos, se debería incluir una verificación multifactorial en el procedimiento de activación de tarjetas SIM que incluya validación de documentos (DNI o pasaporte) junto con un código temporal enviado al teléfono móvil o correo electrónico de la persona que compró la tarjeta SIM.

- **Nuevo enfoque:** Exigir a los operadores de telecomunicaciones que presenten

informes detallados a las autoridades sobre cada compra y activación realizada, los cuales deben ser mantenidos por no menos de 5 años.

C. Establecimiento de nuevas obligaciones para las entidades supervisadas OSIPTEL y empresas telefónicas.

1) **Objetivo:** Fortalecer la cooperación entre los sectores público y privado para garantizar el cumplimiento por parte de los operadores móviles de la ley y regulaciones respecto a la venta y activación de tarjetas SIM.

2) **Acciones:**

Responsabilidad de los operadores móviles (Art. 16 de la Ley 27336 y Artículo 272-A del Código Penal):

- **Innovación sugerida:** Además de otorgar a los órganos relevantes acceso a la información sobre el marketing y activación del servicio, los operadores deberían implementar un sistema de control interno para la venta de chips móviles. Este sistema debería posibilitar la identificación al instante de cualquier transacción sospechosa.

- **Nuevo enfoque:** Exigir a las operadoras que informen a las autoridades sobre las activaciones de tarjetas SIM en un plazo no mayor de un mes desde su activación, especificando vendedor y comprador por razones de transparencia.

Provisión de sistemas digitales de control a supervisión de OSIPTEL y autoridades.

- Equipar a OSIPTEL con sistemas informáticos integrales para la activación de supervisión por medio de SIM card. Esto incluiría *software* de monitoreo de compra y de activación a nivel de SIM Cards que se encargaría de monitorear automáticamente comportamientos sospechosos y generar alertas de manera instantánea.

- Adaptar que OSIPTEL tenga la facultad de auditorías reactivas sobre tesauros de operadores a verificar la consistencia entre la base de datos de identidad usuarios y la información que es queridar.

D. Control sobre SIM cards no autorizadas a nivel internacional.

- **Propuesta innovadora:** Forjar convenios de acuerdo de control comercial de SIM card y desbloqueo de teléfonos móviles en líneas para activar temporalmente regiones con países limítrofes de Perú. Esto permitiría a las

autoridades locales obtener datos sobre la venta internacional de chips a través de otros medios.

- **Nuevo enfoque:** Establecer un sistema de intercambio de información con operadores internacionales así como autoridades nacionales de telecomunicaciones para monitorear las SIM cards compradas en el extranjero y su activación ilegal en Perú.

Conclusión

Aparte de marcos tecnológicos e innovadores utilizando tecnología avanzada, enfoques colaborativos entre diferentes entidades a nivel local e internacional, está claro que se necesitan cambios en los marcos legislativos y regulatorios. Al implementar estas medidas, reduciremos significativamente las actividades asociadas con la venta y activación ilícita de SIM cards, al tiempo que mejoramos la protección de los clientes y la seguridad internacional del estado.

CONCLUSIONES

1) El aumento de los mercados informales de chips móviles ha incrementado la ocurrencia de robo de identidad y otras formas de fraude en Lima. La falta de regulación sobre la venta de tarjetas SIM ha llevado a una mayor perpetración de estos crímenes porque los ciberdelincuentes aprovechan la falta de supervisión para participar en actividades fraudulentas.

2) Las campañas de ventas que son importantes para combatir los riesgos asociados con el tráfico ilegal de chips móviles implican informar al público a través de divulgación comunitaria y campañas educativas que ayudan a crear conciencia sobre el problema. Los resultados obtenidos en la prueba de campo muestran que estas campañas ayudan a despertar la conciencia pública a través de redes sociales y otros canales de comunicación sobre los peligros de estas actividades ilegales y sus consecuencias, por ejemplo, el robo de identidad.

3) Al evaluar las políticas existentes, se encontró una brecha junto a otras políticas que derivan brechas en su enfoque hacia los delitos cibernéticos resultantes del negocio de venta de chips móviles informales. Es crítico incorporar en la ley más disposiciones para penas más severas y reglas más explícitas sobre la venta y activación de tarjetas SIM para mejorar la aplicación de la ley contra dichos delitos.

4) La ayuda de tecnologías de alta complejidad, como la inteligencia artificial relacionada con la supervisión de la activación de chips móviles y la aplicación de sistemas de autenticación multifactor, puede ser invaluable en la prevención de fraudes por suplantación de identidad. Los resultados de la prueba de diseño sostienen que la implementación de sistemas de IA y blockchain para el seguimiento de transacciones podría mejorar la confiabilidad de las activaciones y controlar el uso fraudulento de líneas móviles.

5) La colaboración interinstitucional de los operadores de telecomunicaciones, entidades estatales y la ciudadanía resulta determinante al momento de frenar la delincuencia informática vinculada a la comercialización clandestina de tarjetas SIM. Los resultados sugieren que el establecimiento de espacios de colaboración, tales como sistemas de reportes y acciones comunales orientadas a la vigilancia del comercio informal, complementaría con efectividad el nivel de control y seguridad pública del sistema.

6) Los resultados del diseño de la prueba subrayan la necesidad de sistemas avanzados de trazabilidad y control como blockchain y verificación de geolocalización en tiempo real para la distribución y monitoreo de activaciones de chips móviles. Tales sistemas permitirían a las autoridades prevenir y localizar actividades ilícitas de dispositivos móviles, manteniendo así la integridad durante el proceso de activación.

7) El uso de la activación de chips móviles biométricos junto con algoritmos de IA para el análisis de patrones de comportamiento anómalos son igualmente importantes para la prevención del fraude. Además, los usuarios necesitan ser educados sobre la protección de información personal y las implicaciones legales de actividades ilegales, lo cual fue evidente en los resultados del diseño de pruebas.

8) Todas las medidas propuestas, como aumentar las penalizaciones para quienes sean encontrados culpables de vender ilegalmente tarjetas SIM y establecer un sistema nacional de control y trazabilidad para dichos dispositivos, deben llevarse a cabo con el objetivo de asegurar una mayor seguridad en el espacio digital. Sin embargo, estas políticas también deben incorporar la necesidad de una vigilancia integral, que evolucione en tiempo real para contrarrestar nuevas amenazas tecnológicas emergentes.

RECOMENDACIONES

1) Es fundamental que las autoridades y organizaciones civiles desarrollen activamente campañas en redes sociales destinadas a difundir información sobre los peligros asociados a la compra ilegal de tarjetas SIM y los fraudes subsiguientes. Además, estas campañas deberían incluir relatos de verdaderas víctimas para ayudar a concienciar al público sobre la magnitud del problema y la necesidad de tomar medidas para salvaguardar la identidad. Estas campañas también deben estar dirigidas a escuelas y grupos comunitarios para ayudar a cambiar la percepción en torno a la seguridad digital y promover un cambio cultural profundo.
2) Se recomienda promover la participación activa del público en general en la denuncia de delitos relacionados con la venta ilegal de tarjetas SIM. La creación de líneas telefónicas designadas para denuncias anónimas, o el desarrollo de aplicaciones para teléfonos inteligentes dedicadas a reportar estos delitos, aumentará enormemente la accesibilidad para la denuncia. Además, la colaboración con líderes locales, así como asociaciones de vecinos, incrementará el control social, lo cual es fundamental en la lucha contra la venta ilegal de chips en la calle.
3) Es necesario incluir módulos de enseñanza sobre cibercrimen y protección de la identidad en las escuelas secundarias y primarias. Igualmente, se deberían introducir talleres sobre robo de identidad y las ramificaciones legales de las actividades ilegales en colegios y universidades. Esto asegurará que la nueva generación sea más consciente de los riesgos que presenta el ciberespacio y cómo prevenir ser víctimas de fraudes.
4) Se recomienda implementar sistemas inteligentes basados en inteligencia artificial (IA) para verificar, en tiempo real, la validez de las transacciones durante la activación de líneas móviles. Este sistema debe cruzar información de diversas bases de datos para identificar posibles actividades fraudulentas. Además, el uso de autenticación multifactor en los procesos de activación de tarjetas SIM proporcionará una capa adicional de protección de la identidad.
5) En el caso de las tarjetas SIM, se sugiere incluir la integridad de las transacciones dentro del proceso de activación a través de la inclusión de tecnología blockchain. Esto ayudará en la protección de la veracidad de las activaciones y su facilitación para la auditoría en casos de fraudes. Este sistema deberá ser restringido al uso de autoridades y operadores autorizados.

