UPN
UNIVERSIDAD PRIVADA DEL NORTE

FACULTAD DE DERECHO Y CIENCIAS POLÍTICAS

Carrera de Derecho

"EL COMERCIO ILEGAL DE SIMS CARDS Y SU INFLUENCIA EN LA COMISIÓN DE DELITO DE FRAUDE INFORMATICO REGISTRADOS EN LA DIVINDAT 2019-2022"

Tesis para optar el título profesional de:

ABOGADO

Autores:

Paulo Edgardo Huaman Miraval
Diego Alonso Merino Flores

Asesor:

Dr. Edith Corina Sebastián López
0000-0003-1656-6693

Lima - Perú

2025

UPN UNIVERSIDAD PRIVADA DEL NORTE

JURADO EVALUADOR

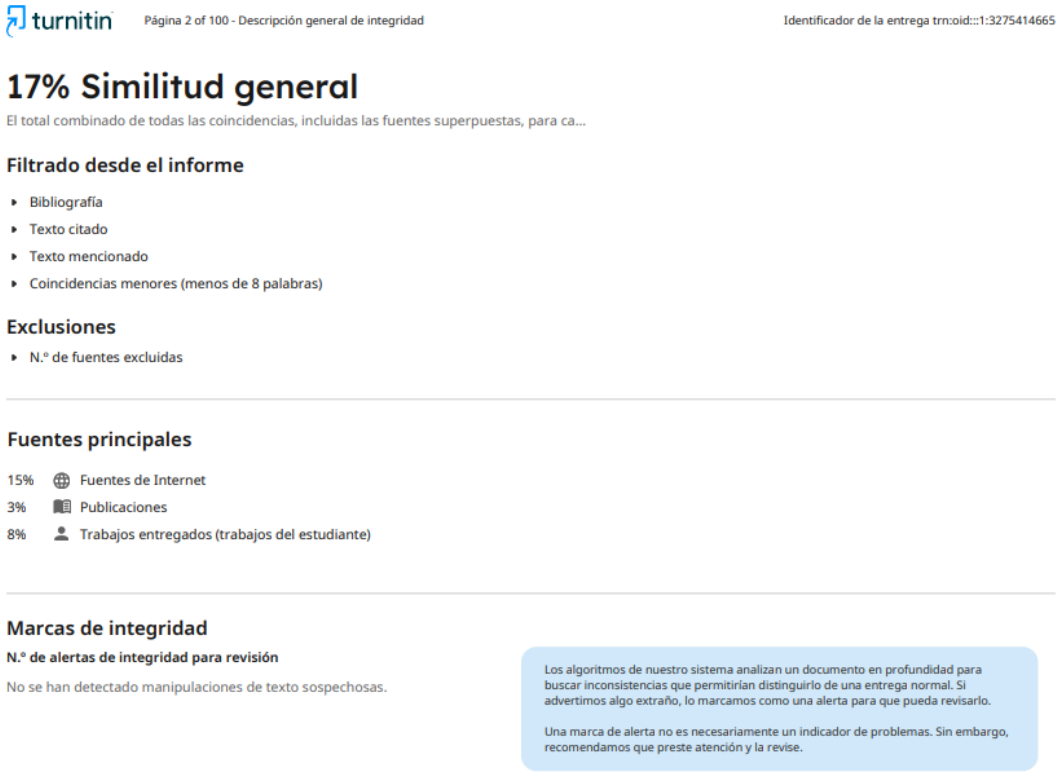
Jurado 1 Presidente(a)	**HAROLD GABRIEL VELAZCO MARMOLEJO**
	Nombre y Apellidos

Jurado 2	**EDWIN ADOLFO MOROCCO COLQUE**
	Nombre y Apellidos

Jurado 3	**EDITH CORINA SEBASTIAN LOPEZ**
	Nombre y Apellidos

UPN UNIVERSIDAD PRIVADA DEL NORTE

INFORME DE SIMILITUD



turnitin Página 2 of 100 - Descripción general de integridad Identificador de la entrega trn:oid:::1:3275414665

17% Similitud general

El total combinado de todas las coincidencias, incluidas las fuentes superpuestas, para ca...

Filtrado desde el informe

- Bibliografía
- Texto citado
- Texto mencionado
- Coincidencias menores (menos de 8 palabras)

Exclusiones

- N.º de fuentes excluidas

Fuentes principales

15% Fuentes de Internet
3% Publicaciones
8% Trabajos entregados (trabajos del estudiante)

Marcas de integridad

N.º de alertas de integridad para revisión

No se han detectado manipulaciones de texto sospechosas.

Los algoritmos de nuestro sistema analizan un documento en profundidad para buscar inconsistencias que permitirían distinguirlo de una entrega normal. Si advertimos algo extraño, lo marcamos como una alerta para que pueda revisarlo.

Una marca de alerta no es necesariamente un indicador de problemas. Sin embargo, recomendamos que preste atención y la revise.

UPN UNIVERSIDAD PRIVADA DEL NORTE

DEDICATORIA

"Dedico esta tesis a mi madre, quien partió el 9 de abril de 2022 y cuya memoria vive en cada paso que doy; su amor, su ejemplo y su fuerza siguen siendo mi guía. A mi hijo, nacido el 24 de septiembre de 2024, quien llegó a iluminar mi vida y darme un motivo aún más grande para luchar y alcanzar mis sueños. Y a mi padre, por su apoyo incondicional y por haber sido el sostén que me permitió continuar este camino; gracias por confiar en mí y hacer posible la culminación de esta etapa. Cada palabra de este trabajo lleva la huella de su amor, su esfuerzo y su presencia en mi vida."

- **Paulo Edgardo Huaman Miraval**

"A mis padres, quienes han sido pilares fundamentales en mi vida. Gracias por enseñarme a poner el "extra" en lo ordinario, por su amor incondicional, su apoyo constante y por mostrarme, con su ejemplo, el verdadero significado del esfuerzo y la dedicación. Esta tesis es tan mía como suya, porque sin ustedes, este logro no habría sido posible."

- **Diego Alonso Merino Flores**

UPN
UNIVERSIDAD PRIVADA DEL NORTE

AGRADECIMIENTOS

Agradecemos a nuestras familias que nos hayan brindado la oportunidad de alcanzar nuestras metas, hacer realidad nuestras aspiraciones y ser el pilar de apoyo durante los retos que surgieron a lo largo de nuestro periplo educativo. Su apoyo firme e inquebrantable ha sido inestimable para nuestras vidas.

Este trabajo no es solamente nuestro, sino el de un largo trecho de generaciones que se concentran en nosotros, gracias por el respaldo constante en cada momento de nuestras vidas en su institución. Aquí plasmo mi amor y agradecimiento eterno.

UPN UNIVERSIDAD PRIVADA DEL NORTE

RESUMEN

Nuestra investigación aborda el incremento respecto del fraude informatico dentro del Perú, destacando el periodo de pandemía como el "punto de partida" para el comercio ilegal de las tarjetas sims, permitiendo con ello el aumento de este tipo de delitos.

Conforme vayamos desarrollando la presente, se iran abordando las modalidades más frecuentas en este tipo de delitos, como el phishing o el smishing, modalidades mediante la cual los sujetos activos (victimario) obtiene información confidencial de las victimas mediante distintas mentiras hacía los sujetos pasivos (victimas). Teniendo como eje principal del problema las tarjetas SIMS adquiridas de manera ilegal, productos que permiten a los ciberdelicuentes operar de manera anónima y dificultando la ubicación de sus acciones, siendo el único beneficiario, como ya dijimos, el victimario, es decir el sujeto, es decir, el ciberdelincuente.

La presente enfatiza la importancia de la regulación y control en la comercialización de SIMs Cards, pues su venta ilegal es una pieza fundamental en esta cadena delictiva. Ello pese a la existencia de normativas y sanciones conforme lo señala el Código Penal a traves de su Art. 222, inciso B, inclusive con ello, la proliferación de SIMs Cards ilegales siguen siendo un desafio para las autoridades.

Asimismo, destacamos la labor de la *"División de Investigación de Delitos de Alta Tecnología (DIVINDAT)",* miembros de la Policia Nacional que se enfrentan a la compleja tarea como lo son estos delitos en la red, un entorno donde los ciberdelincuentes pueden operar desde cualquier parte del mundo, algo que afecta tanto a simples ciudadanos, como también a grandes instituciones del ambito público o privado.

Por último, se hace presente los antecedentes internacionales y nacionales, resaltando la necesidad de fortalecer los marcos legales y la cooperación internacional, como lo sugiere la "Estrategia de Ciberseguridad de la Unión Europea" y la ratificación del "Convenio de Budapest" por parte del Estado Peruano, concluyendose que además de las medidas legales, resulta esencial promover la educación y la concienciación en los sectores público y privado es crucial para detener el fraude informático y aminorar sus efectos, especialmente en relación con el comercio ilícito de tarjetas SIM.

PALABRAS CLAVES

Dentro de la presente investigación tenemos palabras claves como las que pasaremos a mencionar: ***Fraude Informatico, tipos, Sims Cards, Investigación, Enfoque, Diseño, Problemática, Nacional, Internacional, Principios, Instrumentos.***

ABSTRACT

Our research addresses the increase in computer fraud in Peru, highlighting how the pandemic period served as a "starting point" for the illegal trade of SIM cards, which in turn enabled the rise of these types of crimes. As this work develops, we will discuss the most frequent methods used in such offenses, such as phishing and smishing-modalities through which perpetrators obtain confidential information from victims by deceiving them in various ways. The central issue revolves around SIM cards acquired illegally, products that allow cybercriminals to operate anonymously and make it difficult to trace their actions, with the only beneficiary, as mentioned, being the perpetrator-in other words, the cybercriminal.

This paper emphasizes the importance of regulating and controlling the commercialization of SIM cards, since their illegal sale is a key factor in this criminal chain. This persists despite existing regulations and sanctions, as outlined in Article 222, subsection B of the Penal Code. Even so, the proliferation of illegal SIM cards continues to be a challenge for authorities.

We also highlight the work of the Division for the Investigation of High-Tech Crimes (DIVINDAT), members of the National Police who face the complex task of tackling these crimes online-a setting where cybercriminals can operate from anywhere in the world, affecting both ordinary citizens and major public or private institutions.

Lastly, both national and international examples are discussed, highlighting the necessity of fortifying legislative frameworks and fostering international collaboration, as indicated by Peru's acceptance of the Budapest Convention and the European Union Cybersecurity Strategy. The conclusion is that in order to avoid computer fraud and lessen its effects, particularly with regard to the illicit trade of SIM cards, it is crucial to support education and awareness in the public and private sectors in addition to legal measures.

|CAPÍTULO I: INTRODUCCIÓN

1.1. Realidad problemática

El fraude informático es una modalidad de delito contra el patrimonio, que se produce en el ciberespacio, el autor puede encontrarse lejos de la ubicación de la víctima, y las consecuencias pueden producirse en un lugar desconocido tanto para la víctima como para el autor. El fraude informático es un tipo de delito contra la propiedad en el que se utilizan como medio: las tecnologías de la información y la comunicación, y cuyo ámbito territorial no conoce fronteras.

A juicio de Pons (2017) el auge del internet y los sistemas informáticos marcaron un antes y un después en la forma en que las personas se introdujeron a los sistemas, cuyo uso configura y evoluciona nuestra forma de vida.

Nuestra observación es que a raíz de la pandemia y debido al auge del comercio electrónico o virtual, los índices criminales de delitos informáticos específicamente el de fraude informático se ha incrementado notablemente. El coronel PNP Orlando Mendieta, jefe de la División de Investigación de Alta Tecnología (DIVINDAT), precisó a la Agencia Andina que la cantidad de denuncias alcanzaron 2097 casos sobre delitos informáticos presentados el año 2019, además el coronel PNP Luis Edgardo Huaman Santamaria, jefe de la División de Investigación de Alta Tecnología (DIVINDAT), preciso que los delitos informáticos llegaron a una cantidad 3946 casos en el año 2022.

Las modalidades más frecuentes son el “phishing” y “smishing”, donde el delincuente informático a través de un correo electrónico o mensaje de texto envía un link que reconduce

a una página web falsa muy similar a las entidades financieras donde la victima creyendo que esta ante la página oficial de su banco, introduce su clave y contraseña, siendo de esta forma que los delincuentes informáticos acceden a dicha información y los usan para despojar a las víctimas de su patrimonio.

Las tarjetas **SIM** o **CHIP**, que son componentes accesorios de un dispositivo de telefonía móvil (celular) -es decir, tarjetas inteligentes extraíbles que se utilizan en los teléfonos móviles, fungiendo ahora como una herramienta u forma de perpetrar delitos de fraude informático. Estas tarjetas se conectan al dispositivo a través de una ranura de lectura o lector SIM. Permitiendo que sea posible cambiar la suscripción de un cliente de un terminal a otro simplemente cambiando la tarjeta SIM, que almacena de forma segura la clave de servicio del abonado utilizada para la identificación de la red.

Las modalidades de obtención de los servicios telefónicos, los procedimientos de contratación y la validación biométrica están señalados en la resolución del Consejo Directivo N° 172-2022/CD-CONSEJO DIRECTIVO, que tiene por objeto establecer los derechos y obligaciones tanto de las empresas autorizadas como de los usuarios de los servicios públicos de telecomunicaciones. Asimismo, constituye el marco normativo general dentro del cual se desarrollarán las relaciones entre ambos.

La División de Investigación de Delitos de Alta Tecnología de la PNP **(en adelante DIVINDAT)** tiene la misión de prevenir, combatir, investigar y denunciar, en el marco de la conducta legal de la rama fiscal, los delitos relacionados con la información, así como los delitos cometidos a través de las tecnologías de la información y la comunicación; estos delitos son cometidos, en gran parte, por delincuentes comunes u organizaciones criminales.

Dentro de la DIVINDAT labora personal masculino y femenino, personales procedentes de distintas regiones del país, los mismos que por su edad, tiempo de servicios y género. Todos ellos tienen ideas y creencias diferentes sobre la forma en que la venta ilegal de tarjetas SIM contribuye a la comisión de delitos de fraude informático y sobre cómo debería aumentarse la pena prevista en el artículo 222-B para garantizar que la venta de tarjetas SIM no contribuya a la comisión de delitos de fraude informático.

En consecuencia, lo que se busca con esta investigación, respecto a cómo influye la comercialización ilegal de SIMS CARDS en el fraude informático, es informar y resaltar que el crucial aumento en el uso de estas prácticas delictivas desde el 2019 en adelante es perjudicial para el Estado, los órganos autónomos y a la sociedad a pesar de tener en la parte sustantiva (Art. 222-B Código Penal) Por lo tanto, el vínculo entre la distribución ilegal de tarjetas SIM y el fraude de información pone de relieve la necesidad de fortalecer las sanciones penales, lo que tiene el efecto positivo de disminuir el impacto de los delitos cibernéticos en la sociedad.