6) Es fundamental crear un sistema en el que todas las entidades dentro de un país controlen el monitoreo sobre la activación y venta de tarjetas SIM que se consideran ilegales. La existencia de un registro, digital y controlado por las entidades competentes, permitirá que todas las tarjetas SIM estén sometidas a un sistema de verificación biométrica o digital. Este sistema aumentará la eficiencia con la que las autoridades toman control sobre la vigilancia de actividades fraudulentas y medidas preventivas.

7) Con el fin de frenar el mercado informal relacionado con el mercado de activación de tarjetas SIM y líneas ilegales, se sugiere aumentar las sanciones penales asociadas con estas actividades. Esto incluye la imposición de disposiciones de sentencia adicionales contra estos infractores, como la descalificación para participar en actividades de activación ilegales y la confiscación de dispositivos utilizados en la comisión de estos delitos. Además, debe haber algún tipo de castigo para aquellos compradores que obtienen las tarjetas SIM ilegalmente solo para defraudar a los proveedores de servicios de red móvil, ya que esos compradores enfrentarán prisión y prohibiciones de ciertos contratos futuros con proveedores de servicios móviles.

8) Debido a la naturaleza multinacional de este delito, se sugiere formular acuerdos de cooperación internacional con operadores de redes y autoridades extranjeras para la vigilancia y regulación de la venta ilegal de tarjetas SIM. El establecimiento de sistemas de intercambio de información sobre tarjetas SIM compradas en el extranjero y su subsiguiente activación ilegal en Perú ayudará a combatir los crímenes organizados transnacionales relacionados con el robo de identidad.

REFERENCIAS BIBLIOGRÁFICAS

Álvarez, J. (2019). *Telecomunicaciones y la regulación del mercado de SIM cards*. Ediciones del Derecho.

Anderson, R. (2014). *Security engineering: A guide to building dependable distributed systems* (3rd ed.). Wiley.

Baker, C., Jones, M., y Davis, L. (2021). *Digital fraud and the role of unregulated SIM cards in identity theft*. Journal of Cybersecurity and Technology, 15(2), 211-228. https://doi.org/10.1002/jct.10456

Böhme, R. (2010). *Phishing and fraud: A study of cybercrime and the economics of information security*. Springer.

Bowen, G. (2009). Análisis de documentos como método de investigación cualitativa. *Qualitative Research Journal, 9* (2), 27–40. https://doi.org/10.3316/QRJ0902027

Boyd, D. (2014). *It's complicated: The social lives of networked teens*. Yale University Press.

Brenner, S. W. (2007). *Cybercrime: Criminal threats from cyberspace*. Praeger Publishers.

Castells, M. (2000). *The rise of the network society* (2nd ed.). Wiley-Blackwell.

Código Penal Peruano

Convenio de Budapest sobre Cibercriminalidad, 2001.

Fernández, L., y Castillo, M. (2019). *Ciberseguridad y legislación: Desafíos ante el crecimiento de los delitos informáticos*. Editorial Jurídica.

Finn, J., y Longo, L. (2018). *Digital crime: Understanding cybercriminals*. Routledge.

Friese, S. (2019). *Análisis de datos cualitativos con ATLAS.ti* (3.ª ed.). SAGE. https://methods.sagepub.com/book/mono/preview/qualitative-data-analysis-with-atlas.pdf

Fuchs, C. (2017). Social media: A critical introduction. SAGE Publications.

García, A., y Ruiz, M. (2020). *El impacto de la venta ilegal de chips móviles en la ciberseguridad: Un análisis en el contexto latinoamericano*. Revista de Derecho y Tecnología, 12(3), 45-61.

Gibbs, J. (2019). Criminal behavior: A psychological approach. Pearson Education.

González, M. (2019). *Derecho penal informático: Una aproximación a la regulación de los delitos cibernéticos*. Editorial Jurídica.

Holt, T., Bossler, A., y May, D. (2016). *Cybercrime and justice: The criminal justice system in cyberspace*. Routledge.

Kowalski, R. M., Giumetti, G. W., Schroeder, A. N., y Lattanner, M. R. (2014). *Cyberbullying: A review of the legal, policy, and research issues*. Computers in Human Behavior, 36, 2-10.

Kumar, S., y Mallick, P. K. (2018). *Identity theft: Causes, consequences, and prevention strategies*. International Journal of Computer Science and Network Security, 18(9), 1-9.

Kvale, S., y Brinkmann, S. (2009). *InterViews: Aprendiendo el arte de la entrevista cualitativa* (2.ª ed.). SAGE.

Ley de Delitos Informáticos.

Ley de Firma Digital.

Ley de Protección de Datos Personales.

Ley General de Telecomunicaciones.

López, A. (2017). *La teoría general del delito informático: Principios y normas básicas*. Editorial Jurídica.

Mann, L. (2014). The dark web: A digital underground economy. Springer.

Martínez, F. (2019). *El impacto de la venta ilegal de chips móviles en la proliferación de delitos informáticos en Latinoamérica*. Revista Latinoamericana de Derecho y Tecnología, 22(1), 59-75.

Martínez, J., y López, P. (2022). *El fraude digital en el sector financiero: Una mirada a la suplantación de identidad en plataformas de pago móvil*. Journal of Financial Fraud Studies, 19(4), 45-58.

McQuade, S. C. (2006). *Cybercrime: Investigating high-technology computer crime*. Pearson/Prentice Hall.

Ñaupas Paitán, H., Valdivia Dueñas, M. R., Palacios Vilela, J. J., y Romero Delgado, H. E. (2018). *Metodología de la investigación: Cuantitativa - Cualitativa y redacción de la tesis* (5ª ed.). Ediciones de la U. Recuperado de http://www.biblioteca.cij.gob.mx/Archivos/Materiales_de_consulta/Drogas_de_Abuso/Articulos/MetodologiaInvestigacionNaupas.pdf

ONU. (2021). *Informe sobre la suplantación de identidad y los delitos informáticos a nivel mundial*. Naciones Unidas. https://www.un.org

Pérez, J., y García, S. (2020). *El desafío de la legislación frente a los delitos informáticos en el siglo XXI: Un análisis global*. Revista Internacional de Derecho Informático, 28(1), 90-108.

Pfleeger, C. P., y Pfleeger, S. L. (2015). *Security in computing* (5th ed.). Pearson Education.

Policía Nacional del Perú. (2022). *Informe sobre el aumento de delitos informáticos y la suplantación de identidad en el país*. Recuperado de https://www.pnp.gob.pe

Policía Nacional del Perú. (2022). *Informe sobre la incidencia de delitos informáticos en el Perú*. Policía Nacional del Perú. https://www.pnp.gob.pe

Rodríguez, A., y Pérez, M. (2021). *La vulnerabilidad de los sistemas de telecomunicaciones y la incidencia de fraudes digitales en el Perú*. Journal of Digital Law, 34(2), 112-130.

Rodríguez, F. (2021). *El mercado informal de chips móviles: Un estudio sobre su relación con los delitos cibernéticos*. Ciberseguridad y Sociedad, 8(2), 102-115.

Schneier, B. (2018). *Click here to kill everybody: Security and survival in a hyper-connected world*. W.W. Norton & Company.

Schneier, B. (2018). Click here to kill everybody: Security and survival in a hyper-connected world. W.W. Norton & Company.

Shelley, L. (2005). Transnational crime: An overview. The Global Criminal Justice Review, 7(3), 234-246.

Solms, B., y Niekerk, J. (2013). *Cyber security and cybercrime: Understanding the growing threat*. Information Security Journal: A Global Perspective, 22(2), 83-90.

Solove, D. J. (2021). Understanding privacy. Harvard University Press.

Suso, D. (2017). *Delitos informáticos y suplantación de identidad*. Editorial Jurídica Internacional.

Symantec. (2017). *Internet security threat report*. Symantec.

Van der Velde, S. (2018). *Cybercrimes: A legal perspective on unauthorized access*. Cambridge University Press.

Wall, D. (2007). *Cybercrime: The transformation of crime in the information age*. Policing and Society, 17(4), 411-433.

Weimann, G. (2016). *Cybercrime and cyberterrorism: The importance of the digital revolution*. Rowman & Littlefield.

Whitfield, T. (2013). *The identity theft handbook: Detection, prevention, and security*. McGraw-Hill Education.

Young, J. (2014). The criminological imagination. Polity.

ANEXOS

Anexo 1. Matriz de consistencia

MATRIZ DE CONSISTENCIA

CRECIMIENTO DE LOS DELITOS INFORMÁTICOS EN LA MODALIDAD DE SUPLANTACIÓN DE IDENTIDAD, FACILITADOS POR LA VENTA AMBULATORIA DE CHIPS MÓVILES, LIMA – 2020-2025

Problema General	Objetivo General	Hipótesis General	Categorías	Subcategorías
¿Qué consecuencias legales tiene la venta informal de chips móviles en el aumento de los delitos informáticos, especialmente en casos de suplantación de identidad, y cómo afecta esto a la protección de los derechos de los ciudadanos en el Perú?	Analizar cómo la venta informal de chips móviles influye legalmente en el aumento de los delitos informáticos, en particular en los casos de suplantación de identidad, y plantear reformas legales que refuercen la protección de los derechos de los ciudadanos en el Perú.	La venta informal de chips de teléfonos móviles contribuye significativamente al aumento del crimen informático, particularmente al robo de identidad en Perú, debido a la falta de marcos legales adecuados y punitivas limitadas. Este escenario daña los derechos primarios de los ciudadanos, como su privacidad y la protección de datos personales.	**Categoría 1:** Delitos informáticos en la modalidad de suplantación de identidad	- Naturaleza de los delitos de suplantación de identidad - Técnicas utilizadas para la suplantación de identidad - Impacto en las víctimas - Regulación legal de la suplantación de identidad - Percepción pública sobre la suplantación de identidad
Problemas específicos	**Objetivos específicos**	**Hipótesis específicas**	**Categoría 2:** Venta ambulatoria de chips móviles	- Alcance de la venta ambulatoria de chips móviles - Regulación y control de la venta de chips móviles
¿Qué vacíos legales y regulatorios existen en la legislación peruana respecto a la venta informal de chips móviles, y de qué manera estos vacíos facilitan la	Analizar los vacíos legales y regulatorios que existen en la legislación peruana sobre la venta informal de chips móviles, y cómo estos vacíos contribuyen a que se cometan	La falta de límites legales y marcos regulatorios en la legislación peruana acerca de la venta informal de chips de teléfonos móviles favorece la comisión de suplantación de		

comisión de delitos informáticos como la suplantación de identidad? ¿Cómo se podría reforzar el marco legal en el Perú para regular adecuadamente la venta de dispositivos móviles y evitar su uso fraudulento en casos de suplantación de identidad? ¿Cómo abordan las leyes actuales sobre delitos informáticos en el Perú los casos de suplantación de identidad vinculados a la venta ilegal de chips móviles, y qué mejoras podrían implementarse desde el ámbito legislativo? ¿Qué grado de responsabilidad tienen las empresas de telecomunicaciones y los proveedores de servicios móviles en la prevención de delitos informáticos originados por la venta no regulada de chips móviles? ¿Qué consecuencias legales tiene la suplantación de	delitos informáticos como la suplantación de identidad. Evaluar el marco legal vigente en el Perú sobre la comercialización de dispositivos móviles y proponer cambios normativos que ayuden a prevenir su uso fraudulento en casos de suplantación de identidad. Estudiar cómo las leyes peruanas en materia de delitos informáticos enfrentan la suplantación de identidad facilitada por la venta ilegal de chips móviles, e identificar aspectos que podrían mejorarse para garantizar una mayor protección de los derechos ciudadanos. Determinar cuál es la responsabilidad legal de las empresas de telecomunicaciones y los proveedores de servicios móviles en la prevención de delitos informáticos relacionados con la venta no regulada de chips. Analizar las consecuencias jurídicas de la suplantación de	identidad porque no existe una regulación estricta que imponga castigos proporcionales para esta actividad delictiva. El orden jurídico en el Perú puede fortalecerse mediante la formulación de leyes específicas que regulan la venta de teléfonos móviles y chips, exigiendo que se implementen controles más estrictos contra posibles fraudes de uso para suplantación de identidad, mejorando así la protección legal de los ciudadanos. Existe una carencia de leyes que regulan adecuadamente la suplantación de identidad ligada a la venta ilegal de tarjetas SIM. Esto, en consecuencia, dificulta la investigación profunda de estos delitos. En el caso de delitos informáticos que se generan a raíz de la venta ilegal de chip de teléfono, las compañías de telecomunicaciones y sus prestadores de servicio móvil		- Perfil de los vendedores ambulantes de chips móviles - Conocimiento y cumplimiento de las regulaciones por parte de los vendedores. - Impacto social y económico de la venta ambulatoria de chips de móviles

identidad a través de la compra ilegal de chips móviles en relación con los derechos fundamentales de las personas afectadas, como el derecho a la privacidad y la protección de datos personales?	identidad a través de la compra ilegal de chips móviles, en relación con los derechos fundamentales de las personas afectadas, como la privacidad y la protección de datos personales, y proponer soluciones legales viables.	tienen una alta percepción de culpa. La falta de políticas de control y supervisión por parte de estas empresas propicia el incremento de delitos de suplantación de identidad. La suplantación de identidad mediante la adquisición clandestina de tarjetas SIM implica un atentado directo y considerable a los derechos de los ciudadanos afectados en relación a la protección de su información personal. Además, afecta la seguridad jurídica y los derechos de bienestar.		

Anexo 2. Instrumentos de recolección de datos

Anexo 2.1. Guía de entrevista semi estructurada

GUÍA DE ENTREVISTA SEMI ESTRUCTURADA

TESIS: "Crecimiento de los delitos informáticos en la modalidad de suplantación de identidad, facilitados por la venta ambulatoria de chips móviles, Lima 2020-2025".

OBJETIVO DE LA INVESTIGACIÓN: Analizar cómo la venta informal de chips móviles influye legalmente en el aumento de los delitos informáticos, en particular en los casos de suplantación de identidad, y plantear reformas legales que refuercen la protección de los derechos de los ciudadanos en el Perú.

I. DATOS GENERALES

Entrevistado: .....
DNI N°: .....
CIP N°: .....
CAL N°: .....
Lugar de trabajo: .....

II. INTERROGANTES:

1. **¿Cuáles son los factores que, a su juicio, facilitan la suplantación de identidad en el contexto de la venta informal de chips de teléfono en Lima, y qué medidas se podrían tomar para prevenir este tipo de delitos?**

2. **Desde su experiencia en ciberdelincuencia, ¿cómo califica la efectividad de la prevención y persecución de la venta de chips para la comisión de delitos de suplantación de identidad, y qué modificaciones consideran que deben realizarse para fortalecer la lucha contra estos delitos?**

Firma entrevistado
DNI N°:

GUÍA DE ENTREVISTA

Entrevistado 1: Rosa Clara Tuesta Estela

DNI N°: 46499897

CIP N°: 31529756

CAL N°: 95148

Lugar de trabajo: Dirección de Investigación de Ciberdelincuencia de la PNP (antes DIVINDAT PNP).

Preguntas:

1. ¿Cuáles son los factores que, a su juicio, facilitan la suplantación de identidad en el contexto de la venta informal de chips de teléfono en Lima, y qué medidas se podrían tomar para prevenir este tipo de delitos?

Rpta.- El problema no proviene únicamente de la falta de supervisión respecto al procedimiento de activación de los chips, sino también de la inexistencia de un marco legal de efectivo que regule la venta de chips móviles en la calle. En muchas áreas de la ciudad, los vendedores ambulantes venden chips sin ningún tipo de verificación de identidad, y el pago se realiza de manera completamente indetectable. Este anonimato facilita a aquellos que ya han robado información personal, o incluso a aquellos que portan documentos falsos, obtener un chip y usarlo para suplantar una identidad. Además, muchos de los vendedores no conocen las consecuencias legales de vender chips a personas sin un procedimiento de verificación establecido. Como solución, creo que debería haber un registro obligatorio para todos estos vendedores donde cada comerciante debe estar debidamente acreditado y autorizado, teniendo todas las transacciones registradas en un sistema de control centralizado. Esto permitiría rastrear cada una de las ventas de chips, llevando a un sistema de vigilancia más eficiente de estos chips para que no puedan ser usados fraudulentamente.