Basándose en los argumentos anteriores, se formula el siguiente problema de investigación: ¿Cómo influye el comercio ilegal de tarjetas SIMS CARDS en la comisión de delitos de fraude informático, según los registros de la DIVINDAT durante el periodo 2019 - 2022?

UPN UNIVERSIDAD PRIVADA DEL NORTE

1.2. ANTECEDENTES

1.2.1. Antecedentes internacionales

La Estrategia de Ciberseguridad de la UE (Unión Europea - 2020) en Diciembre del año 2020, la Comisión Europea y el Servicio Europeo de Acción Exterior (SEAE) su estrategia sobre "seguridad cibernética" tiene por objeto reforzar que los países de la UE estén bien preparados y dispuestos para gestionar y reaccionar a los ciberataques en la que son víctimas tanto ciudadanos como empresas de distintos países pertenecientes a la unión europea, razón por la cual buscan erradicar las ciber amenazas y garantizar que estos ciudadanos y empresas tengan un salvaguardias, teniendo servicios y herramientas seguras y fiables. Como metodología aplican un tipo de investigación propositiva y hace uso de un método analítica; y, como conclusiones se sugieren tres métodos para mejorar la ciberseguridad: "1) Responsabilidades de seguridad para los proveedores de servicios digitales (mercados en línea, motores de búsqueda y servicios en la nube) y los operadores de servicios críticos (en industrias críticas como la energía, el transporte, la sanidad y las finanzas). 2) Colaborar con socios mundiales para garantizar la seguridad y estabilidad globales en el ciberespacio, y 3) Establecer una Unidad Cibernética Conjunta puede garantizar la mejor respuesta posible a las ciberamenazas aprovechando los recursos y conocimientos combinados que la UE y sus Estados miembros tienen a su disposición. Creemos que con la aplicación de estas normas se reforzaría la ciberseguridad de nuestra nación y se evitaría y eliminaría el fraude informático provocado por la venta ilícita de tarjetas SIM."

Consideramos que estos criterios permitirían fortalecer la seguridad cibernética de nuestro país para así prevenir y erradicar el fraude informático producto de la comercialización ilegal de SIMS CARDS.

Según ***Macías-Lara, RA., Boné Andrade, MF., Quiñonez Angulo, F., Mendoza Loor, JJ, Estupiñan-Troya, G., & Rodríguez Vizuete, JD . (2022)*** en su investigación "Casos frecuentes, criminalización y prevención de los delitos informáticos en el Ecuador: una breve revisión sistemática", el objetivo de este estudio es dar a conocer las tácticas empleadas por los ciberdelincuentes ecuatorianos y brindar información sobre las consecuencias y consejos para prevenir este tipo de delitos. Se recomienda que el gobierno y las instituciones públicas y privadas apoyen capacitaciones donde se socialicen los riesgos y tipos de delitos informáticos, normativas que regulen estos actos delictivos en relación a la tecnología y consejos para protegerse y adelantarse a los ciberdelincuentes. El Estudio de Mapeo Sistemático (SMS) fue la metodología utilizada, que permitió el inicio de la definición de la búsqueda, seguida de la ejecución de la búsqueda, la discusión y los resultados. Consideramos que la promoción de capacitaciones permitiría reducir los casos de fraude informático puesto que la mayoría son producto de la comercialización ilegal de los SIMS CARDS.

Según Acosta, Benavides y García (2020), en su investigación sobre "delitos informáticos: Impunidad organizacional y su complejidad en el mundo de los negocios", pretende identificar las principales categorías de ciberdelitos actuales y las amenazas que plantean a los gobiernos, las empresas y la sociedad. Se trata de una forma mixta de investigación que hace hincapié en las teorías y leyes pertinentes y se

apoya tanto en estudios exploratorios como confirmatorios. Según sus conclusiones, los delitos informáticos son cualquier actividad ilegal llevada a cabo mediante el uso del ciberespacio con el objetivo de erradicar y, en determinadas situaciones, difamar y extorsionar a los usuarios de redes de Internet y medios electrónicos. Este criterio, en nuestra opinión, responde a la exigencia de entender la delincuencia digital diseccionando el fraude informático y su progresión, comenzando por la comercialización ilícita de tarjetas SIM.

Según ***Campos, N. J. O. (2019)*** en su investigación sobre "Normativa Legal sobre Delitos Informáticos en Ecuador", tiene por objeto dar a conocer sobre los beneficios, el avance tecnológico y la creciente accesibilidad al internet, pero estos beneficios se tornan peligrosos cuando se infiltran programas maliciosos que dañan a los equipos tecnológicos. Como metodología aplican una investigación de tipo cualitativa, descriptiva, jurídica y comparativa; además, como demuestran los resultados: La mayoría de los ciberdelitos implican el uso de ingeniería social por parte de los delincuentes para engañar a sus víctimas. Además, se observa que las empresas públicas y comerciales de Ecuador no cuentan con un sistema de gestión de seguridad eficiente que les permita disminuir los efectos de los ciberataques internos o externos. Al respecto, se menciona que el cibercrimen es cada vez más frecuente en toda América Latina y que combatirlo es un reto porque no existe un marco legal uniforme que permita enfrentar este tipo de delitos. Para combatir el cibercrimen que cruza las fronteras nacionales, también se enfatiza lo crucial que es que las autoridades de muchas naciones trabajen juntas. Por último, se mencionan algunos de los delitos informáticos más perjudiciales en términos económicos y sociales a nivel global,

como el ciberterrorismo. Por último, consideramos que Ecuador, como país en desarrollo, enfrenta desafíos importantes en la lucha contra el cibercrimen debido a la falta de recursos y la complejidad de las leyes internacionales. Y a pesar de que el país tomo medidas reguladoras sobre el uso de la tecnología y las sanciones de delitos cibernéticos. Creemos que se necesita más educación y concientización para prevenir el cibercrimen y mejorar la seguridad.

1.2.2. Antecedentes nacionales

Según ***Vilca Aira, G. L. (2018)*** en su investigación sobre "Los hackers delito informático frente al código penal peruano", pretende identificar las lagunas legales de nuestro código penal en materia de comunicaciones electrónicas comerciales (la existencia de hackers). Para ello, se evalúa la relevancia jurídica de estas comunicaciones desde la perspectiva de sus efectos perjudiciales para la sociedad en general y para el derecho fundamental a la intimidad en particular. A partir de los resultados, se establecen soluciones y se proponen mejoras para su regulación. Tiene como metodología una investigación dogmática, jurídica, descriptiva; y, como conclusiones proponen siete criterios fundamentales sobre el vacío legal en nuestro código penal tiene: 1) Las tecnologías de la información, que permiten un marco de referencia adecuado para el manejo de estas circunstancias, requieren mayor comprensión. 2) Si bien el Perú controla los delitos informáticos, lo hace de manera inadecuada. 3) El tema de los delitos cometidos en línea es un tema que impacta a la sociedad globalmente, 4) El alto índice de delitos informáticos en el Perú no hace más que contribuir al desconocimiento general sobre el tema, 5) Es esencial y necesaria una adecuada capacitación de los investigadores de delitos informáticos, 6) Para cumplir con los requisitos de admisibilidad, la evidencia

digital debe ser cuidadosamente recopilada y procesada antes de ser presentada en juicio. 7) En el curso de la investigación, es crucial confirmar la autenticidad de las pruebas digitales. Consideramos que estos criterios responden a las necesidades de una estructura normativa que permita combatir al delito de fraude informático producto de la comercialización de tarjetas SIMS CARDS, puesto que en nuestro país se tiene muy poco conocimiento sobre el tema.

Según ***Los Estados del Consejo Europeo***, El Perú ratificó el Convenio de Budapest (2019) y que de su preámbulo se desprende que esta tiene por finalidad que los estados miembros puedan contar con una política penal compartida para salvaguardar a la sociedad de la ciberdelincuencia mediante la promulgación de leyes que repriman con éxito la ciberdelincuencia tanto desde el punto de vista sustantivo como procesal. A ello se añade una cooperación internacional suficiente, ya que es esencial detener las acciones que ponen en peligro la disponibilidad, confidencialidad e integridad de los sistemas, redes y datos informáticos, así como el uso indebido de estos sistemas, redes y datos.

Respecto de las realidades locales y regionales, pensamos que este acuerdo de Budapest nos permitirá combatir, prevenir y erradicar delitos digitales como el fraude informático.

Según ***Huamán Cruz, M. Y. (2020)*** en su investigación sobre "Los delitos informáticos en Perú y la suscripción del Convenio de Budapest", tiene por objeto pretende comprender el papel que desempeña nuestro Estado en la lucha contra los ciberdelitos y examinar un mundo en el que estos delitos son cada vez más frecuentes. Utilizan como metodología la investigación cualitativa, la descriptiva jurídica y la comparativa, y sus conclusiones señalan que 1) la adhesión al Convenio de Budapest

influye de manera relativa en el tratamiento de los delitos informáticos, 2) el desarrollo legislativo de los delitos informáticos, 3) la problemática actual de los delitos informáticos en el Perú, 4) la adhesión de los países sudamericanos a este convenio y 5) los efectos de la firma del convenio. Consideramos que la ratificación del Convenio de Budapest por parte de Perú ha permitido combatir delitos informáticos como el fraude informático provocado por la venta ilícita de tarjetas SIM.

Según ***Vásquez (2022)*** en su investigación sobre "el procesamiento penal de la persona jurídica involucrada en la comisión de delitos informáticos en el Perú, 2022", el objetivo de este estudio es determinar si la persona jurídica que comete delitos informáticos en el Perú es adecuadamente perseguida penalmente. Asimismo, se pretende analizar los componentes de juicio a fin de integrarlos en un proceso penal por delitos informáticos y sugerir una fórmula de persecución penal adecuada para entes colectivos en casos de ciberdelitos. Al ser el primer estudio de este tipo, la investigación es exploratoria y cualitativa. Como resultado, ofrece a los operadores de justicia penal los fundamentos teóricos y el apoyo dogmático que necesitan para manejar eficazmente los casos que involucran a empresas y delitos informáticos. El estudio concluye que los delitos informáticos deberían agregarse a la lista de delitos contemplados en la Ley 30424, Ley que Regula la Responsabilidad Administrativa de la Persona Jurídica. Consideramos que no solo las personas naturales son las que cometen delitos de fraude informático, sino también las personas jurídicas en nombre de ellas o a favor de terceros, en especial a las compañías que brindan SIMS CARDS.

Según ***Robles Sotomayor, F. M. (2018)*** en su investigación titulada "La protección de datos personales como medio de prevención de los delitos informáticos en el Perú, en

los años 2017 y 2018" los objetivos son determinar si la prevención de delitos informáticos en el Perú y la protección de datos personales están relacionadas. Utiliza una metodología deductiva, inductiva y dogmática; como conclusiones sugiere tres normas esenciales que permiten relacionar los delitos informáticos y los datos personales:1) Se ha encontrado que los datos personales si se relaciona en forma directa con la prevención de los delitos informáticos, 2) que se pone en riesgo al titular de los datos personales por las actividades de comercio electrónico, 3) La ley 29733 sí se relaciona de manera directa con la prevención de los delitos informáticos en el Perú. Consideramos que estos criterios responden a nuestro tema sobre la comercialización ilegal de SIMS CARDS para la comisión del delito de fraude informático puesto que se pone en riesgo los datos personales del titular de los datos personales.

1.3. Marco teórico

1.3.1. Fraude Informático

De manera concreta, tenemos que hacer mención de lo que señalado por Laura Mayer Luz, quien de manera breve y mediante su artículo ***"El bien Jurídico Protegido en los Delitos Informáticos",*** que el delito informático se refiere a conductas antijuridicas que buscan afectar software's, soporte lógico o el almacenamiento de datos de un sistema, llevándose a cabo a través del internet y causando una afectación en el bien jurídico protegido, el cual trata de la información que se guarda dentro de dichos sistemas.

En ese hilo de ideas, y de manera conjunta, Laura Mayer Luz y Guillermo Oliver Calderón (2020), nos dicen que el delito del fraude informático trata; del acceso de un agente -de una forma clandestina/indebida- a datos contenidos en un sistema informático con el propósito de generar un daño en el patrimonio de terceros.

Por tanto, desglosando y dándole un concepto de delitos informáticos, tenemos que, dentro del derecho penal el concepto de delito es un concepto evolutivo y que estos delitos informáticos se realizan dentro del ciberespacio/internet.

1.3.2. Tipos De Fraude informático

Según ***Álvaro Castro de Control System Line Manager & Digital Champion de ABB en Perú*** a través de su artículo de "El Peruano" (2022), describe los siguientes.

- "*Phishing*: Básicamente es la suplantación de identidad de una persona natural o jurídica, la cual mediante correo electrónico o sitio web busca obtener información bancaria de las víctimas."
- "*Vishing*: Utilizando la vía telefónica se engaña al usuario a fin de obtener información personal sin que note que se trata de una estafa."
- "*Smishing*: Esta es una variante del phishing, en el cual mediante sistemas de mensajería instantánea y de los mensajes de texto (SMS) se busca sacar esta información bancaría de las personas."
- *Malware*, según nos dice ***Malwarebytes (2023)***, *"viene a ser un software malicioso que es utilizado para dañar, alterar o tomar el control de cualquier sistema informático, dejando al usuario sin conocimiento o consentimiento de esta acción. Esto acarrearía graves consecuencias como virus, gusanos, troyanos, spyware o adwares."*
- Por su lado, Camila Laval, de Abogado.com (2023), nos menciona el *Robo de Identidad.* "Este tipo de fraude se da cuando un ladrón experimentado obtiene tu número de Seguro Social, los números de cuenta de su tarjeta de crédito u

otros datos financieros que tengas. Siendo las formas más comunes del robo de identidad el: duplicado de tarjetas, la suplantación de páginas reales, el llenar formularios falsos, etc.”

1.3.1. Sims Cards

Según Alai Secure, filial del grupo Ingenium Tecnología, empresa especializada en la Seguridad Telco, una tarjeta SIM (Subscriber Identity Module, por sus siglas en inglés) viene a ser básicamente una tarjeta inteligente que se utiliza en teléfonos móviles y otros dispositivos móviles para poder almacenar cualquier tipo de información de un usuario, como su número de teléfono, contactos y configuraciones de red.