El núcleo del problema es la ausencia de una regulación clara sobre la venta de chips en mercados informales. Actualmente, la legislación no exige a los vendedores ambulantes llevar un registro de la venta de chips y, por lo tanto, hay margen para que los chips se utilicen de manera fraudulenta. Hay un vacio en la ley que podria solucionarse con leyes más estrictas que controlen la venta informal de chips y exijan a las corporaciones establecer una plataforma donde se registren todas las ventas realizadas. También es necesario que se establezca el requisito de que el vendedor esté obligado a registrar quién está comprando el chip y vincular cada chip vendido con una entidad identificable.

2. Desde su experiencia en ciberdelincuencia, ¿cómo califica la efectividad de la prevención y persecución de la venta de chips para la comisión de delitos de suplantación de identidad, y qué modificaciones consideran que deben realizarse para fortalecer la lucha contra estos delitos?

Rpta.- Las estrategias implementadas, como la verificación de la identidad de los compradores, no son suficientes porque todavía hay muchos puntos ciegos, sobre todo en el mercado informal. Las operadoras de telefonía móvil son claves, pero la necesaria integración entre las autoridades y las empresas de telecomunicaciones aún no se logra. Para mí, la solución debe ser mucho más estructural: establecer un sistema de auditoría constante en todos los puntos de venta, incluso los informales. Es vital que las operadoras estén obligadas a reportar cualquier verta realizada fuera de sus canales oficiales y que las autoridades tengan la posibilidad de actuar de manera inmediata ante la detección de responsabilidades. Además, creo que se deben soportar las sanciones para quienes comercializan chips de forma ilegal.

Las leyes existentes sobre el uso de servicios de telecomunicaciones son insuficientes para abordar las lagunas identificadas en el control de las ventas de chips. Es necesario que la ley exija la trazabilidad obligatoria de cada chip desde su fabricación hasta su activación. Esto mitigaría el fraude y aumentaria la seguridad de las transacciones. Además, la ley debería imponer duras penalizaciones a los vendedores y establecer un mecanismo de control que permita el seguimiento de todas las ventas de chips.

Rosa Clara Tuesta Estela
DNI N° 46499897

GUÍA DE ENTREVISTA

Entrevistado 2: Víctor Espinoza Prado
DNI Nº: 15708633
CIP Nº: 30888844
CAL Nº: 90571
Lugar de trabajo: Dirección de Investigación de Ciberdelincuencia de la PNP (antes DIVINDAT).

Preguntas:

1. **¿Cuáles son los factores que, a su juicio, facilitan la suplantación de identidad en el contexto de la venta informal de chips de teléfono en Lima, y qué medidas se podrían tomar para prevenir este tipo de delitos?**

   Rpta.- Además de la ausencia de verificación de identidad para los compradores como un factor, otro factor que contribuye al robo de identidad es la falta de verificación de identidad respecto a los riesgos atractivos que rodean la compra informal de estos chips. La mayoría de las personas simplemente no sabe que se están exponiendo al riesgo de fraude o, aún peor, de que sus nombres se asocien con actividades criminales debido a que el chip que compraron fue utilizado fraudulentamente. Esto se debe en gran medida a la ausencia de campañas publicitarias informativas que eduquen sobre los peligros relacionados con esta actividad. Además, los vendedores informales aprovechan esta falta de información y muchos operan sin supervisión de las autoridades locales. Para remediar esto, recomiendo que se enfoquen en la necesidad de diseñar e implementar iniciativas de campaña de defensa primarias destinadas a combatir la venta informal de chips en el mercado informal educando al público sobre no solo los peligros medidas legales, sino también las de protección relacionadas con la información personal.
   A pesar de los avances realizados en la legalización de la compra y venta de equipos de telecomunicaciones, aún no existe un control sólido en relación con la venta informal de chips. Este escenario deja un vacío legal que facilita el robo de identidad. Se deben promulgar leyes que prohíban la venta de chips en lugares informales sin requerir una solicitud y registro previos, así como exigir el pago electrónico para todas las ventas. Es necesario establecer un sistema de verificación de identidad, compatible con bases de datos nacionales, para garantizar que los chips se vendan exclusivamente a compradores verificados.

2. **Desde su experiencia en ciberdelincuencia, ¿cómo califica la efectividad de la prevención y persecución de la venta de chips para la comisión de delitos de suplantación de identidad, y qué modificaciones consideran que deben realizarse para fortalecer la lucha contra estos delitos?**

Rpta.- El control inalámbrico de la identidad es un buen primer paso. Sin embargo, desde el control de identidad hasta la implementación de la ley existe un gran vacío. Para cerrar este vacío, es indispensable que exista un sistema de monitoreo que inicie desde la venta del chip y se extienda hasta su activación. Las operadoras deben hacerse responsables de que todos los chips vendidos estén correctamente registrados como una persona verificada, con información suficiente para determinar que, en el caso de hacer la venta, no se esté usando información falsa o robada. También es posible que las operadoras de telefonía estén obligadas a establecer otros tipos de verificación a través de sus aplicaciones donde los propietarios comprueben si el chip que compran está realmente asociado a su persona o no antes de activarlo.
Las estrategias actuales por sí solas no son suficientes, ya que se aplica poca ejecución en las leyes que rigen la venta de chips en mercados informales. Los operadores de redes móviles deben ser obligados a trabajar más estrechamente con las agencias de cumplimiento para desarrollar un sistema conjunto de control para monitorear las ventas ilegales de chips. La ley debe permitir la verificación en tiempo real de todas las ventas para que las autoridades relevantes puedan seguir las transacciones e identificar cualquiera.

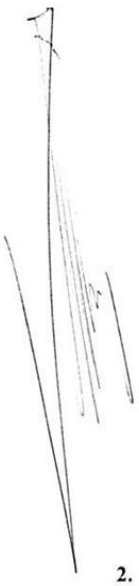
Víctor Espinoza Prado
DNI N°: 15708633

GUÍA DE ENTREVISTA

Entrevistado 3: Evans Daniel Velásquez Medina
DNI N°: 43352902
CIP N°: 343775
Lugar de trabajo: Dirección de Investigación de Ciberdelincuencia de la PNP (antes DIVINDAT).

Preguntas:

1. **¿Cuáles son los factores que, a su juicio, facilitan la suplantación de identidad en el contexto de la venta informal de chips de teléfono en Lima, y qué medidas se podrían tomar para prevenir este tipo de delitos?**



Rpta.- Un gran problema con la venta de chips en la calle es que no hay un sistema en marcha para verificar si los chips vendidos son de origen legítimo. El mercado informal sigue siendo un agujero enorme para criminales oportunistas que compran estos chips, solo para que sean registrados bajo identidades robadas. Los compradores en la calle a menudo lo hacen a precios mucho más baratos que los precios estándar, o simplemente no saben en qué se están metiendo. En mi opinión, la alternativa más adecuada es implementar un sistema de seguimiento para estos chips utilizando etiquetas RFID para rastrear el chip desde su producción hasta el comprador. De esta manera, las autoridades podrían determinar en cualquier momento de dónde provenían los chips ya dónde fueron.
La suplantación de identidad se ha convertido en un problema a causa de la informalidad en la venta de chips, ya que no hay normas legales que regule su comercialización. Hay leyes que no indican con precisión cuál es el algoritmo que deben seguir estos vendedores. Tampoco existe un controlador automotor que lleve un registro de ventas de chips y lo consolide en un solo sitio. A mi juicio, el ordenamiento jurídico debe establecer la obligación de que todos los vendedores, incluso los informales, dispongan de un sistema de registro que esté integrado al sistema de registro civil nacional. Con esto se puede comprobar la veracidad de quienes se dicen ser vendedores y se podrán monitorear los controles y las ventas.

2. **Desde su experiencia en ciberdelincuencia, ¿cómo califica la efectividad de la prevención y persecución de la venta de chips para la comisión de delitos de suplantación de identidad, y qué modificaciones consideran que deben realizarse para fortalecer la lucha contra estos delitos?**

Rpta.- Si las ventas ilegales ocurren sin ningún tipo de registro, controlar las activaciones se queda muy corto como parte de una solución. El uso de un sistema

físico de rastreo como las etiquetas RFID le permitiría a las operadoras controlar el ciclo de vida del chip, desde su fabricación hasta su uso final. Este sistema tendría que estar vinculado a una base de datos central en la que se recojan todos los chips que han sido vendidos y activados, de manera que las autoridades dispongan en tiempo real de información sobre cualquier transacción que esté marcando señales de alarma. Con esto, a la práctica estas medidas permitirían que la probabilidad de que los chips terminen en manos equivocadas sea bastante limitada.

Las leyes actuales son insuficientes debido a que no abordan cada faceta del proceso de venta de chips. Las penas por la venta ilegal de chips no representan una amenaza, y no hay un método para rastrear las ventas realizadas fuera de los puntos de venta oficiales. Es esencial que la ley de telecomunicaciones integre una regulación que requiera la vigilancia activa de cada venta para que las compañías de teléfonos móviles capturen todas las transacciones y permita a las autoridades de supervisión responder rápidamente en casos de abuso.

Evans Daniel Velásquez Medina
DNI N°: 43352902

GUÍA DE ENTREVISTA

Entrevistado 4: Carlos Oré Cordero
DNI N°: 45640993
CIP N°: 31513741
Lugar de trabajo: División de Investigación de Delitos Informáticos de la Dirección de Ciberdelincuencia de la PNP - DIRCIBERD PNP (antes DIVINDAT).

Preguntas:

1. **¿Cuáles son los factores que, a su juicio, facilitan la suplantación de identidad en el contexto de la venta informal de chips de teléfono en Lima, y qué medidas se podrían tomar para prevenir este tipo de delitos?**

   Rpta.- La falta de procedimientos sistematizados para la comercialización de chips en lugares informales legales constituye uno de los factores que propician la falta de control referente a la suplantación de identidad. En este caso, los vendedores informales acceden a chips en condiciones que los supuestos requisitos de verificación de la identidad no se obligatoriamente tienen que cumplirse. Si bien existen medidas que se ejecutan a partir de dispositivos biométricos, el riesgo siempre existe. Para que el enfoque propuesto sea doblemente efectivo, sugiero que en las zonas públicas se establezcan quioscos autorizados donde se presten los servicios mencionados y donde cada vendedor esté obligado a verificar electrónicamente cada venta ingresando en un sistema central que se vincula con las instituciones que manejan la seguridad.
   El problema principal es la falta de control suficiente sobre la venta de chips fuera de los centros autorizados. La legislación actual no exige a los vendedores ambulantes que verifiquen la identidad del comprador o incluso que registren las ventas. Se sugiere que se cree una ley específica que controle la venta de chips en kioscos informales y que exija que cada venta se registre en un sistema informático. Esto no solo mejoraría el control sobre las transacciones en sí, sino que también ayudaría a las autoridades a determinar rápidamente quiénes son los suplantadores.

2. **Desde su experiencia en ciberdelincuencia, ¿cómo califica la efectividad de la prevención y persecución de la venta de chips para la comisión de delitos de suplantación de identidad, y qué modificaciones consideran que deben realizarse para fortalecer la lucha contra estos delitos?**

   Rpta.- Hasta la fecha, las estrategias de control para las ventas informales no han sido cumplidas con éxito. El control biométrico, si bien es importante, no puede ser la única solución. Lo que más me preocupa, sin embargo, es el hecho de que no hay una

forma posible de rastrear los chips una vez que se venden fuera de los canales oficiales. Sugiero la creación de centros de recolección de chips en rutas donde las personas puedan verificar si el chip que están comprando es genuino. Este centro podría estar conectado a un sistema que verifique no solo la identidad del comprador, sino también la identidad del chip y asegure que no ha sido robado o abusado en el pasado.

A pesar de que la legislación actual ha logrado algún nivel de control en la venta de dispositivos móviles, aún no gestiona óptimamente los mercados informales. Se necesita una mayor aplicación de estas leyes, y los operadores de telecomunicaciones deben asumir la responsabilidad de las ventas fuera de sus puntos de venta autorizados. Sugiero que se obliga a los operadores a implementar un sistema para monitorear ventas y activaciones, donde todas las transacciones se registran electrónicamente para prevenir actividades fraudulentas. Además, las autoridades deben tener acceso en tiempo real a los registros para poder monitorear actividades ilegales.

Carlos Oré Cordero
DNI N°: 45640993

GUÍA DE ENTREVISTA

Entrevistado 5: Gonzálo Jair Rodríguez Mezarina
DNI N°: 44544436
Lugar de trabajo: EXPERIS PERÚ SAC.

Preguntas:

1. **¿Cuáles son los factores que, a su juicio, facilitan la suplantación de identidad en el contexto de la venta informal de chips de teléfono en Lima, y qué medidas se podrían tomar para prevenir este tipo de delitos?**

   Rpta.- El problema más grave de la venta ambulatoria de chips es la irresponsabilidad de quienes los venden. No hay un mecanismo efectivo de control que certifique la legitimidad de los chips que se venden. Aunque hay algunos sistemas de verificación que se utilizan, la red de suministro de los chips no se monitorea exhaustivamente y, por lo tanto, existe la posibilidad de que se obtengan de manera ilegal. Para este tema, sugerimos que se implemente un sistema que controle toda la venta de los chips a través de blockchain, desde la fabricación hasta la activación. Esto permite a las autoridades verificar la autenticidad de cada chip y constatar que no se utilizan para delitos de suplantación de identidad.
   Los mercados informales móviles aún son un área poco regulada, incluso con los controles biométricos que se han implementado. La legislación actual no exige a los vendedores informales informar las ventas de chips ni existe un sistema de verificación confiable de la identidad de los compradores.

2. **Desde su experiencia en ciberdelincuencia, ¿cómo califica la efectividad de la prevención y persecución de la venta de chips para la comisión de delitos de suplantación de identidad, y qué modificaciones consideran que deben realizarse para fortalecer la lucha contra estos delitos?**

   Rpta.- Actualmente, las estrategias se concentran en gran medida en la verificación biométrica, que aún es inadecuada porque no cubre cada faceta del proceso de ventas. En mi opinión, la solución debe ser una arquitectura que permita la verificación no solo en el momento de la activación, sino desde la primera venta. La solución, en mi opinión, debe tener la posibilidad de un sistema de verificación en línea donde los compradores puedan utilizar una aplicación móvil para confirmar que el chip que están comprando está efectivamente registrado y es legítimo. Esto puede requerir el desarrollo de una plataforma digital que esté integrada con las bases de datos de los operadores móviles y las fuerzas de seguridad, lo que haría posible frenar de manera más precisa y efectiva los controles sobre transacciones ilegales.

Las estrategias actuales no logran mitigar los riesgos asociados con la venta informal de chips. Si bien los controles biométricos abordan parte del problema, la legislación debe avanzar hacia un enfoque más holístico que cubra todos los aspectos del proceso de venta, desde la fabricación hasta la activación. Sugiero que los legisladores tomen medidas para hacer obligatorio que los operadores de telecomunicaciones registren electrónicamente todas las transacciones, y que estas bases de datos sean accesibles para los servicios de seguridad. Este sistema permitiría a las autoridades responder de manera oportuna si se detectan ventas ilegales o de robo de identidad.

Ing. Gonzálo Jair Rodríguez Mezarina
DNI N°: 44544436

Anexo 2.2. Ficha de análisis documental

FICHA DE RESUMEN DE ANÁLISIS DE DATOS

Documento: Texto Sustitutorio Consensuado recaído en los Proyectos de Ley 9136/2024-CR, 9240/2024-CR y 9656/2024-CR, que, con texto sustitutorio proponen la Ley que modifica la Ley 30096, Ley de Delitos informáticos, y el Código Penal, Decreto Legislativo 635, respecto a la activación ilegal de líneas de servicios móviles y a la posesión ilegal de SIM CARD.