Ahora, la aclamada tarjeta SIM fue concebida desde el año 1968, de la mano de la compañía Giesecke+Devrient - SecurityTech, sin embargo, pasarían dos décadas para que en el año 1991 se comercializara, siendo desde entonces que se puede insertar en los dispositivos sirviendo más que todo para que los usuarios accedan a los servicios de telefonía móvil y así puedan mantenerse comunicados con otras personas.

Según RedesTelecom, Es así que, una tarjeta Sim tiene como principales características el que se inserta en dispositivos móviles para poder autentificar al usuario en la red de telefonía móvil y almacenar información como contactos y mensajes. Así como también es de tamaño compacto y puede ser reemplazado en caso de pérdida o daño.

Tipos de Sims Cards

Según ***Yubal Fernandez, de Xataka Basics (2019)*** existen 4 tipos de tarjeta Sim, los cuales son los siguientes:

- "*SIM (DESCONTINUADA): Este tipo de tarjetas, las originales, ya no se utilizan, debido a que eran de un tamaño parecido al de una tarjeta de crédito.*"
- "*MiniSIM: Es la que actualmente se usa en el mercado, pero no fue la primera en existir. Fue desarrollada más que todo para que entrara en los teléfonos móviles.*"
- "*MicroSIM: Para el 2003 se creó este nuevo tipo de tarjeta, siendo en la llegada del iPad que Apple hizo que toda la industria empezase a adoptarla.*"
- "*NanoSIM: Una fase posterior a las Micro SIM, consiguiéndose crear una tarjeta todavía más pequeña que la anterior. Y teniendo como misión el optimizar el espacio del hardware de un teléfono, manteniendo su tamaño externo, pero con mayor volumen para ciertos componentes.*"

1.4. Marco normativo

El marco normativo internacional es:

- ***El convenio Budapest sobre la ciberdelincuencia (2004),*** Establece leyes y protocolos penales uniformes en todos sus Estados que lo conforman es el objetivo del Convenio de Budapest, un pacto internacional para combatir la delincuencia organizada transnacional, incluida la ciberdelincuencia. Esto en un mecanismo y/o

esfuerzo de la comunidad internacional por fortalecer el Estado de Derecho en el ciberespacio.

En cuanto al marco normativo nacional, encontramos lo siguiente:

- ***Código penal de 1991***, señala el primer delito informático de nuestra nación, el robo telemático, se tipifica como delito contra el patrimonio en el artículo 186. Por tratarse de un delito cuyo bien jurídico protegido es el patrimonio, estableció la práctica nacional de clasificar los delitos informáticos como aquellos que inciden inherentemente en el patrimonio.
- ***La ley 27309***, promulgada de fecha 17 de julio del 2000, incluye las disposiciones del código penal 207-A (interferencia, acceso o copia indebida a una base de datos, sistema o red de ordenadores), 207-B (alteración, daño o destrucción de una base de datos (sabotaje informático) y 207-C (circunstancias agravantes).
- ***La ley 30076***, promulgada de fecha 19 de agosto del 2013, incorpora el artículo 207-D (Tráfico ilegal de datos) en el código penal.
- ***La ley 30096***, promulgada de fecha 19 de setiembre del 2013, regula los delitos relacionados con el uso inadecuado de equipos y programas informáticos, incluidos el fraude informático, el tráfico ilícito de datos y la interceptación de datos informáticos.
- ***La ley 30171***, promulgada de fecha 10 de marzo del 2014, tiene por objetivo el detener y penalizar las actividades ilegales que comprometen los datos y los sistemas informáticos.
- ***Código penal de 2004***, estipula la posesión ilegítima de SIMs Cards activados en el artículo 222 – B, refleja la regulación del uso de tecnología de comunicación,

buscando prevenir su uso en actividades ilícitas. Dentro del delito, el bien jurídico que se busca proteger la seguridad pública y el orden social son los intereses jurídicos que deben salvaguardarse, ya que pretenden impedir el uso de la tecnología de la comunicación para permitir acciones ilegales como la usurpación de identidad y la extorsión.

- ***La Ley 31839***, promulgada de fecha 18 de julio de 2023, estipula regulaciones sobre la comercialización y manejo de SIMs Cards en Perú, con un enfoque claro en la seguridad y la prevención del comercio ilegal. Asimismo, se busca fortalecer la regulación sobre el uso y comercialización de SIMs Cards para proteger a los consumidores y combatir el comercio ilegal, asegurando un mejor control sobre los servicios móviles en el país.
- ***El Texto Único Ordenado de las Condiciones de Uso de los Servicios Públicos de Telecomunicaciones – OSIPTEL***, tiene como objetivo combatir el uso ilegal de las SIM Cards y proteger la seguridad de los usuarios. Además, el Decreto Supremo N° 023-2014-MTC, mismo que entró en vigencia des del año 2012, hace obligatorio para todas las empresas que ofrecen sus servicios de telecomunicaciones, registrar a todo aquel que contrate sus servicios de telefonía móvil y no activar líneas antes de ser registrados los datos del abonado.

1.5. FORMULACIÓN DEL PROBLEMA

1.5.1. Pregunta general

1.5.1.1. ¿Cómo influye el comercio ilegal de tarjetas SIMS CARDS en la comisión de delitos de fraude informático, según los registros de la DIVINDAT durante el periodo 2019 - 2022?

1.5.2. Preguntas especificas

1.5.2.1. ¿Cómo contribuye el comercio ilegal de tarjetas SIM al fraude informático registrado en los informes de la DIVINDAT durante el periodo 2019-2022, en el contexto de las tecnologías de la información y telecomunicaciones?

1.5.2.2. ¿Qué impacto tienen las sanciones legales impuestas por el comercio ilegal de tarjetas SIM y el fraude informático registrado en la DIVINDAT, y cómo son percibidas por las autoridades y expertos en ciberseguridad?

1.6. Objetivos

El objetivo del estudio es examinar cómo afecta la venta ilícita de SIM CARDS para la Comisión del Delito de Fraude Informático, y los pensamientos aplicados a un grupo de efectivos que laboran en la División de Investigación de delitos de Alta Tecnología de la PNP para combatirlo.

De lo cual se espera que los resultados de este estudio aporten a la comprensión del delito de fraude informático y de qué manera influye el comercio ilegal de SIM CARDS en la comisión de este delito, ya que conocer la forma en que piensan los efectivos policiales permitiría una mejora continua de las estrategias a aplicarse.

1.6.1. Objetivo general

1.6.1.1. Analizar la influencia del comercio ilegal de tarjetas SIM en la comisión de delitos de fraude informático, según los registros de la DIVINDAT durante el periodo 2019-2022.

1.6.2. Objetivos específicos

1.6.2.1. Investigar cómo el comercio ilegal de tarjetas SIM contribuye a la comisión de fraude informático, según los informes registrados por la DIVINDAT entre 2019 y 2022, en el contexto de las tecnologías de la información y telecomunicaciones.

1.6.2.2. Analizar el impacto de las sanciones legales impuestas por el comercio ilegal de tarjetas SIM y el fraude informático registrado en la DIVINDAT, y examinar cómo son percibidas por las autoridades y expertos en ciberseguridad.

1.7. Supuestos de Hecho

La presente investigación no formulará hipótesis debido a que solo se limitará a describir los hallazgos de los estudios, debemos indicar que según Flick (2012), "los supuestos teóricos se vuelven relevantes como versiones preliminares de la manera de comprender el objeto que se estudia y la perspectiva sobre él, que se reformulan y sobre todo se elaboran más durante el proceso de investigación"

Es decir, los supuestos no son fijos, sino que se ajustan y refinan a medida que se recopilan y analizan los datos.

1.8. Justificación

1.8.1. Justificación teórica

De las estadísticas de Denuncias del año 2015 al 2021, que fueron brindadas por la Agencia Peruana de Noticias – ANDINA, mediante la cual se infiere que los delitos de fraude informático últimamente se han incrementado y que los ciberdelincuentes utilizan teléfonos con SIMS CARDS a nombre de terceros para enviar mensajes de texto con links y de esta manera obtener datos como: (i) número de tarjetas, (ii) claves de app móviles, (iii) número de token y otros datos que le permiten realizar transferencias electrónicas sin el consentimiento de la víctima. Los SIMS CARDS siempre se encuentran activados con nombres de personas que han sido suplantadas para así el ciberdelincuente ocultar su identidad y evitar su identificación durante las investigaciones policiales.

1.8.2. Justificación práctica

Al conocer el significado que le atribuyen los operadores policiales al fraude informático y al comercio ilegal de SIMs Cards, y cómo podría cambiar el panorama con un eventual aumento de la pena prevista en el artículo 222-B del Código Penal, esta investigación pretende brindar a los efectivos PNP de la DIVINDAT un mayor entendimiento sobre las conductas típicas del fraude informático. Ello contribuirá no solo a fortalecer la identificación y prevención de estos delitos, sino también a respaldar propuestas de reforma penal y operativa, que permitan enfrentar con mayor eficacia esta problemática en constante crecimiento.

1.8.3. Justificación metodológica

Podemos justificar la metodología, como metodología cualitativa para resolver la cuestión del fraude informático y el comercio ilícito de tarjetas SIM, basándonos en los párrafos anteriores. La base de este enfoque cualitativo será la recopilación y el examen de datos exhaustivos y descriptivos relativos a las prácticas habituales de fraude informático relacionadas con el uso de tarjetas SIM, así como las formas en que el comercio ilícito de tarjetas SIM afecta a la comisión de este delito.

La recolección de datos cualitativos se obtendrá mediante entrevistas con expertos en delitos informáticos, investigadores policiales y profesionales de la ***"División de Investigación de Delitos de Alta Tecnología".*** Gracias a estas entrevistas se podrá explorar en detalle las estrategias utilizadas por los ciberdelincuentes, los métodos de suplantación de identidad, las técnicas de envío de mensajes de texto con links, y además la obtención de datos confidenciales, así como las consecuencias que acarrea el usuario al dar estos datos, como las dificultades para la identificación de los responsables.

Los resultados de esta investigación buscan proporcionar una comprensión profunda de las conductas y estrategias que son utilizadas por los ciberdelincuentes en relación al uso de las SIMs Cards en el fraude informático. Permitiéndose así la presentación de alternativas de solución para abordar esta problemática, como el fortalecimiento de las medidas de seguridad en la venta y activación de las tarjetas SIM, la implementación de campañas de concientización y educación sobre el uso seguro de los dispositivos móviles, el establecimiento de mecanismos de colaboración entre las autoridades y las compañías telefónicas para detectar y prevenir el comercio ilegal de

SIM Cards, así como también la implementación drástica de la pena (Artículo 222-B).

CAPÍTULO II: METODOLOGÍA

2.1. El tipo de investigación

Dado que el estudio se centrará en cómo afecta la venta ilegal de tarjetas SIM al fraude informático, será de naturaleza teórica o empírica. A continuación, se pedirá a los miembros de la **DIVINDAT** que debatan sobre este tema. Según ***Vargas (2011)*** quien sostiene en su obra titulada "Cómo hacer investigación cualitativa. Una guía práctica para saber qué es la investigación en general y cómo hacerla, con énfasis en las etapas de la investigación cualitativa." que: "nombramos investigación teórico empírica a aquellos trabajos que encuentran primero la estructura empírica y categorial de alguna realidad concreta para luego ponerla a dialogar con distintos autores teóricos." En este contexto, el estudio se llevará a cabo en las instalaciones de la DIVINDAT en 2023 con el objetivo de determinar la importancia del delito de fraude informático derivado del comercio ilegal de SIMS CARDS para un grupo de personal de la PNP. El estudio también describirá los comportamientos típicos que componen el delito, y los resultados se compararán con diversas teorías relativas al concepto del delito mencionado.

2.2. Diseño de investigación

Debido a que esta investigación se desarrolla bajo la figura de un enfoque de investigación no experimental y longitudinal, se observa y examina el fenómeno del comercio ilegal de SIMS CARDS y su relación con el delito de fraude informático sin manipular variables, basándose en conclusiones o puntos de vistas propuestas (estudio de casos) por los miembros de la División de Investigación de Delitos de Alta Tecnología (DIVINDAT).

Según ***Lancheros Florián, L. (2012)*** en su obra "Métodos de Investigación no Experimental" señala que: "el estudio de casos es una investigación generalmente de tipo descriptivo que se lleva a cabo mediante el análisis de una única unidad muestral ya sea un sujeto, una persona o un individuo dentro de un grupo"

2.3. Enfoque de la investigación

Dado que el comercio ilícito de tarjetas SIM y su repercusión en la comisión de delitos de fraude informático son fenómenos complicados y variados que requieren **investigación**, por lo que correspondería utilizar la técnica de investigación cualitativa. Según ***Ruedas Marrero, M., Ríos Cabrera, M. M., & Nieves, F. (2009)*** en su obra "Hermenéutica: La roca que rompe el espejo" señalan que "la investigación cualitativa intenta desentrañar la naturaleza profunda de los fenómenos." Es por ello que este tipo de investigación nos permitirá conocer una realidad desde sus diversas complejidades e interrelaciones.

2.4. Población

Según ***Arias-Gómez, J., Villasís-Keever, M. Á., & Novales, M. G. M. (2016)*** en su obra "El protocolo de investigación III: la población de estudio" definen a la población como: ***"un conjunto de casos, definido, limitado y accesible, que formará el referente para la elección de la muestra, y que cumple con una serie de criterios predeterminados".*** Nuestra población de estudio serán los policías PNP que laboran en la ***"División De Delitos De Alta Tecnología"*** involucrados en el tema de los delitos informáticos, en especial al delito de fraude informático producto de la comercialización ilegal de SIMS CARDS.

2.5. Muestra

Según ***Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, P. (2018)*** en su obra "Metodología de la investigación" manifiestan que la muestra es: "un subconjunto de elementos que pertenecen a ese conjunto definido en sus características a las que llamamos población.". La investigación se realizará con seis (6) miembros pertenecientes a la **"División de Delitos de Alta Tecnología – DIVINDAT"**

2.6. Tipo de muestreo

2.6.1. Muestreo no probabilístico por conveniencia

Según **Salvadó, I. E. (2016)** en su obra "Tipos de muestreo. Investigación científica" describe al muestreo no probabilístico por conveniencia como: "la muestra que está disponible en el tiempo o periodo de investigación". Por lo tanto, en esta investigación se utilizará el muestreo de conveniencia, junto con la selección intencionada de funcionarios de la PNP encargados de perseguir el delito, planificar, desarrollar, llevar a cabo y evaluar planes

estratégicos para combatir el delito de fraude informático provocado por la comercialización ilegal de tarjetas SIMS, así como la documentación relacionada con el delito.

2.7. Técnicas e instrumentos de estudio, procedimiento de recolección de datos.

2.7.1. Técnicas

Será la entrevista, observación directa y análisis de respuestas. Según **Callejo Gallego, J. (2002)** en su obra "Observación, entrevista y grupo de discusión: el silencio de tres prácticas de investigación." explica a la entrevista como un diálogo típico con algunos elementos singulares, en el que el entrevistador sugiere temas y el entrevistado intenta dar respuestas adecuadas al contexto local.

2.7.2. Instrumentos de estudio

El presente trabajo de investigación se realizará a base de la Guía de entrevista y ficha de registro de datos a los expertos de la ***"División de Delitos de Alta Tecnología – DIVINDAT"***. Según **Troncoso-Pantoja, C., & Amaya-Placencia, A. (2017)** en su obra "Entrevista: guía práctica para la recolección de datos cualitativos en investigación de salud." Manifiesta que los instrumentos de estudio: "La guía de entrevista es un instrumento que permite al entrevistador tener un esquema de preguntas y temas a tratar durante la entrevista, mientras que la ficha de registro de datos es un documento que permite al entrevistador registrar la información obtenida durante la entrevista."

2.7.3. Procedimiento de recolección de datos

2.7.3.1. Acceso al campo

Se solicitó permiso al encargado de la ***"División de Delitos de Alta Tecnología – DIVINDAT"***, para realizar el trabajo de campo en el contexto del delito investigado realizaremos la examinación de documentos. Para llevar a cabo las entrevistas, se seleccionará a los informantes en función de sus conocimientos y experiencia en la gestión de la ciberdelincuencia. También se ubicará al encargado del archivo de atestados e informes policiales para que proporcione la documentación pertinente. 2.7.3.2. Recogida productiva de datos durante la entrevista que se les efectuará a los informantes (policías con conocimientos adecuados del delito de fraude informático y con experiencia la lucha contra ese delito), se buscará crear un clima de confianza a fin de obtener datos relevantes y que guardan relación con los objetivos de la investigación. De igual forma se tratará con el encargado de proporcionar los atestados e informes policiales.

2.7.3.2. Recogida productiva de datos

Durante la entrevista que se les efectuará a los informantes (policías con conocimientos adecuados del delito de fraude informático y con experiencia la lucha contra ese delito), se buscará crear un clima de confianza a fin de obtener datos relevantes y que tengan vínculo directo con los objetivos de la investigación. De igual forma se tratará con el encargado de proporcionar los atestados e informes policiales.

2.7.3.3. Reducción de datos

Los datos recolectados durante la entrevista efectuada a los efectivos PNP, así como del análisis de los atestados e informes policiales serán reducidos, seleccionando únicamente a los que se encuentran relacionados con los observables en este caso: el delito de fraude informático aplicadas por la **"División de Delitos de Alta Tecnología – DIVINDAT"**, desde la perspectiva de los significados de un grupo de efectivos policiales que labora en dicha unidad especializada y la descripción de los caracteres que configuran el delito de fraude informático desde una perspectiva proveniente de los informantes policías, a fin de categorizar y codificar la información obtenida.

2.7.3.4. Disposición y transformación de datos

Tras la reducción, los datos se organizarán para facilitar su examen y comprensión, lo que influirá en las decisiones que se tomen posteriormente tras el análisis pertinente.

2.7.3.5. Método de análisis de datos

Dado que el análisis parte de una problemática general, en este estudio se utilizó el método deductivo de análisis de datos, respecto del comercio ilegal de tarjetas SIM y su influencia en la comisión de delitos de fraude informático, según los registros de la DIVINDAT-2022. La investigación se desarrolló a través de la formulación de una propuesta basada en este problema, comparando los datos recopilados mediante la aplicación de diversas técnicas de recolección de datos.

La metodología deductiva nos permitió analizar detalladamente la relación entre estos elementos, partiendo de la información general y llegando a conclusiones específicas respaldadas por la evidencia recopilada durante el proceso de investigación.

2.7.3.6. Obtención de resultados y verificación de conclusiones

Los resultados se obtendrán después de contrastar los objetivos de la investigación con los datos encontrados en el escenario, en este caso la ***"División de Delitos de Alta Tecnología – DIVINDAT"***. La interpretación que se hará de los resultados estará apegada a la originalidad de los datos, descripciones y construcciones analíticas. Luego, se elaborará el informe final después de haber alcanzado una mayor comprensión del delito de fraude informático y comprender la influencia que tiene la comercialización ilegal de SIMS CARDS en estos delitos.

2.8. Principios éticos

En este trabajo de tesis se aplicarán los siguientes principios éticos:

2.8.1. Principio de justicia

Según ***Hoyos, J. G. O. (2000)*** en su obra "Principios éticos de la investigación en seres humanos y en animales" describe lo siguiente: "la justicia se realiza no sólo en la comprensión y reconocimiento de los principios sino en la búsqueda efectiva de las consecuencias buenas de todo el actuar investigativo" En el contexto de un trabajo de fraude informático, el principio de justicia se aplicará bajo la obligación de tratar a todas las partes involucradas de manera equitativa y respetar sus derechos. Además, el trabajo de investigación tiene un propósito legal claro puesto que tiene conformidad con las leyes y regulaciones aplicables para el beneficio de la sociedad.

2.8.2. Principio de beneficencia

Según **Hoyos, J. G. O. (2000)** en su obra "Principios éticos de la investigación en seres humanos y en animales" describe lo siguiente: "el principio de beneficencia se trata del deber ético de buscar el bien para las personas participantes en una investigación, con el fin de lograr los máximos beneficios y reducir al mínimo los riesgos de los cuales deriven posibles daños o lesiones. Es decir, que los riesgos sean razonables frente a los beneficios previstos, que el diseño tenga validez científica y que los investigadores sean competentes integralmente para realizar el estudio y sean promotores del bienestar de las personas." Con respecto al principio de beneficencia se aplicaría en la obligación de maximizar el beneficio para las personas afectadas y minimizar el daño causado por el fraude informático.

2.8.3. Principio de responsabilidad

Según **Polo Santillán, M. Á. (2019)** en su obra "La responsabilidad ética" nos dice que: "Esta responsabilidad ética surge de nuestro mero hecho de existir y ser conscientes del mundo en el que vivimos." Cabe resaltar que el principio de responsabilidad se aplicaría en la obligación de asumir la responsabilidad de las consecuencias de la investigación y de las acciones tomadas para resolver el tema de fraude informático producto de la comercialización ilegal de SIMs Cards.

CAPÍTULO III: RESULTADOS

En este capítulo se presentan los resultados de la recogida de datos mediante las pautas de entrevista, que se realizó con el consentimiento de los expertos y con el de la muestra de expertos de la **"División de Delitos de Alta Tecnología – DIVINDAT"**. El objetivo de esta investigación es determinar en como la comercialización ilegal de SIMS CARDS influye en la comisión de delitos de fraude informático y como deberían reforzarse la normativa aplicable al caso.

Tabla 1: Pregunta general realizada en la entrevista N° 01, ello en base al Objetivo General, mismo que trata de analizar la relación entre el comercio ilegal de SIM CARDS y el aumento en la incidencia de delitos de fraude informático.

PREGUNTA	RESPUESTA DE LOS MIEMBROS DE LA DIVINDAT
¿Cómo influye el comercio ilegal de tarjetas SIMS CARDS en la comisión de delitos de fraude informático, según los registros de la DIVINDAT durante el periodo 2019-2022?	**Edward Iván Scott Arenaza CI: OA-272162:** Desde mi óptica, como experto en la PNP especializado en tecnología, el fraude informático vinculado al comercio ilegal de SIMs Cards puede causar daños financieros significativos a las víctimas, ya que los delincuentes pueden acceder a cuentas bancarias mediante suplantación de identidad con datos obtenidos de SIMS Cards robadas, realizando transacciones no autorizadas. Detectarlo y perseguirlo es una labor compleja debido a su naturaleza digital y la participación de actores dispersos

	geográficamente. La investigación precisa y la colaboración interdisciplinaria son fundamentales para abordar estos delitos de manera efectiva y proteger la seguridad y bienestar de la población.
	Roberto Manuel Rouillon Bermudez **CI: OP-344625:** El comercio ilegal de sims cards influye demasiado en la comisión de estos delitos. Este comercio puede ocasionar mucha desconfianza sobre la verificación de operadoras de telecomunicación, pues permitirían que grupos criminales aprovechen de sus vulnerabilidades, por lo que resulta crucial que las compañías de telecomunicaciones adopten medidas de seguridad efectivas para prevenir la comercialización ilícita de tarjetas SIM. Esto implica establecer sistemas de autenticación más rigurosos y colaborar con las fuerzas del orden en la identificación y persecución de los infractores.
	Rosa Clara Tuesta Estela **CI: SA-31529756:** El comercio ilegal de tarjetas SIMs CARDs puede permitir que los delincuentes cibernéticos lleven a cabo una activación masiva de dichas tarjetas con

	documentación falsa, y a la fecha del 2022, OSIPTEL responsabiliza al menos un 68% a este tipo de fraudes. Por lo que fundamental que la población esté al tanto de los peligros asociados con la venta ilegal de tarjetas SIM y de las acciones preventivas que pueden llevar a cabo para no caer en esta actividad delictiva. Haciendo algo tan fácil como activación de seguridad en sus dispositivos móviles hasta verificar la legitimidad de los vendedores antes de efectuar una adquisición.
	Andrea Estaurofela Rodriguez Flores **CI: CIP 31478012:** El incremento de este Fraude Informático permite que los delincuentes digitales puedan activar líneas telefónicas con identidades falsas o robadas, haciendo con esa acción que se les pueda mandar códigos de verificación bancaria de estas personas a las que suplantan, realizando con eso transferencias fraudulentas.
	Julio Enrique Farfan Chiun **CI: OS-368123:** A mi criterio, el delito de fraude informático producto del comercio ilegal de SIM CARDS es un delito que puede tener graves consecuencias para las víctimas, ya que puede generar un perjuicio patrimonial importante ya que este delito puede ser difícil de detectar y

	perseguir, ya que se lleva a cabo utilizando medios informáticos y puede involucrar a personas de diferentes lugares del mundo, no solo del Perú.
	Angel Leonardo Leyva Cabello **CI: SA-31081930:** El delito de fraude informático producto del comercio ilegal de SIM CARDS puede tener un impacto negativo en la economía y la seguridad del país, ya que puede afectar la confianza de los ciudadanos en los sistemas financieros y de telecomunicaciones.

INTERPRETACION: *En base a la pregunta realizada en los entrevistados E.I.S.A., A.E.R.F. y J.E.F.C., podemos destacar que el fraude informático relacionado con el comercio ilegal de SIM CARDS es un delito grave que puede causar daños financieros significativos a las víctimas. Detectarlo y perseguirlo puede ser complejo debido a su naturaleza digital y la participación de actores dispersos geográficamente. No obstante, también se enfatiza la importancia de la investigación precisa y la colaboración interdisciplinaria para abordar estos delitos de manera efectiva y proteger la seguridad y bienestar de la población. Además, es crucial que las compañías de telecomunicaciones adopten medidas de seguridad efectivas para prevenir la comercialización ilícita de tarjetas SIM y que la población esté al tanto de los peligros asociados con la venta ilegal de tarjetas SIM y de las acciones preventivas que pueden llevar a cabo para no caer en esta actividad delictiva.*

Tabla N° 02 – Pregunta específica realizada en la entrevista N° 02, ello en base al Objetivo Específico, mismo que trata de vincular la comercialización ilegal de Sims Cards con el delito de fraude informático según la percepción y experiencia de los efectivos policiales en la división de investigación de delitos de alta tecnología.

PREGUNTA	RESPUESTA DE LOS MIEMBROS DE LA DIVINDAT
¿Cómo contribuye el comercio ilegal de tarjetas SIM al fraude informático registrado en los informes de la DIVINDAT durante el periodo 2019-2022, en el contexto de las tecnologías	**Edward Iván Scott Arenaza CI: OA-272162:** Esto no solo perjudica económicamente a las víctimas, también perjudica la confianza con los servicios digitales y financieros ya que los delincuentes digitales suelen manipular los datos personales para activar estas tarjetas de manera ilegal, lo que genera una afectación digital al país entero.

de la información y telecomunicaciones?	**Roberto Manuel Rouillon Bermudez** **CI: OP-344625:** Contribuye que de manera ilícita se realice la utilización de medios informáticos o telemáticos para obtener un beneficio económico ilícito, causando daño o perjuicio a la víctima. Ejemplos: -Uso de malware para robar información personal o financiera de las víctimas, séase tarjetas SIMS, laptops, etc. -Suplantación de identidad para realizar transacciones fraudulentas. -Robo de contraseñas para acceder a cuentas bancarias o de comercio electrónico.
	Rosa Clara Tuesta Estela **CI: SA-31529756:** El fraude informático considero que es algo clave porque le permite al delincuente llevar a cabo la suplantación de identidad desde el anonimato y permitiéndose la usurpación identidades para cometer fraudes; para que se realice eso se necesita de una tarjeta sim a nombre de otra persona.
	Andrea Estaurofela Rodriguez Flores **CI: CIP 31478012:** Esto contribuye de manera negativa a una cadena delictiva donde la suplantación de identidad

	hace que los delincuentes puedan evadir medidas de seguridad como autentificación de dos pasos, Esto presentado de diferentes formas (mensajes de texto, imágenes, audios, entre otras cosas). Un celular robado que porta una tarjeta sim es un medio por el cual, yo como delincuente, cometería mis delitos.
	Julio Enrique Farfan Chiun CI: OS-368123: Creo que contribuye a modalidades de fraude como el phishing y el robo de identidad. Ya que una vez el delincuente controla el número telefónico de la víctima, este puede interceptar comunicaciones y obtener información bancaria, lo que en consecuencia genera un aumento de fraudes complejos.
	Angel Leonardo Leyva Cabello **CI: SA-31081930:** Desde que empezó el tema de la pandemia, el incremento de delitos de fraude informático contribuyó en base a celulares robados que en la mayoría de casos no son reportado como robados.