Objetivo	Analizar cómo la venta informal de chips móviles influye legalmente en el aumento de los delitos informáticos, en particular en los casos de suplantación de identidad, y plantear reformas legales que refuercen la protección de los derechos de los ciudadanos en el Perú.	
Modalidad del análisis	**Presencial**	**Virtual**
		X
Conclusión de análisis, según objetivo	La venta informal de chips móviles representa un problema muy serio en la seguridad de los ciudadanos, sobre todo en relación con delitos cibernéticos como la usurpación de identidad. El análisis del marco de la legislación aplicable, que propone modificaciones a la Ley 30096 y al Código Penal en Perú, establece regulaciones de control más rigurosas con respecto a la activación ilegal de servicios móviles, lo que contribuye a la disminución de este tipo de delitos. La venta ilegal de chips de los cuales se puede hacer mal uso es ampliamente fomentada con el artículo 9-A de la ley que estipula la activación no permitida de líneas móviles y el artículo 222-B que estipula la tenencia ilegal de tarjetas SIM. En alineación con el objetivo establecido en este estudio, la reforma legal propuesta aumenta, más que lo que se había hecho anteriormente, la protección accesible a los ciudadanos con respecto a las crecientes actividades de ciberdelincuencia relevantes al comercio malicioso de tarjetas SIM. La legislación modificada tiene como objetivo tanto frenar el comercio ilegal de estos dispositivos como proteger las identidades de los usuarios y la información personal del fraude por suplantación. Así, la adopción de tales cambios legales busca no solo castigar a los perpetradores, sino también proporcionar un marco más sólido para la protección de los derechos digitales de los ciudadanos, lo que mejora libremente la certeza legal en el campo de las telecomunicaciones y la mitigación de la ciberdelincuencia. Este enfoque es crucial para contener las consecuencias del comercio ilegal de chips móviles, que es una nueva tendencia que socava la fe de los ciudadanos en el sistema de telecomunicaciones mientras los pone en un riesgo significativo de fraude y robo de identidad. Los cambios están destinados a abordar la necesidad de no solo castigar, sino también proporcionar componentes de prevención y educación que traten sobre estas actividades ilegales.	

Texto Sustitutorio Consensuado recaído en los Proyectos de Ley 9136/2024-CR, 9240/2024-CR y 9656/2024-CR, que, con texto sustitutorio proponen la Ley que modifica la Ley 30096, Ley de Delitos informáticos, y el Código Penal, Decreto Legislativo 635, respecto a la activación ilegal de líneas de servicios móviles y a la posesión ilegal de SIM CARD

SUSTENTO DEL TEXTO SUSTITUTORIO CONSENSUADO:

Los cambios en la fórmula legal del presente texto sustitutorio incorporan sugerencias formuladas por los congresistas Rosangella Andrea Barbarán Reyes y Alejandro Soto Reyes.

Vale mencionar que este es un Texto consensuado con la Comisión de Defensa del Consumidor y Organismos Reguladores de los Servicios Públicos, presidida por el Congreso Idelso Manuel García Correa.

LEY QUE MODIFICA LA LEY 30096, LEY DE DELITOS INFORMATICOS, Y EL CODIGO PENAL, DECRETO LEGISLATIVO 635, RESPECTO A LA ACTIVACION ILEGAL DE LINEAS DE SERVICIOS MOVILES Y A LA POSESION ILEGAL DE SIM CARD

Artículo 1. Incorporación del articulo 9-A en la Ley 30096, Ley de Delitos Informáticos

Se incorpora el articulo 9-A en la Ley 30096, Ley de Delitos informáticos, con la siguiente redacción:

> **"Articulo 9-A. Activación de una SIM Card o de una línea de servicio móvil sin consentimiento del titular**
> **El que, mediante sistemas informáticos u otro mecanismo, active una SIM Card o una línea de servicio móvil en la plataforma de abonados de una empresa operadora sin el consentimiento del titular, o cuando la información proporcionada del titular sea falsa, será reprimido con pena privativa de libertad no menor de cuatro ni mayor de ocho años y con inhabilitación conforme al numeral 4 del artículo 36 del Código Penal".**

Artículo 2. Modificación del artículo 222-B del Código Penal, Decreto Legislativo 635

Se modifica el artículo 222-B del Código Penal, Decreto Legislative) 635, en los siguientes términos:

Texto Sustitutorio Consensuado recaído en los Proyectos de Ley 9136/2024-CR, 9240/2024-CR y 9656/2024-CR, que, con texto sustitutorio proponen la Ley que modifica la Ley 30096, Ley de Delitos informáticos, y el Código Penal, Decreto Legislativo 635, respecto a la activación ilegal de líneas de servicios móviles y a la posesión ilegal de SIM CARD

> **"Articulo 222-B. Posesión ilegitima de una SIM card u otro medio activado que este asociado a una línea de servicio móvil**
> El que provea, comercialice o facilite la adquisición de una SIM card **u otro medio activado ilegalmente que este asociado a una línea de servicio móvil** será reprimido con pena privativa de libertad no menor de cinco ni mayor de nueve años y con inhabilitación conforme al numeral 4 del artículo 36 del código Penal. Si el agente adquiere o posee el SIM card **u otra medida activada ilegalmente que este asociado a una línea de servicio móvil**, será reprimido con pena privativa de libertad no menor de **cuatro** ni mayor **de ocho años**".

Artículo 3. Incorporación del articulo 272-A en el Código Penal, Decreto Legislativo 635
Se incorpora el articulo 272-A en el Código Penal, Decreto Legislativo 635, con la siguiente redacción:

> **"Articulo 272-A. Comercialización ilegal de servicios públicos móviles**
> **El que ofrezca, promocione, comercialice o realice contrataciones de servicios públicos móviles de forma ambulatoria o en la vía pública, salvo aquellos casos que la norma lo autorice, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con una multa de trescientos sesenta y cinco a setecientos treinta dias multa."**

DISPOSICION COMPLEMENTARIA FINAL

ÚNICA. Disposiciones adicionales
El Poder Ejecutivo, a través de la Presidencia del Consejo de Ministros, del Ministerio de Justicia y Derechos Humanos y del Ministerio de Transportes y Comunicaciones, en un plazo de sesenta dias calendarios contados a partir de la entrada en vigor de la presente ley, emite las disposiciones adicionales necesarias para la aplicación de las modificaciones dispuestas por esta ley.

DISPOSICION COMPLEMENTARIA MODIFICATORIA

Texto Sustitutorio Consensuado recaído en los Proyectos de Ley 9136/2024-CR, 9240/2024-CR y 9656/2024-CR, que, con texto sustitutorio proponen la Ley que modifica la Ley 30096, Ley de Delitos informáticos, y el Código Penal, Decreto Legislativo 635, respecto a la activación ilegal de líneas de servicios móviles y a la posesión ilegal de SIM CARD

UNICA. Modificación del artículo 16 de la Ley 27336, Ley de Desarrollo de las Funciones y Facultades del Organismo Supervisor de inversión Privada en Telecomunicaciones - OSIPTEL

Se modifica el literal f) del artículo 16 de la Ley 27336, Ley de Desarrollo de las Funciones y Facultades del Organismo Supervisor de inversión Privada en Telecomunicaciones - OSIPTEL, en los siguientes términos:

> **"Articulo 16.- Obligaciones de las entidades supervisadas Las entidades supervisadas se encuentran obligadas a:**
> **[...]**
> **f) Proporcionar y facilitar al OSIPTEL, a través de herramientas informáticas, el acceso a toda la información del proceso de comercialización, contratación y activación de los servicios públicos de telecomunicaciones en donde se identifique al personal que interviene, para que sea entregada al Ministerio Publico, a la Policía Nacional del Perú y a las demás entidades que lo requieran."**

Sala del Pleno, 10 de abril de 2025.