INTERPRETACION: *De modo breve, podemos decir que los expertos A.L.L.C., J.E.F.C., E.I.S.A. nos explican que el delito de fraude informático ha contribuido de manera negativa al país, pues, estos delitos, al cometerse mediante el uso de medios tecnológicos para obtener un beneficio económico ilícito, causa en el proceso, un daño o perjuicio a la víctima, actuando como un catalizador para diversas modalidades del fraude informatico, permitiendo que los delincuentes en la mayoría de los casos tomen el control de números telefónicos legítimos, así como datos personales de las víctimas, lo que abre las puertas que se vulnere sistemas de autentificación, interceptan códigos de seguridad y con ello acceder a información financiera personal sensible.*

Tabla N° 03 – Pregunta específica realizada en la entrevista N° 02, ello en base al Objetivo Específico, mismo que trata de describir la viabilidad y la necesidad de implementar una sensación penal más drástica para las personas o entidades que comercializan ilegalmente tarjetas SIM,

PREGUNTA	RESPUESTA DE LOS MIEMBROS DE LA DIVINDAT
¿Qué impacto tienen las sanciones legales impuestas por el comercio ilegal de tarjetas SIM y el fraude informático registrado en la DIVINDAT, y cómo son percibidas por las autoridades y expertos en ciberseguridad?	**Edward Iván Scott Arenaza** **CI: OA-272162:** Soy de la idea de que las penas podrían tener un efecto disuasivo para los delincuentes. Este tipo de delitos (Comercio ilegal de SIMs Cards), es un problema social que permite cometer muchos delitos, entonces para mí, el endurecimiento de las penas podría contribuir a frenar y reducir casos de fraude informático.
	Roberto Manuel Rouillon Bermudez **CI: OP-344625:** Los delitos informáticos se han vuelto cada vez más organizados, lo que al menos para mí justifica la necesidad de que se frene la comercialización de tarjetas SIMs. El aumento de la pena sería un paso a que el Ministerio Público pueda requerir prisión preventiva y otras medidas coercitivas efectivas que permitan entender a los delincuentes que el comercio ilegal de SIMs Cards no es un juego.

	Rosa Clara Tuesta Estela **CI: SA-31529756:** La sanción actual de 4 años es muy poca, al ser muy garantista este artículo del código penal permite que los delincuentes continúen cometiendo fraudes por medio de las SIMs Cards producto de un comercio ilegal, sin un temor a las reales consecuencias. Creo que el aumento y endurecimiento de las sanciones sería lo mejor para mitigar este tipo de delitos.
	Andrea Estaurofela Rodriguez Flores **CI: CIP 31478012:** Es primordial que la pena se ajuste a la magnitud del daño ocasionado, ya que hoy en día se sigue comercialización tarjetas SIMS para cometer fraude informático que afectan a gran cantidad de personas y empresas.
	Julio Enrique Farfan Chiun **CI: OS-368123:** Desde una perspectiva de protección a la sociedad, el endurecimiento de la pena en caso de comercialización de tarjetas SIMs puede ser crucial. El estado tiene la responsabilidad de proteger a los ciudadanos, y nosotros como miembros de la DIVINDAT de parar estos delitos que afectan a la población.
	Angel Leonardo Leyva Cabello

	CI: SA-31081930: El aumento de la pena al artículo 222-B para el comercio ilegal de SIMs Cards es fundamental para enfrentar el crecimiento de este tipo de actividades ilícitas. Este delito no solo afecta la seguridad individual de la ciudadanía, sino que también facilita otros crímenes como el fraude, el robo de identidad entre otras cosas. Dado que las SIM Cards son utilizadas en muchos casos para facilitar actividades ilícitas sin que se pueda rastrear fácilmente a los responsables.

INTERPRETACION: *En base a la pregunta, podemos destacar que cada uno de los miembros de la División de Delitos de Alta Tecnología, están a favor de que se aumente la pena al artículo 222-B, toda vez que es necesario frenar los delitos de fraude informático ya que no se habla de un solo individuo sino también de organizaciones criminales. Es por ello que las autoridades mencionan que la sanción actual es muy garantista y permiten así la continuidad de los delitos informáticos, en base a la realidad peruana es que debe existir un endurecimiento de la pena ya que el fin primordial del Estado es proteger a la sociedad por medio de la seguridad pública.*

UPN UNIVERSIDAD PRIVADA DEL NORTE

CAPÍTULO IV: DISCUSIONES Y CONCLUSIONES

4.1. DISCUSIONES

- Según el objetivo principal, dado que el analizar la relación e influencia entre el comercio ilegal de SIM CARDS y como permite el aumento en la incidencia de delitos de fraude informático, a través del cómo se afecta las operaciones y estrategias de investigación de los efectivos de la PNP en la **"División de Delitos de Alta Tecnología – DIVINDAT"**, tenemos de los resultados recabados en la Tabla N°01 qué, el fraude informático constituye un delito de alto impacto, capaz de ocasionar graves perjuicios económicos a las víctimas. Detectar y sancionar este tipo de delitos representa un gran desafío para las autoridades, debido a su naturaleza digital, el anonimato que permite el uso de chips no registrados y la participación de individuos ubicados en distintas zonas geográficas. La investigación precisa y la colaboración interdisciplinaria son fundamentales para abordar estos delitos de manera efectiva y proteger la seguridad y bienestar de la población, toda vez que se deben adoptar medidas de control más estrictas para evitar la distribución de chips fuera del marco legal, así como en la necesidad de sensibilizar a la población sobre los riesgos asociados al uso de SIM CARDS adquiridas en el mercado informal y las acciones preventivas que pueden tomar para no verse involucrados en actividades delictivas.

Datos que se acoplan perfectamente con lo que ***Campos, N. J. O. (2019)*** dice en su investigación sobre "Normativa Legal Sobre Delitos Informáticos en Ecuador", investigación que enfatiza la necesidad de tomar medidas para abordar los delitos informáticos, mejorar la seguridad cibernética en empresas y promover la cooperación internacional para combatir estos delitos en un entorno cada vez más interconectado. Con estos resultados se afirma que

el fraude informático relacionado con SIM CARDS es un problema grave que requiere esfuerzos tanto a nivel local como internacional para su detección, prevención y persecución eficaz. Las recomendaciones coinciden con la necesidad de fortalecer la seguridad cibernética y promover la cooperación global en la lucha contra los delitos informáticos.

Además, la defensa de la ética en la seguridad informática es esencial para salvaguardar la seguridad y los derechos de las personas. Según el autor Rafael Capurro, la ética en la seguridad informática incluye la necesidad de salvaguardar la intimidad y los derechos humanos de las personas, así como la necesidad de cooperar para resolver problemas que repercuten en la sociedad en general. Las empresas y las personas deben tomar precauciones contra el fraude informático y otros delitos informáticos, y los gobiernos deben cooperar para resolver estos problemas tanto a nivel nacional como mundial.

- Según el primer objetivo específico, investigar las conductas típicas del fraude informático según la percepción y experiencia de los efectivos policiales que laboran en la DIVINDAT. Los resultados obtenidos en esta segunda tabla mencionan qué, los efectivos policiales entrevistados coinciden en que muchas de estas actividades delictivas se apoyan el uso de medios informáticos obtenidas de manera ilegal para obtener ganancias ilícitas y dañar a la víctima, las cuales permiten ocultar la identidad de los infractores y dificultar su rastreo. Entre las conductas más comunes asociadas al fraude informático se encuentran la suplantación de identidad, el robo de contraseñas, el fraude bancario, la propagación de malware y la manipulación de datos a través de dispositivos móviles. Estas prácticas vulneran directamente la privacidad y los derechos de los ciudadanos. Se recomienda el uso de contraseñas seguras y únicas, así como fortalecer la seguridad cibernética y promover la cooperación global para combatir estos delitos. Datos que se comparan con lo expuesto por

Robles Sotomayor, F. M. (2018) en su investigación titulada "La protección de datos personales como medio de prevención de los delitos informáticos en el Perú, en los años 2017 y 2018 texto que llega a la conclusión de que la comercialización ilícita de tarjetas SIM, que se utilizan en fraudes informáticos, pone en peligro la información personal de las personas. Esto pone de relieve lo crucial que es preservar esta información y las leyes que existen para detener los delitos informáticos. Además de eso, se tiene en claro que el fraude informático involucra el uso de sistemas informáticos para obtener ganancias ilícitas y causar daño a la víctima. Ejemplos de conductas típicas incluyen la suplantación de identidad y el robo de contraseñas. Fortalecer la seguridad cibernética y promover la cooperación global son esenciales en la lucha contra estos delitos. Robles Sotomayor afirma que la venta ilegal de tarjetas SIM utilizadas en fraudes informáticos pone en peligro la privacidad de las personas, haciendo hincapié en la necesidad de salvaguardar la información personal y promulgar leyes firmes para poner fin a estos delitos. La ética de la seguridad informática implica la necesidad de defender la intimidad y los derechos humanos, lo que hace necesaria la cooperación para resolver los problemas que afectan a la sociedad en general.

- Según el segundo objetivo específico, este busca describir la viabilidad y la necesidad de implementar una sensación penal más drástica para las personas o entidades que comercializan ilegalmente tarjetas SIM, ya que la mayoría de casos de fraude informático se realiza gracias a la comercialización ilegal de las mismas. Es así qué, los resultados obtenidos en la tercera tabla expresan qué, el comercio ilegal de tarjetas SIM CARDS en Perú está en aumento y está vinculado a delitos informáticos como el fraude de identidad y el robo de datos. "La División de Delitos de Alta Tecnología – DIVINDAT", de la PNP recomienda tomar medidas más drásticas que permitan hacerle frente al fraude informático producto de

la comercialización de tarjetas SIMS, asimismo, solicitan la concienciación pública y la cooperación internacional (Convenio de Budapest), para abordar este problema y prevenir el fraude informático. La ética en la seguridad informática destaca la responsabilidad de proteger los derechos humanos y la privacidad, enfatizando la necesidad de colaborar en la resolución de problemas que afectan a la sociedad en su conjunto, en la presente investigación sería la de hacerle frente y reducir el comercio ilegal de SIMS CARDS para la comisión de delitos de fraude informático.

Datos que se asemejan a lo expuesto por **Huamán Cruz, M. Y. (2020)** en su investigación sobre “Los delitos informáticos en Perú y la suscripción del Convenio de Budapest”, misma que concluye que la suscripción al convenio de Budapest se considera una medida que ha permitido a Perú combatir los delitos informáticos, incluyendo el fraude informático relacionado con la comercialización ilegal de SIM CARDS.

El texto resalta la importancia de la cooperación internacional y el desarrollo legislativo en la lucha contra estos delitos. Y, además, se establece que el comercio ilegal de tarjetas SIM CARDS en Perú está en aumento y está vinculado a delitos informáticos como el fraude de identidad y el robo de datos. La ética en la seguridad informática destaca la responsabilidad de proteger los derechos humanos y la privacidad, enfatizando la necesidad de colaborar en la resolución de problemas que afectan a la sociedad en su conjunto. En este sentido, el autor **Renzo Vinelli Vereau (2021)** en su artículo "Los delitos informáticos y su relación con la criminalidad económica " destaca la importancia de la ética en la seguridad informática y la necesidad de proteger los derechos humanos y la privacidad en el contexto de los delitos informáticos. El autor señala que la ética en la seguridad informática debe ser un componente clave en la lucha contra los delitos informáticos, y que los profesionales de la seguridad

informática deben ser conscientes de su responsabilidad ética en la protección de los derechos humanos y la privacidad.

4.2. LIMITACIONES

La DIVINDAT ha demostrado ser una entidad crucial para contrarrestar la criminalidad digital; sin embargo, se identifican limitaciones específicas que requieren atención legislativa. En particular, la normativa actual presenta desafíos en términos de alcance internacional, especialmente en la persecución y prevención de delitos cometidos desde y hacia otros países. Es crucial abordar estas deficiencias legales para garantizar una respuesta efectiva y coordinada a nivel global.

Además, el fenómeno del comercio ilegal de tarjetas SIM agrega una capa adicional de complejidad a la labor de las autoridades. La adaptación de la normativa legal debe contemplar estrategias que permitan abordar este tipo de actividades ilícitas como se debe, considerando la evolución constante de las tecnologías y tácticas utilizadas por los ciberdelincuentes. La colaboración internacional también se vuelve esencial para enfrentar eficazmente este problema transfronterizo.

Por último, debemos de indicar que, para poder mitigar estas limitaciones, el proyecto podría considerar la posibilidad de ampliar su alcance para incluir otros factores que influyen en el fraude informático, como el aumento en la seguridad de las redes informáticas y la educación cibernética. Además, se podría buscar colaboración con expertos en legislación nacional para abordar el aumento de la pena para toda persona que lleve a cabo este delito a nivel nacional y así las autoridades puedan ejercer todo el peso de la ley para brindar la seguridad pública que tanto se busca.

4.3. IMPLICANCIAS

Para comenzar, debemos dejar en claro que la presente investigación tiene relevancia teórica, siendo uno de los pocos abordajes que se dan al estudio de métodos cualitativos para el cálculo del índice del Comercio ilegal de Sims Cards y su Influencia en la comisión de Delito de Fraude Informático registrados en la Divindat durante el año 2022, teniendo un gran potencial para mejorar la comprensión de los delitos de fraude informático e incluso informar las políticas de seguridad y contribuir al aumento de la pena para hacerle frente a la comercialización de SIMS CARDS y así se vea reflejado un aminoramiento de casos de fraude informático producto del comercio ilegal.

En sus locales se encuentra la DIVINDAT, un equipo encargado de examinar el índice de vulnerabilidad de los ciberataques y fraudes informáticos en curso. Su objetivo es mejorar la seguridad pública mediante la prevención, la lucha, la investigación y la denuncia de los delitos informáticos, así como de los delitos que utilizan las tecnologías de la información y la comunicación, todo ello bajo la supervisión jurídica del fiscal.

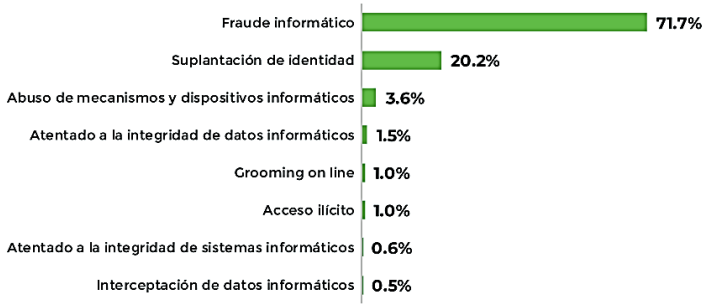
Esta investigación tiene relevancia social, ya que, a lo largo de los años, tanto en el mundo, como en nuestro país de origen, fuimos testigos de los fraudes informáticos, mismos que afectan a un gran número de personas, empresas e instituciones, generando pérdidas económicas y daños a la privacidad. La relación entre el fraude informático y el comercio ilícito de tarjetas SIM revela un fallo en la seguridad de las comunicaciones que podría repercutir en toda la sociedad. Además, estos delitos tendrían una influencia negativa sustancial en la confianza pública en las transacciones electrónicas y en la seguridad de la

información personal, lo que pone de relieve lo crucial que es que la sociedad aborde esta cuestión y la trate adecuadamente con arreglo a la ley.

4.3. CONCLUSIONES

- Respecto del análisis realizado dentro de la presente investigación, tenemos que decir que el comercio ilegal de Sims Cards es un problema relevante en la comisión de delitos de fraude informático en Perú. En razón a que desde el año 2015 hubo un incrementó de denuncias por delitos informáticos en el Perú lo cual evidencia que el fraude informático y la suplantación de identidad se han convertido en amenazas significativas, teniendo un gran incremento dentro de los años de pandemia, no solo para los ciudadanos, sino también para el propio gobierno. La información proporcionada por la Defensoría del Pueblo y la DIVINDAT [ESTADISTICAS] confirma que los servicios y prestaciones estatales son frecuentemente utilizados con fines fraudulentos, lo que resalta la urgente necesidad de incrementar las medidas de ciberseguridad y protección de los datos en el sector público peruano.

Gráfico N° 8
Tipos de ciberdelitos denunciados ante la PNP
(Perú, 2021)



Fuente: Sistema de Registro de Denuncias de Investigación Criminal PNP
Elaboración: Defensoría del Pueblo

- Respecto de los delincuentes informáticos de quienes basamos esta investigación tenemos que se tratan en su mayoría de hombres que rondan edades entre 15 y 40 años, con habilidades

en sistemas informáticos. Ocupando puestos estratégicos donde tienen acceso a información personal debido a sus trabajos o incluso por sus conocimientos en el área informática. Así mismo, las motivaciones de estos delincuentes en el Perú, en su mayoría, son para obtener un beneficio personal, o inclusive por el mero hecho de querer vengarse.

- Asimismo, este del análisis de la presente investigación, concluimos que esta problemática puede acarrear problemas tales como la desconfianza de la gran mayoría de los ciudadanos en el gobierno y sus empresas por la violación de su seguridad informática, siendo estos dos, grandes pilares que generarían una gran afectación y perdida de verse atacados de manera informática, visión que compartimos con la del analista de datos y desarrollador de Software, Dominic Ligot, respecto de los problemas que pueden generar este tipo de delitos.

- Como bien sabemos, en la era digital, el fraude informático se ha convertido en una preocupación creciente alrededor del mundo, y Perú no se queda fuera. Ser víctima de fraude informático puede tener consecuencias financieras y personales significativas. Por ello, en base a artículos informáticos expedidos por MAPFRE e INDECOPI, si te encuentras en situación de víctima por fraude informático en Perú, es fundamental tomar medidas inmediatas para proteger tus intereses y minimizar los daños

- Es crucial tener a mano pruebas que puedan corroborar el hecho de que algo ocurrió, como correos electrónicos, capturas de pantalla, grabaciones de audio o vídeo, etc. Además, un notario público puede, si es necesario, crear un registro de la pantalla del ordenador u otro componente electrónico que muestre la acción que condujo al fraude reclamado.

- Llevar a cabo una denuncia inmediata, un delito informático puede ser denunciado en cualquier comisaría del país, así como de manera directa en la División de Investigación de Delitos de Alta Tecnología al número 942 440 729 o a su mismo correo *divindat.servicioguardia@policia.gob.pe*.
- Ir a Indecopi, en caso se vea involucrada publicidad engañosa, usted podrá presentar un reclamo ante el Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (Indecopi)
- Podemos decir que las SIM CARDS cumplen funciones esenciales para la autenticación e identificación de cualquier usuario, incluyéndose su autenticidad en la red, así como el almacenamiento de información personal, gestión de contactos y mensajes, la gestión de la conectividad móvil, protección de información personal y la personalización de los servicios ofrecidos por los operadores de telecomunicaciones.

- Asimismo, la importancia de la SIMS CARDS en la autenticación de la identidad del usuario es la de brindar una protección a la identidad del usuario, ya que esta tarjeta SIM almacena de forma segura todas las claves de portales bancarios o a fines, lo que garantiza la protección del usuario móvil ya que la combinación del número de teléfono móvil y el identificador de la tarjeta SIM (IMSI) es difícil de falsificar, lo que brinda una autenticación más segura.

- Algunos gobiernos implementaron el registro obligatorio de las tarjetas SIM prepagas para poder combatir el uso ilegal de las mismas tarjetas y así proteger la seguridad de los usuarios y que las redes de los operadores que brindan estas tarjetas SIM, pueden identificar a un

usuario específico mediante esta tarjeta, lo que permite ofrecerles los servicios correspondientes.

- Y para ir concluyendo, tenemos que, lo más probable que suceda es que las tarjetas SIM físicas desaparezcan en un futuro, ya que hoy en día, los fabricantes de teléfonos móviles están eliminando gradualmente las bandejas de tarjetas SIM en cada uno de sus dispositivos. Dando pase agigantados a los cambios en la industria, siendo estos la aparición y transición a lo que es la tecnología eSIM, misma que no requiere tener un formato físico para funcionar y que, por ende, podría cambiar la forma en que los operadores de telecomunicaciones ofrecen sus servicios, así como también el cómo los usuarios eligen y cambian de operador, y además, esto podría reducir en grandes números los fraudes informáticos al ser un método más seguro.

- Esta investigación puede ser utilizado como referencia para futuras investigaciones sobre delitos informáticos y el comercio ilegal de SIMs Cards en Perú y en otros contextos. La metodología utilizada en este estudio puede ser adaptada y mejorada para abordar otros problemas relacionados con la seguridad digital y la prevención de delitos informáticos. También necesario considerar los factores sociales, económicos y tecnológicos que influyen en la comisión de estos delitos, así como las perspectivas y experiencias de los actores involucrados en su prevención y control.

REFERENCIAS

- Pons Gamón, V. (2017). Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad. Recuperado de: https://acortar.link/szBCME
- Andina: (Consultado el 11 de junio del 2022). Recuperado de: http://surl.li/hxooa
- El Peruano: (Consultado el 11 de junio 2022). Recuperado de: http://surl.li/hxong
- Oas.org. Recuperado el 11 de junio de 2023, de https://www.oas.org/juridico/english/cyb_pry_convenio.pdf
- Macías-Lara, RA., Boné Andrade, MF., Quiñonez Angulo, F., Mendoza Loor, JJ, Estupiñan-Troya, G., & Rodríguez Vizuete, JD . (2022) Recuperado de: https://acortar.link/BDPIkb
- Acosta, M. G., Benavides, M. M., & García, N. P. (2020). Delitos informáticos: Impunidad organizacional y su complejidad en el mundo de los negocios. *Revista venezolana de gerencia*, *25*(89), 351-368. Recuperado de: https://acortar.link/xHmNsj
- Campos, N. J. O. (2019). Normativa Legal sobre Delitos Informáticos en Ecuador. *Revista Científica Hallazgos21*, *4*(1), 100-111. Recuperado de: https://dialnet.unirioja.es/servlet/articulo?codigo=7148227
- Vilca Aira, G. L. (2018). Los hackers delito informático frente al código penal peruano. Recuperado de: https://web.archive.org/web/20200530095959/https://repositorio.unasam.edu.pe/handle/UNASAM/2496
- Huamán Cruz, M. Y. (2020). Los delitos informáticos en Perú y la suscripción del Convenio de Budapest. Recuperado de: https://repositorio.uandina.edu.pe/handle/20.500.12557/4116
- Vasquez Villacorta, Renzo Jesus. El procesamiento penal de la persona jurídica involucrada en la comisión de delitos informáticos en el Perú, 2022. Recuperado de: https://acortar.link/gJXAxX
- Robles Sotomayor, F. M. (2018). La protección de datos personales como medio de prevención de los delitos informáticos en el Perú, en los años 2017 y 2018. Recuperado de: https://repositorio.uap.edu.pe/handle/20.500.12990/8889
- MAYER LUX, L., (2017). EL BIEN JURÍDICO PROTEGIDO EN LOS DELITOS INFORMÁTICOS. Revista Chilena de Derecho, 44(1), 235-260 recuperado de: https://www.redalyc.org/articulo.oa?id=177051304011
- Mayer Lux, Laura, & Oliver Calderón, Guillermo. (2020). El delito de fraude informático: concepto y delimitación. *Revista chilena de derecho y tecnología*, *9*(1), 151-184. Recuperado de: https://acortar.link/GGUziI

- Según Álvaro Castro de Control System Line Manager & Digital Champion de ABB en Perú – El diario El Peruano (2022). Recuperado de: https://elperuano.pe/noticia/174955-cuide-sus-
- MalwareByte: (Consultado el 24 de Julio del 2023). Recuperado de: https://shorturl.at/ghn57
- Abogado.Com (Consultado el 24 de Julio del 2023). Recuperado de: https://shorturl.at/hlptJ
- Según Alai Secure, filial del grupo Ingenium Tecnología, empresa especializada en la Seguridad Telco. Recuperado de:
- https://alaisecure.co/blog/tarjetas-sim-para-alarmas-caracteristicas-y-ventajas/
- Xataca Basics: (Consultado el 24 de Julio del 2023). Recuperado de: https://www.xataka.com/basics/tarjeta-sim-como-funciona-como-saber-que-tipo-tuya
- Flick, U. (2012). Introducción a la investigación cualitativa. Madrid, España: Ediciones Morata. Recuperado de: https://investigaliacr.com/investigacion/la-teoria-en-la-investigacion-cualitativa/
- De las estadísticas de Denuncias del año 2015 al 2021, que fueron brindadas por la Agencia Peruana de Noticias – ANDINA. Recuperado de: https://andina.pe/agencia/noticia-cuidado-los-fraudes-informaticos-estas-son-las-modalidades-mas-denunciadas-peru-928425.aspx
- Vargas B (2011) ¿Cómo hacer investigación cualitativa? Recuperado de https://www.paginaspersonales.unam.mx/files/981/94805617-Xavier-Vargas-B-COMO-HACER-INVESTIGA.pdf
- Lancheros Florián, L. (2012). Métodos de Investigación no Experimental. 2012. Disponible en: https://repositorio.konradlorenz.edu.co/handle/001/5296
- Ruedas Marrero, M., Ríos Cabrera, M. M., & Nieves, F. (2009). Hermenéutica: la roca que rompe el espejo. Investigación y Postgrado, 24(2), 181-201. Recuperado de: https://www.redalyc.org/articulo.oa?id=65817287009
- Arias-Gómez, J., Villasís-Keever, M. Á., & Miranda Novales, M. G. (2016). El protocolo de investigación III: la población de estudio. Revista Alergia México, 63(2), 201-206. Recuperado de: https://www.redalyc.org/articulo.oa?id=486755023011
- Hernández Sampieri, R. y Mendoza, C. (2018). Metodología de la investigación: las rutas cuantitativa, cualitativa y mixta. México: Mc. Graw Hill. Recuperado de: https://www.academia.edu/download/64312353/Investigacion_Rutas_cualitativa_y_cuantitativa.pdf

- Salvadó, I. E. (2016). Tipos de muestreo. Investigación científica [presentación de diapositivas]. Recuperado de: http://www.bvs.hn/Honduras/Embarazo/Tipos.de.Muestreo.Marzo.2016.pdf
- Callejo Gallego, J. (2002). Observación, entrevista y grupo de discusión: el silencio de tres prácticas de investigación. Revista española de salud pública, 76, 409-422. Recuperado de: https://www.scielosp.org/pdf/resp/2002.v76n5/409-422/es
- Troncoso-Pantoja, C., & Amaya-Placencia, A. (2017). Entrevista: guía práctica para la recolección de datos cualitativos en investigación de salud. Revista de la Facultad de Medicina, 65(2), 329-332. Recuperado de: http://www.scielo.org.co/scielo.php?pid=S0120-00112017000200329&script=sci_arttext
- Hoyos, J. G. O. (2000). Principios éticos de la investigación en seres humanos y en animales. Medicina (B Aires)[Internet], 60(2), 255-8. Recuperado de: https://www.medicinabuenosaires.com/demo/revistas/vol60-00/2/v60_n2_255_258.pdf
- Hoyos, J. G. O. (2000). Principios éticos de la investigación en seres humanos y en animales. Medicina (B Aires)[Internet], 60(2), 255-8. Recuperado de: https://www.medicinabuenosaires.com/demo/revistas/vol60-00/2/v60_n2_255_258.pdf
- Polo Santillán, M. Á. (2019). La responsabilidad ética. Veritas, (42), 49-72. Recuperado de: https://www.scielo.cl/scielo.php?pid=S0718-92732019000100049&script=sci_arttext&tlng=pt
- Campos, N. J. O. (2019). Normativa Legal sobre Delitos Informáticos en Ecuador. *Revista Científica Hallazgos21*, *4*(1), 100-111. Recuperado de: https://dialnet.unirioja.es/servlet/articulo?codigo=7148227
- Rafael Capurro, la ética en la seguridad informática implica la responsabilidad de proteger los derechos humanos. Recuperado de: https://www.capurro.de/colombia.htm
- Robles Sotomayor, F. M. (2018). La protección de datos personales como medio de prevención de los delitos informáticos en el Perú, en los años 2017 y 2018. Recuperado de: https://repositorio.uap.edu.pe/handle/20.500.12990/8889
- Huamán Cruz, M. Y. (2020). Los delitos informáticos en Perú y la suscripción del Convenio de Budapest. Recuperado de: https://alicia.concytec.gob.pe/vufind/Record/UACI_2fc020cca5ff1f4278a8a4d2658b4ea2
- Renzo Vinelli Vereau (2021) en su artículo "Los delitos informáticos y su relación con la criminalidad económica ". Recuperado de: https://revistas.ulima.edu.pe/index.php/Ius_et_Praxis/article/view/4995

- 12 González (2013), p. 1.085; Jijena (1993-1994), p. 364; Moscoso (2014), p. 13.
- CLAUS, Roxin et. Al. Problemas fundamentales de política criminal y derecho penal. México: Editorial de la Universidad Autónoma de México, 2002, 87 y 88.
- Andina: (Consultado el 16 de Julio del 2023). Recuperado de: https://shorturl.at/inpO9
- Texto Oficial de ‘’El Peruano’’, de fecha 1 de Junio del 2021, recuperado de: https://shorturl.at/dmuOY
- Biblioteca del congreso nacional de chile (2020), recuperado de: https://acortar.link/CCZCp0
- Texto oficial de “El peruano” de fecha 17 de julio de 2000, recuperado de: https://acortar.link/KaBCNu
- Texto oficial de “El peruano” de fecha 19 de agosto del 2013, recuperado de: https://acortar.link/7uRFG8
- Texto oficial de “El peruano” de fecha 19 de setiembre del 2013, recuperado de: https://acortar.link/5YkwYQ
- Texto oficial de “El peruano” de fecha 10 de marzo del 2014, recuperado de: https://acortar.link/zzK4x4
- Directiva de la Unión Europea sobre Seguridad Cibernética (2016), recuperado de: https://acortar.link/YWcjNc
- Ortega Giménez, Alfonso, & Gonzalo Domenech, Juan José. (2018). Nuevo marco jurídico en materia de protección de datos de carácter personal en la Unión Europea. *Revista de la Facultad de Derecho*, (44), 31-73. Recuperado de: https://doi.org/10.22187/rfd2018n44a2
- Macías-Lara , R. A. ., Boné Andrade, M. F. ., Quiñonez Angulo, F. ., Mendoza Loor, J. J., Estupiñan-Troya, G. ., & Rodríguez Vizuete, J. D. . (2022). Frequent cases, criminalization and prevention of computer crimes in Ecuador: a brief systematic review. *Sapienza: International Journal of Interdisciplinary Studies*, *3*(2), 231–243. Recuperado de: https://doi.org/10.51798/sijis.v3i2.324
- Riega Virú, Y., Huamani Chirinos, H. L., & Machuca Vílchez, J. A. (2021). Contratación electrónica y los delitos informáticos. En protección al consumidor en el Perú. *Lex (Lima)*, *19*(28), 197-236. Recuperado de https://biblat.unam.mx/es/revista/lex-lima/articulo/contratacion-electronica-y-los-delitos-informaticos-en-proteccion-al-consumidor-en-el-peru

Sobre los estilos de redacción:

El formato de la tesis, las citas y las referencias se harán de acuerdo con el Manual de Publicaciones de la American Psychological Association séptima edición, los cuales se encuentran disponibles en todos los Centros de Información de UPN, bajo la siguiente referencia:

Código: 808.06615 APA/D

También pueden consultar la siguiente página web:

http://www.apastyle.org/learn/tutorials/index.aspx

Nota importante: La Facultad de Salud (excepto Psicología) utilizará el estilo Vancouver.