ISAAC MITA ALANOCA
Presidente de la
Comisión de Justicia y Derechos Humanos

IDELSO MANUEL GARCIA CORREA
Presidente de la Comisión de Defensa del Consumidor y Organismos Reguladores de los Servicios Públicos

Anexo 2.3. Ficha de grupo focal (*focus group*)

FICHA DE GRUPO FOCAL

Facilitador: Gonzálo Rodríguez Peña		
Fecha: 29 de abril de 2025.		**Hora**: 6:38pm
Lugar: Virtual (Plataforma Zoom)		**Nº de participantes:** Cinco (05).
OBJETIVO GENERAL	**OBJETIVOS ESPECÍFICOS**	**ANÁLISIS**
Objetivo General: Analizar cómo la venta informal de chips móviles influye legalmente en el aumento de los delitos informáticos, en particular en los casos de suplantación de identidad, y plantear reformas legales que refuercen la protección de los derechos de los ciudadanos en el Perú.	**Objetivo específico 1:** Analizar los vacíos legales y regulatorios que existen en la legislación peruana sobre la venta informal de chips móviles, y cómo estos vacíos contribuyen a que se cometan delitos informáticos como la suplantación de identidad.	Se sigue advirtiendo que la falta de legislación y reglamentación en torno a la venta informal de chips móviles en Perú continúa siendo una de las principales causas de delitos informáticos, como la suplantación de identidad. A pesar de la intención de controlar la venta de chips a través del control biométrico y otras regulaciones, aún persisten varios silos que permiten el acceso no autorizado a la red de telecomunicaciones, permitiendo así fraudes y el uso indebido de identidades. El grupo de participantes coinciden que aunque la venta de tarjetas SIM está controlada dentro de muchos pasos del proceso, todavía hay algunas prácticas informales que escapan al control de las autoridades. La brecha en la ley significa que en muchas instancias los vendedores informales pueden y quedan impunes. Esta falta de control es fundamental para entender por qué los delitos asociados con el robo de identidad aumentan de manera tan pronunciada; las tarjetas SIM compradas ilegalmente pueden ser utilizadas para abrir cuentas bancarias, cometer fraudes en línea y otras transacciones bancarias de ese tipo. Además, el grupo destacó la insuficiencia de las sanciones para los perpetradores de la venta ilegal de chips móviles. La penalización para estas personas es inadecuada, lo que permite la continuación del delito sin consecuencias graves. Aunque hay leyes que exigen la captura de la identidad del comprador, las autoridades no cuentan con un sistema de monitoreo centralizado que pueda identificar rápidamente actividades ilegales asociadas con la venta y activación de tarjetas SIM, lo que hace que detectar fraudes y rastrear a los perpetradores sea aún más difícil.

		Ante este contexto, estas brechas en la ley no solo ayudan y fomentan la proliferación de esquemas informales que involucran la venta de chips móviles, sino que también facilitan una amplia gama de delitos cibernéticos, incluido el robo de identidad. La venta descontrolada de tarjetas SIM, junto con la completa falta de supervisión estricta y normas débiles, sienta las bases para que los criminales obtengan fácilmente información sensible sobre las víctimas y sea utilizada indebidamente. Por lo tanto, se sugiere que, aunque la biometría ha avanzado en desarrollo, otras áreas regulatorias y legislativas aún requieren un fortalecimiento en su impacto. Desarrollar aún más las relaciones entre OSIPTEL y los operadores de telecomunicaciones, mejorar su coordinación y hacer cumplir sanciones más estrictas para el comercio ilegal de tarjetas SIM también ayudaría. Además, es crucial contar con un sistema de monitoreo más proactivo para identificar, rastrear y penalizar el comercio ilícito de chips móviles en tiempo real. Solo abrazando una reforma integral que aborde estas brechas se puede controlar de manera efectiva la venta informal de tarjetas SIM, reducir el cibercrimen y defender mejor los derechos de los ciudadanos.
	Objetivo específico 2: Evaluar el marco legal vigente en el Perú sobre la comercialización de dispositivos móviles y proponer cambios normativos que ayuden a prevenir su uso fraudulento en casos de suplantación de identidad.	El análisis del marco legal en Perú relacionado con la comercialización de dispositivos móviles muestra ciertas deficiencias. Estos intentos de restringir el mercado y proteger a los consumidores no son suficientes para salvaguardar contra el uso indebido de estos dispositivos, particularmente en lo que respecta al robo de identidad. A pesar de las normas que exigen verificaciones de identidad para la compra y activación de tarjetas SIM, las prácticas informales continúan haciendo que los dispositivos móviles y los servicios de telecomunicaciones sean accesibles sin los controles adecuados. Esta laguna regulatoria permite que individuos sin escrúpulos utilicen dispositivos móviles bajo alias o identidades robadas, lo que a su vez incrementa los delitos cibernéticos como el robo de identidad. Dado que no hay un control completo sobre la venta de dispositivos móviles en Perú hasta el momento, existe una política de activación de líneas móviles que utiliza identificación biométrica. La falta de procedimientos de verificación exhaustivos en el punto de venta significa que los criminales pueden comprar dispositivos sin ninguna verificación de identificación precisa. La ausencia de tales controles integrales permite la comisión de actividades fraudulentas, como asociar dispositivos móviles con identidades robadas, lo que a su vez permite que los criminales se hagan pasar por otras personas en redes sociales, fraudes bancarios y muchos más. Hay claros vacíos en la ley respecto a las medidas punitivas y herramientas de supervisión. Existen leyes que restringen activamente la venta informal de dispositivos móviles, sin embargo, la aplicación y la imposición de medidas punitivas son demasiado lenientes. Esta falta de aplicación deja a los dispositivos móviles expuestos al mercado negro criminal, donde los delincuentes pueden comprarlos para usarlos con documentos de identidad fraudulentos.

		Para prevenir el uso fraudulento de los dispositivos móviles, es importante modificar la legislación incluyendo más control en la comercialización de dispositivos, así como en la activación de las líneas móviles y en la venta o distribución del equipo. Esto podría incluir hacer obligatorio el registro de los compradores de dispositivos móviles de la misma manera que se registra a los titulares de tarjetas SIM, utilizando tecnologías como la identificación biométrica o la verificación de documentos oficiales. Además, debería haber regulaciones más severas y específicas contra la venta o comercialización ilegal de dispositivos sin el registro o documentación adecuados. También podría ser razonable diseñar un sistema único que permita a las autoridades monitorear las ventas y activaciones de dispositivos móviles, permitiendo el acceso para controlar el uso fraudulento o irregular de estos dispositivos. En conclusión, el marco legal existente en Perú requiere reformas para mejorar el control sobre la comercialización de dispositivos móviles. Con medidas que involucren registros más completos y la aplicación de técnicas sofisticadas para la inspección de la identidad del comprador, el uso fraudulento de estos dispositivos podría ser más efectivamente mitigado, protegiendo a los ciudadanos del robo de identidad y delitos relacionados con computadoras.
	Objetivo específico 3: Estudiar cómo las leyes peruanas en materia de delitos informáticos enfrentan la suplantación de identidad facilitada por la venta ilegal de chips móviles, e identificar aspectos que podrían mejorarse para garantizar una mayor protección de los derechos ciudadanos.	La revisión de las normas legales sobre delitos informáticos emite un juicio de valor negativo sobre el Perú, porque incluso la legislación que se tiene para el caso de la suplantación de identidad por el uso fraudulento de chips móviles o celular tiene graves lagunas que no ofrece solución alguna. Actualmente se pretende evitar el delito de suplantación de identidad mediante el control de SIM cards. Sin embargo, la venta ilegal de SIM chips continúa siendo un blanco fácil para los criminales que burlan los controles. De este modo, facilitan el obtención ilícito de servicios de telecomunicaciones y, a su vez, el acceso a la suplantación de identidad. Primero, como la Ley 30096 (Ley de delitos informáticos), las leyes peruanas al respecto estudios sobre suplantación de identidad y delitos conexos, pero la venta clandestina de chips móviles sigue sin estar del todo controlada. Si bien hay intentos regulando la activación de líneas móviles a través del registro biométrico, la venta de teléfonos móviles se encuentra reglamentada. Esto permite un margen de error dentro de la legislación donde la delincuencia puede hacerse de dispositivos y SIM cards sin ninguna verificación de identidad siendo esto un gran potencial para ser violadas las leyes de suplantación de identidad. La legislación peruana tiene un problema más y es la falta de efectividad en la aplicación de las leyes y en las sanciones. La falta de proporcionalidad en las sanciones que se establecen para las personas que se dedican a la venta ilegal de chips móviles hace que este tipo de infracción no esté acompañada por las consecuencias necesarias. Además, lo que permite que sin un sistema de monitoreo eficiente centralizado se

		limite la identificación y control de actividades ilegales que permiten la multiplicación de las suplantaciones de identidad. Una mayor protección a los derechos de los ciudadanos exige reformas que incluyan el fortalecimiento de las sanciones por venta ilegal de dispositivos móviles, así como de los mecanismos para su seguimiento y verificación. Además, se debería exigir registro obligatorio, no solo para la activación de las SIM cards, sino para toda la compra de dispositivos móviles, mediante tecnologías que garanticen el reconocimiento del comprador. También resulta de gran relevancia el incremento de la articulación entre los organismos reguladores y la fuerza de seguridad para el incremento de la detección y control de las actividades ilícitas. A manera de conclusión, es evidente que las disposiciones relativas a los delitos informáticos en Perú han iniciado el camino hacia la protección frente a la suplantación de identidad que, hasta ahora, carecía de redacción legislativa. No obstante, el marco normativo exige ajustes en la derogada atención a la venta ilícita de chips móviles. Su adecuación para elevar la contundencia en las contravenciones, sumar un control integral sobre la distribución de teléfonos móviles y motu proprio la vertebración normativa cobra importancia en defensa de los derechos de los ciudadanos frente a la suplantación de identidad y otros delitos informáticos.
	Objetivo específico 4: Determinar cuál es la responsabilidad legal de las empresas de telecomunicaciones y los proveedores de servicios móviles en la prevención de delitos informáticos relacionados con la venta no regulada de chips.	El análisis sobre la responsabilidad legal que tienen las empresas de telecomunicaciones, así como los proveedores de servicios móviles, en la prevención de delitos informáticos vinculados a la venta ilegal de chips SIM, revela aspectos relevantes. Los operadores móviles y las empresas de telecomunicaciones tienen una función central en la gobernanza y control del mercado de dispositivos móviles y las SIM cards, puesto que son los que efectivamente activan las líneas móviles y administran los servicios que se suscriben. A partir de la legislación peruana, estas compañías tienen la responsabilidad de instaurar métodos de control de identidad que impidan el acceso ilícito a SIM cards que, de igual manera, permiten la comisión de delitos informáticos tales como el “impersonation”. Aun considerando los intentos de regulación, como el biometría para la activación de SIM cards, la comercialización sin control de chips continúa siendo una de las principales rutas que los delincuentes utilizan para la obtención ilegal de servicios móviles, promoviendo, así, el acceso no autorizado a los sistemas de telecomunicaciones. Dentro de las empresas de telecomunicaciones y de servicios móviles yace la responsabilidad legal que exige a estas gestionarse y controlar la venta de tarjetas SIM tanto por sus tiendas oficiales como por sus distribuidores. Estas empresas estánlegalmente obligadas a prevenir que la venta al por menor y la activación de dispositivos móviles y servicios se realicen de manera que socave la seguridad y verificación de la identidad, lo cual, al menos, debería involucrar la identificación clara del comprador y la confirmación de sus credenciales antes de la activación de una línea móvil.

		La ausencia de un mecanismo de control estricto para la supervisión y seguimiento de la venta de tarjetas SIM a través de canales informales es una omisión por parte de estas empresas. En muchas situaciones, estos proveedores no supervisan adecuadamente sus redes de venta y distribución, lo que resulta en la venta ilegal de tarjetas SIM que carecen de una verificación adecuada de identidad. Tal negligencia no solo permite la perpetración de delitos cibernéticos, sino que también compromete la seguridad de personas inocentes y del sistema de telecomunicaciones en su totalidad. Con respecto a los delitos contemplables en las sanciones impuestas, se ha señalado que las empresas de telecomunicaciones estarían expuestas a la responsabilidad legal si no toman medidas efectivas para impedir la venta no autorizada de chips. Con relación a la normativa vigente, podrían ser castigadas por incumplimiento con las obligaciones de verificación de identidad y control de comercialización de chips por configurar un control fraudulento generador de suplantación de identidad. Para el caso de las empresas de telecomunicaciones y los proveedores de servicios de telefonía móvil, podrían señalarse que tienen, a partir de la legislación nacional, una obligación jurídica ante la macrociber delincuencia en la modalidad referida a la venta sin control de chips. Para dar cumplimiento a esta obligación, deberían controlar que sus canales de venta se encuentren debidamente regulados; realizar controles de verificación más exigentes, así como contribuir con las autoridades en la identificación y sanción de conductas ilícitas. Es con este tipo de abordajes donde se contempla la responsabilidad tanto del control de la venta como de la activación que permiten mitigar a gran medida el impacto de los delitos informáticos asociados a la venta descontrolada de chips.
	Objetivo específico 5: Analizar las consecuencias jurídicas de la suplantación de identidad a través de la compra ilegal de chips móviles, en relación con los derechos fundamentales de las personas afectadas, como la privacidad y la protección de datos personales, y proponer soluciones legales viables.	La suplantación mediante la compra ilegal de chips móviles es problemática ya que afecta profundamente el orden legal, lo que impacta en los derechos fundamentales de una persona, en particular en el derecho a la privacidad y la protección de datos personales. El análisis del problema muestra que el uso indebido de tarjetas SIM ilegales permite a los delincuentes obtener información personal sensible de las víctimas, como detalles bancarios, contraseñas y otra información confidencial, lo que a su vez facilita la comisión de fraude, robo de identidad y otros delitos cibernéticos. Un análisis legal sugiere que el fraude de identidad a través de la compra ilegal de chips móviles infringe los derechos constitucionales en Perú, como la privacidad (Artículo 2 de la Constitución) y el derecho a la protección de datos (Ley N° 29733, Ley de Protección de Datos Personales). Estos derechos tienen como objetivo defender la integridad y seguridad de las personas frente a la manipulación y el uso indebido de la información personal. La falta de control efectivo en el mercado y la activación de tarjetas SIM, más allá de la venta ilegal de chips, lleva a que las víctimas sean privadas de vulneraciones fundamentales de sus derechos.

		Las consecuencias legales para las personas afectadas por el fraude de identidad son bastante severas. Una víctima puede sufrir daños económicos y psicológicos, como la incapacidad de acceder a sus cuentas bancarias, reputación personal, y la cantidad sustancial de tiempo y energía necesaria para resolver los problemas legales posteriores al robo de identidad. Además, personas no autorizadas pueden usar la identidad para cometer actividades fraudulentas, lo que agrava la vulneración de los derechos de la persona afectada. Respecto a las consecuencias penales asociadas a la venta ilegal de chips de teléfonos móviles, la legislación actual prevé un castigo bajo los delitos cibernéticos por robo de identidad, pero la aplicación de tales leyes deja mucho que desear. Las sanciones, en general, no son muy efectivas, y las redes informales de comercio de tarjetas SIM pasan desapercibidas. Por lo tanto, los vendedores de chips de teléfonos móviles operan de manera ilegal y venden chips sin ser atrapados. Esto resulta en que continúan en un entorno que no respeta las leyes y su venta de tales productos pasa sin consecuencia. Esto, más a menudo que no, lleva a que la integridad de las leyes y las violaciones no sean mantenidas ni defendidas. En un intento de asegurar una defensa y protección adecuadas de los derechos básicos de los ciudadanos, se necesitan introducir varias soluciones de trabajo. En primer lugar, para prevenir la venta excesiva de tarjetas SIM, se necesita implementar un control más estricto sobre su venta y sus procedimientos de identificación que efectivamente aumenten junto con los procedimientos de registro adecuados evitando la presentación de identificaciones falsas. También debe haber vínculos avanzados de ventas informales de chips móviles y directrices sobre violaciones de la seguridad de la protección de datos. Con el fin de fomentar investigaciones más efectivas y un castigo apropiado de los infractores, una recomendación adicional es mejorar la coordinación entre las autoridades reguladoras, como OSIPTEL, y las agencias de aplicación de la ley. Además, sería necesario crear conciencia entre los consumidores y los operadores de empresas de telecomunicaciones sobre la importancia de la protección de datos personales y los riesgos que plantea la venta ilegal de tarjetas SIM. La facilidad para cometer suplantación de identidad mediante la compra ilegal de chips móviles representa un peligro significativo para los derechos fundamentales de una persona, más aún para su privacidad y protección de datos personales. Existe la necesidad de introducir políticas de acción legales y regulatorias más efectivas sobre este problema y garantizar la seguridad de los ciudadanos mientras se defienden sus derechos contra el cibercrimen.

Anexo 2.3.1. Evidencia de *focus group* (*Google meet*)