CONSTANCIA DE REVISIÓN DEL PROYECTO DE TESIS

El/la docente asesor/a ……, de la Universidad Privada del Norte, de la Facultad de ……, carrera profesional de ……, ha realizado el seguimiento en el desarrollo del Proyecto de Investigación del/os estudiante/s:

- …..
- ……

Por cuanto considera que los dos primeros capítulos (Introducción y Metodología) de la Tesis titulado ……, reúne las condiciones adecuadas para continuar con los siguientes capítulos, previo levantamiento de las observaciones indicadas al/los estudiantes/s, las mismas que son (Marcar con un check según corresponda):

Algunos aspectos de forma	
Algunos aspectos de fondo	
Algunos aspectos de fondo y forma	
Aplicar APA 7ma edición	

Por lo que, AUTORIZO la presentación de los dos primeros capítulos de la Tesis a al/los interesados/s/as, recomendando levantar sus observaciones previo al inicio del curso de Taller de Tesis 2.

_____

Ing. /Lic./Mg./Dr. Nombre y Apellidos

Asesor

UPN UNIVERSIDAD PRIVADA DEL NORTE

UPN UNIVERSIDAD PRIVADA DEL NORTE

PROTOCOLO DE CONSENTIMIENTO INFORMADO PARA ENCUESTAS

La finalidad de este protocolo en Ciencias Sociales, es informarle sobre el proyecto de investigación y solicitarle su consentimiento. De aceptar, los investigadores y usted se quedarán con una copia.

La presente investigación se titula: El comercio ilegal de SIMS CARDS y su influencia en la comisión de delito de fraude informático registrado en la DIVINDAT 2019-2022

y es dirigido por los estudiantes Paulo Edgardo Huaman Miraval y Diego Alonso Merino Flores, investigadores de la UNIVERSIDAD PRIVADA DEL NORTE.

El propósito de la investigación es:

ANALIZAR EL SIGNIFICADO DE FRAUDE INFORMATICO Y LOS PENSAMIENTOS DE COMO INFLUYE EL COMERCIO ILEGAL DE SIMS CARDS APLICADAS A MIEMBROS DE LA DIVINDAT.

Para ello, se le invita a participar en una encuesta que le tomará 10 minutos de su tiempo.

Su participación en la investigación es completamente voluntaria y anónima. Usted puede decidir interrumpirla en cualquier momento, sin que ello le genere ningún perjuicio. Si tuviera alguna inquietud y/o duda sobre la investigación, puede formularla cuando crea conveniente.

Al concluir la investigación, usted será informado de los resultados a través del WhatsApp 982800832 o 950861802. Si desea, también podrá escribir a los correos N00183304@upn.pe o N00184094@upn.pe para recibir más información.

Si está de acuerdo con los puntos anteriores, complete sus datos a continuación:

Nombre: Edward Ivan Scott Arenaza

Fecha: 02/10/2023 Correo electrónico: edward_ivanscott@hotmail

Firma del participante (*):

Firma del investigador:

EDWARD SCOTT ARENAZA
COMANDANTE PNP

(*)La firma de la presente es la voluntad libre y expresa del consentimiento informado para la realización de la encuesta para el estudio de investigación.

UPN UNIVERSIDAD PRIVADA DEL NORTE

UPN UNIVERSIDAD PRIVADA DEL NORTE

MATRIZ PARA EVALUACIÓN DE EXPERTOS

Título de la investigación:	El comercio ilegal de SIMS CARDS y su influencia en la comisión de delito de fraude informático registrado en la DIVINDAT 2019-2022
Línea de investigación:	Tecnologías emergentes
Apellidos y nombres del experto:	Scott Arenaza, Edward Juan
El instrumento de medición pertenece a la variable:	Guía de entrevista

Mediante la matriz de evaluación de expertos, Ud. tiene la facultad de evaluar cada una de las preguntas marcando con una "x" en las columnas de SÍ o NO. Asimismo, le exhortamos en la corrección de los ítems, indicando sus observaciones y/o sugerencias, con la finalidad de mejorar la coherencia de las preguntas sobre la variable en estudio.

Items	Preguntas	Aprecia		Observaciones
		SÍ	NO	
1	¿El instrumento de medición presenta el diseño adecuado?	x		
2	¿El instrumento de recolección de datos tiene relación con el título de la investigación?	x		
3	¿En el instrumento de recolección de datos se mencionan las variables de investigación?	x		
4	¿El instrumento de recolección de datos facilitará el logro de los objetivos de la investigación?	x		
5	¿El instrumento de recolección de datos se relaciona con las variables de estudio?	x		
6	¿La redacción de las preguntas tienen un sentido coherente y no están sesgadas?	x		
7	¿Cada una de las preguntas del instrumento de medición se relaciona con cada uno de los elementos de los indicadores?	x		
8	¿El diseño del instrumento de medición facilitará el análisis y procesamiento de datos?	x		
9	¿Son entendibles las alternativas de respuesta del instrumento de medición?	x		
10	¿El instrumento de medición será accesible a la población sujeto de estudio?	x		
11	¿El instrumento de medición es claro, preciso y sencillo de responder para, de esta manera, obtener los datos requeridos?	x		

Sugerencias:

Firma del experto:

CIP-272162
EDWARD SCOTT ARENAZA
COMANDANTE PNP

UPN UNIVERSIDAD PRIVADA DEL NORTE

UPN UNIVERSIDAD PRIVADA DEL NORTE

PROTOCOLO DE CONSENTIMIENTO INFORMADO PARA ENCUESTAS

La finalidad de este protocolo en Ciencias Sociales, es informarle sobre el proyecto de investigación y solicitarle su consentimiento. De aceptar, los investigadores y usted se quedarán con una copia.

La presente investigación se titula: El comercio ilegal de SIMS CARDS y su influencia en la comisión de delito de fraude informático registrado en la DIVINDAT 2019-2022

y es dirigido por los estudiantes Paulo Edgardo Huaman Miraval y Diego Alonso Merino Flores, investigadores de la UNIVERSIDAD PRIVADA DEL NORTE.

El propósito de la investigación es:

Analizar el significado de fraude informatico y los pensamientos de como influye el comercio ilegal de sims cards aplicadas a miembros de la divindat.

Para ello, se le invita a participar en una encuesta que le tomará 10 minutos de su tiempo.

Su participación en la investigación es completamente voluntaria y anónima. Usted puede decidir interrumpirla en cualquier momento, sin que ello le genere ningún perjuicio. Si tuviera alguna inquietud y/o duda sobre la investigación, puede formularla cuando crea conveniente.

Al concluir la investigación, usted será informado de los resultados a través del WhatsApp 982800832 o 950861802. Si desea, también podrá escribir a los correos N00183304@upn.pe o N00184094@upn.pe para recibir más información.

Si está de acuerdo con los puntos anteriores, complete sus datos a continuación:

Nombre: Julio Enrique Jorjan Chuin

Fecha: 02OCT2023 Correo electrónico: jeforfanch@outlook.com

Firma del participante (*):

Firma del investigador:

(*)La firma de la presente es la voluntad libre y expresa del consentimiento informado para la realización de la encuesta para el estudio de investigación.

UPN UNIVERSIDAD PRIVADA DEL NORTE

UPN UNIVERSIDAD PRIVADA DEL NORTE

MATRIZ PARA EVALUACIÓN DE EXPERTOS

Título de la investigación:	El comercio ilegal de SIMS CARDS y su influencia en la comisión de delito de fraude informático registrado en la DIVINDAT 2019-2022
Línea de investigación:	Tecnologías emergentes
Apellidos y nombres del experto:	Farfan Chiun Julio Enrique
El instrumento de medición pertenece a la variable:	Guía de entrevista

Mediante la matriz de evaluación de expertos, Ud. tiene la facultad de evaluar cada una de las preguntas marcando con una "x" en las columnas de SÍ o NO. Asimismo, le exhortamos en la corrección de los ítems, indicando sus observaciones y/o sugerencias, con la finalidad de mejorar la coherencia de las preguntas sobre la variable en estudio.

Items	Preguntas	Aprecia		Observaciones
		SÍ	NO	
1	¿El instrumento de medición presenta el diseño adecuado?	X		
2	¿El instrumento de recolección de datos tiene relación con el título de la investigación?	X		
3	¿En el instrumento de recolección de datos se mencionan las variables de investigación?	X		
4	¿El instrumento de recolección de datos facilitará el logro de los objetivos de la investigación?	X		
5	¿El instrumento de recolección de datos se relaciona con las variables de estudio?	X		
6	¿La redacción de las preguntas tienen un sentido coherente y no están sesgadas?	X		
7	¿Cada una de las preguntas del instrumento de medición se relaciona con cada uno de los elementos de los indicadores?	X		
8	¿El diseño del instrumento de medición facilitará el análisis y procesamiento de datos?	X		
9	¿Son entendibles las alternativas de respuesta del instrumento de medición?	X		
10	¿El instrumento de medición será accesible a la población sujeto de estudio?	X		
11	¿El instrumento de medición es claro, preciso y sencillo de responder para, de esta manera, obtener los datos requeridos?	X		

Sugerencias:

Firma del experto:

CIP. 368121
JULIO ENRIQUE FARFAN CHIUN
MAY S. PNP

UPN UNIVERSIDAD PRIVADA DEL NORTE

PROTOCOLO DE CONSENTIMIENTO INFORMADO PARA ENCUESTAS

La finalidad de este protocolo en Ciencias Sociales, es informarle sobre el proyecto de investigación y solicitarle su consentimiento. De aceptar, los investigadores y usted se quedarán con una copia.

La presente investigación se titula: El comercio ilegal de SIMS CARDS y su influencia en la comisión de delito de fraude informático registrado en la DIVINDAT 2019-2022

y es dirigido por los estudiantes Paulo Edgardo Huaman Miraval y Diego Alonso Merino Flores, investigadores de la UNIVERSIDAD PRIVADA DEL NORTE.

El propósito de la investigación es:

Analizar el significado de fraude informatico y los pensamientos de como influye el comercio ilegal de sims cards aplicadas a miembros de la DIVINDAT

Para ello, se le invita a participar en una encuesta que le tomará 10 minutos de su tiempo.

Su participación en la investigación es completamente voluntaria y anónima. Usted puede decidir interrumpirla en cualquier momento, sin que ello le genere ningún perjuicio. Si tuviera alguna inquietud y/o duda sobre la investigación, puede formularla cuando crea conveniente.

Al concluir la investigación, usted será informado de los resultados a través del WhatsApp 982800832 o 950861802. Si desea, también podrá escribir a los correos N00183304@upn.pe o N00184094@upn.pe para recibir más información.

Si está de acuerdo con los puntos anteriores, complete sus datos a continuación:

Nombre: Andrea Estaurofila Rodriguez Flores

Fecha: 02/10/2023 Correo electrónico: andrea.erf1989@gmail.com

Firma del participante (*):

Firma del investigador:

(*)La firma de la presente es la voluntad libre y expresa del consentimiento informado para la realización de la encuesta para el estudio de investigación.

UPN UNIVERSIDAD PRIVADA DEL NORTE

UPN UNIVERSIDAD PRIVADA DEL NORTE

MATRIZ PARA EVALUACIÓN DE EXPERTOS

Título de la investigación:	El comercio ilegal de SIMS CARDS y su influencia en la comisión de delito de fraude informático registrado en la DIVINDAT 2019-2022
Línea de investigación:	Tecnologías emergentes
Apellidos y nombres del experto:	Rodríguez Flores, Andrea Estefanie
El instrumento de medición pertenece a la variable:	Guía de entrevista

Mediante la matriz de evaluación de expertos, Ud. tiene la facultad de evaluar cada una de las preguntas marcando con una "x" en las columnas de SÍ o NO. Asimismo, le exhortamos en la corrección de los ítems, indicando sus observaciones y/o sugerencias, con la finalidad de mejorar la coherencia de las preguntas sobre la variable en estudio.

Items	Preguntas	Aprecia		Observaciones
		SÍ	NO	
1	¿El instrumento de medición presenta el diseño adecuado?	X		
2	¿El instrumento de recolección de datos tiene relación con el título de la investigación?	X		
3	¿En el instrumento de recolección de datos se mencionan las variables de investigación?	X		
4	¿El instrumento de recolección de datos facilitará el logro de los objetivos de la investigación?	X		
5	¿El instrumento de recolección de datos se relaciona con las variables de estudio?	X		
6	¿La redacción de las preguntas tienen un sentido coherente y no están sesgadas?	X		
7	¿Cada una de las preguntas del instrumento de medición se relaciona con cada uno de los elementos de los indicadores?	X		
8	¿El diseño del instrumento de medición facilitará el análisis y procesamiento de datos?	X		
9	¿Son entendibles las alternativas de respuesta del instrumento de medición?	X		
10	¿El instrumento de medición será accesible a la población sujeto de estudio?	X		
11	¿El instrumento de medición es claro, preciso y sencillo de responder para, de esta manera, obtener los datos requeridos?	X		

Sugerencias:

Firma del experto:

Andrea E. Rodríguez Flores
S..... PNP
CIP: 31478612

UPN UNIVERSIDAD PRIVADA DEL NORTE

PROTOCOLO DE CONSENTIMIENTO INFORMADO PARA ENCUESTAS

La finalidad de este protocolo en Ciencias Sociales, es informarle sobre el proyecto de investigación y solicitarle su consentimiento. De aceptar, los investigadores y usted se quedarán con una copia.

La presente investigación se titula: El comercio ilegal de SIMS CARDS y su influencia en la comisión de delito de fraude informático registrado en la DIVINDAT 2019-2022

y es dirigido por los estudiantes Paulo Edgardo Huaman Miraval y Diego Alonso Merino Flores, investigadores de la UNIVERSIDAD PRIVADA DEL NORTE.

El propósito de la investigación es:

ANALIZAR EL SIGNIFICADO DE FRAUDE INFORMATICO Y LOS PENSAMIENTOS DE COMO INFLUYE EL COMERCIO ILEGAL DE SIMS CARDS APLICADAS A MIEMBROS DE LA DIVINDAT

Para ello, se le invita a participar en una encuesta que le tomará 10 minutos de su tiempo.

Su participación en la investigación es completamente voluntaria y anónima. Usted puede decidir interrumpirla en cualquier momento, sin que ello le genere ningún perjuicio. Si tuviera alguna inquietud y/o duda sobre la investigación, puede formularla cuando crea conveniente.

Al concluir la investigación, usted será informado de los resultados a través del WhatsApp 982800832 o 950861802. Si desea, también podrá escribir a los correos N00183304@upn.pe o N00184094@upn.pe para recibir más información.

Si está de acuerdo con los puntos anteriores, complete sus datos a continuación:

Nombre: ROBERTO MANUEL ROVILLOU BERMUDEZ

Fecha: 02-OCT-2023 Correo electrónico: rovillou16@hotmail.com.

Firma del participante (*):

Firma del investigador:

(*)La firma de la presente es la voluntad libre y expresa del consentimiento informado para la realización de la encuesta para el estudio de investigación.

UPN UNIVERSIDAD PRIVADA DEL NORTE

UPN UNIVERSIDAD PRIVADA DEL NORTE

MATRIZ PARA EVALUACIÓN DE EXPERTOS

Título de la investigación:	El comercio ilegal de SIMS CARDS y su influencia en la comisión de delito de fraude informático registrado en la DIVINDAT 2019-2022
Línea de investigación:	Tecnologías emergentes
Apellidos y nombres del experto:	Rouillon Bermudez Roberto Manuel
El instrumento de medición pertenece a la variable:	Guía de entrevista

Mediante la matriz de evaluación de expertos, Ud. tiene la facultad de evaluar cada una de las preguntas marcando con una "x" en las columnas de SÍ o NO. Asimismo, le exhortamos en la corrección de los ítems, indicando sus observaciones y/o sugerencias, con la finalidad de mejorar la coherencia de las preguntas sobre la variable en estudio.

Items	Preguntas	Aprecia		Observaciones
		SÍ	NO	
1	¿El instrumento de medición presenta el diseño adecuado?	X		
2	¿El instrumento de recolección de datos tiene relación con el título de la investigación?	X		
3	¿En el instrumento de recolección de datos se mencionan las variables de investigación?	X		
4	¿El instrumento de recolección de datos facilitará el logro de los objetivos de la investigación?	X		
5	¿El instrumento de recolección de datos se relaciona con las variables de estudio?	X		
6	¿La redacción de las preguntas tienen un sentido coherente y no están sesgadas?	X		
7	¿Cada una de las preguntas del instrumento de medición se relaciona con cada uno de los elementos de los indicadores?	X		
8	¿El diseño del instrumento de medición facilitará el análisis y procesamiento de datos?	X		
9	¿Son entendibles las alternativas de respuesta del instrumento de medición?	X		
10	¿El instrumento de medición será accesible a la población sujeto de estudio?	X		
11	¿El instrumento de medición es claro, preciso y sencillo de responder para, de esta manera, obtener los datos requeridos?	X		

Sugerencias:

Firma del experto:

CIP - 344621
Roberto M. ROUILLON BERMUDEZ
MAYOR PNP

UPN UNIVERSIDAD PRIVADA DEL NORTE

PROTOCOLO DE CONSENTIMIENTO INFORMADO PARA ENCUESTAS

La finalidad de este protocolo en Ciencias Sociales, es informarle sobre el proyecto de investigación y solicitarle su consentimiento. De aceptar, los investigadores y usted se quedarán con una copia.

La presente investigación se titula: El comercio ilegal de SIMS CARDS y su influencia en la comisión de delito de fraude informático registrado en la DIVINDAT 2019-2022

y es dirigido por los estudiantes Paulo Edgardo Huaman Miraval y Diego Alonso Merino Flores, investigadores de la UNIVERSIDAD PRIVADA DEL NORTE.

El propósito de la investigación es:

ANALIZAR EL SIGNIFICADO DE FRAUDE INFORMATICO Y LOS PENSAMIENTOS DE COMO INFLUYE EL COMERCIO ILEGAL DE SIMS CARDS APLICADOS A MIEMBROS DE LA DIVINDAT.

Para ello, se le invita a participar en una encuesta que le tomará 10 minutos de su tiempo.

Su participación en la investigación es completamente voluntaria y anónima. Usted puede decidir interrumpirla en cualquier momento, sin que ello le genere ningún perjuicio. Si tuviera alguna inquietud y/o duda sobre la investigación, puede formularla cuando crea conveniente.

Al concluir la investigación, usted será informado de los resultados a través del WhatsApp 982800832 o 950861802. Si desea, también podrá escribir a los correos N00183304@upn.pe o N00184094@upn.pe para recibir más información.

Si está de acuerdo con los puntos anteriores, complete sus datos a continuación:

Nombre: Rosa Clara Tuesta Estela

Fecha: 02OCT2023 Correo electrónico: rtuestae10@gmail.com

Firma del participante (*):

Firma del investigador:

(*)La firma de la presente es la voluntad libre y expresa del consentimiento informado para la realización de la encuesta para el estudio de investigación.

UPN UNIVERSIDAD PRIVADA DEL NORTE

UPN UNIVERSIDAD PRIVADA DEL NORTE

MATRIZ PARA EVALUACIÓN DE EXPERTOS

Título de la investigación:	El comercio ilegal de SIMS CARDS y su influencia en la comisión de delito de fraude informático registrado en la DIVINDAT 2019-2022
Línea de investigación:	Tecnologías emergentes
Apellidos y nombres del experto:	Tuesta Estela Rosa Clara
El instrumento de medición pertenece a la variable:	Guía de entrevista

Mediante la matriz de evaluación de expertos, Ud. tiene la facultad de evaluar cada una de las preguntas marcando con una "x" en las columnas de SÍ o NO. Asimismo, le exhortamos en la corrección de los ítems, indicando sus observaciones y/o sugerencias, con la finalidad de mejorar la coherencia de las preguntas sobre la variable en estudio.

Items	Preguntas	Aprecia		Observaciones
		SÍ	NO	
1	¿El instrumento de medición presenta el diseño adecuado?	X		
2	¿El instrumento de recolección de datos tiene relación con el título de la investigación?	X		
3	¿En el instrumento de recolección de datos se mencionan las variables de investigación?	X		
4	¿El instrumento de recolección de datos facilitará el logro de los objetivos de la investigación?	X		
5	¿El instrumento de recolección de datos se relaciona con las variables de estudio?	X		
6	¿La redacción de las preguntas tienen un sentido coherente y no están sesgadas?	X		
7	¿Cada una de las preguntas del instrumento de medición se relaciona con cada uno de los elementos de los indicadores?	X		
8	¿El diseño del instrumento de medición facilitará el análisis y procesamiento de datos?	X		
9	¿Son entendibles las alternativas de respuesta del instrumento de medición?	X		
10	¿El instrumento de medición será accesible a la población sujeto de estudio?	X		
11	¿El instrumento de medición es claro, preciso y sencillo de responder para, de esta manera, obtener los datos requeridos?	X		

Sugerencias:

Firma del experto:

SA-31529756
Rosa Clara TUESTA ESTELA
S1 PNP

UPN UNIVERSIDAD PRIVADA DEL NORTE

UPN UNIVERSIDAD PRIVADA DEL NORTE

PROTOCOLO DE CONSENTIMIENTO INFORMADO PARA ENCUESTAS

La finalidad de este protocolo en Ciencias Sociales, es informarle sobre el proyecto de investigación y solicitarle su consentimiento. De aceptar, los investigadores y usted se quedarán con una copia.

La presente investigación se titula: El comercio ilegal de SIMS CARDS y su influencia en la comisión de delito de fraude informático registrado en la DIVINDAT 2019-2022

y es dirigido por los estudiantes Paulo Edgardo Huaman Miraval y Diego Alonso Merino Flores, investigadores de la UNIVERSIDAD PRIVADA DEL NORTE.

El propósito de la investigación es:

ANALIZAR EL SIGNIFICADO DE FRAUDE INFORMATICO Y LOS PENSAMIENTOS DE COMO INFLUYE EL COMERCIO ILEGAL DE SIMS CARDS APLICADAS A MIEMBROS DE LA DIVINDAT.

Para ello, se le invita a participar en una encuesta que le tomará 10 minutos de su tiempo.

Su participación en la investigación es completamente voluntaria y anónima. Usted puede decidir interrumpirla en cualquier momento, sin que ello le genere ningún perjuicio. Si tuviera alguna inquietud y/o duda sobre la investigación, puede formularla cuando crea conveniente.

Al concluir la investigación, usted será informado de los resultados a través del WhatsApp 982800832 o 950861802. Si desea, también podrá escribir a los correos N00183304@upn.pe o N00184094@upn.pe para recibir más información.

Si está de acuerdo con los puntos anteriores, complete sus datos a continuación:

Nombre: ANGEL LEONARDO LEYVA CABELLA

Fecha: 02/04/23 Correo electrónico: hunosymongolo@gmail.com

Firma del participante (*):

Firma del investigador:

(*)La firma de la presente es la voluntad libre y expresa del consentimiento informado para la realización de la encuesta para el estudio de investigación.

UPN UNIVERSIDAD PRIVADA DEL NORTE

UPN UNIVERSIDAD PRIVADA DEL NORTE

MATRIZ PARA EVALUACIÓN DE EXPERTOS

Título de la investigación:	El comercio ilegal de SIMS CARDS y su influencia en la comisión de delito de fraude informático registrado en la DIVINDAT 2019-2022
Línea de investigación:	Tecnologías emergentes
Apellidos y nombres del experto:	LEYVA CABELLO ANGEL LEONARDO
El instrumento de medición pertenece a la variable:	Guía de entrevista

Mediante la matriz de evaluación de expertos, Ud. tiene la facultad de evaluar cada una de las preguntas marcando con una "x" en las columnas de SÍ o NO. Asimismo, le exhortamos en la corrección de los ítems, indicando sus observaciones y/o sugerencias, con la finalidad de mejorar la coherencia de las preguntas sobre la variable en estudio.

Items	Preguntas	Aprecia		Observaciones
		SÍ	NO	
1	¿El instrumento de medición presenta el diseño adecuado?	X		
2	¿El instrumento de recolección de datos tiene relación con el título de la investigación?	X		
3	¿En el instrumento de recolección de datos se mencionan las variables de investigación?	X		
4	¿El instrumento de recolección de datos facilitará el logro de los objetivos de la investigación?	X		
5	¿El instrumento de recolección de datos se relaciona con las variables de estudio?	X		
6	¿La redacción de las preguntas tienen un sentido coherente y no están sesgadas?	X		
7	¿Cada una de las preguntas del instrumento de medición se relaciona con cada uno de los elementos de los indicadores?	X		
8	¿El diseño del instrumento de medición facilitará el análisis y procesamiento de datos?	X		
9	¿Son entendibles las alternativas de respuesta del instrumento de medición?	X		
10	¿El instrumento de medición será accesible a la población sujeto de estudio?	X		
11	¿El instrumento de medición es claro, preciso y sencillo de responder para, de esta manera, obtener los datos requeridos?	X		

Sugerencias:

Firma del experto:

SA - 31081930
ÁNGEL LEYVA CABELLO
SB PNP

UPN UNIVERSIDAD PRIVADA DEL NORTE

UPN UNIVERSIDAD PRIVADA DEL NORTE

PROTOCOLO DE CONSENTIMIENTO INFORMADO PARA ENCUESTAS

La finalidad de este protocolo en Ciencias Sociales, es informarle sobre el proyecto de investigación y solicitare su consentimiento. De aceptar, los investigadores y usted se quedarán con una copia.

La presente investigación se titula: EL COMERCIO ILEGAL DE SIMS CARDS Y SU INFLUENCIA EN LA COMISIÓN DE DELITO DE FRAUDE INFORMATICO REGISTRADOS EN LA DIVINDAT 2019-2022

Y es dirigido por los estudiantes Paulo Edgardo Huaman Miraval y Diego Alonso Merino Flores, investigadores de la UNIVERSIDAD PRIVADA DEL NORTE.

El propósito de la investigación es:

ANALIZAR LA INFLUENCIA DEL COMERCIO ILEGAL DE TARJETAS SIMS EN LA COMISION DE DELITOS DE FRAUDE INFORMATICO, SEGUN REGISTRO DE LA DIVINDAT DURANTE EL PERIODO 2019 - 2022

Para ello, se le invita a participar en una encuentras que le tomará 10 minutos de su tiempo.

Su participación en la investigación es completamente voluntaria y anónima. Usted puede decidir interrumpirla en cualquier momento, sin que ello le genere ningún perjuicio. Si tuviera alguna inquietud y/o duda sobre la investigación, puede formularla cuando crea conveniente.

Al concluir la investigación, usted será informado de los resultados a través del WhatsApp 982800832 o 950861802. Si desea, también para escribir a los correos N00183304@upm.pe o N00184094@upn.pe para recibir más información.

Si está de acuerdo con los puntos anteriores, complete sus datos a continuación:

Nombre: Manuel Antonio Reyes Bolovich

Fecha: 16/05/25 Correo electrónico: bolovich2011@gmail.com

Firma del participante (*):

Firma del investigador:

(*) La firma de la presente es la voluntad libre y expresa del consentimiento informado para la realización de la encuesta para el estudio de la investigación.

UPN UNIVERSIDAD PRIVADA DEL NORTE

Preguntas para los INFORMÁTICOS (peritos, policías, expertos)

1. **¿Cómo facilita el comercio ilegal de tarjetas SIM la comisión de delitos de fraude informático?**

Cada tarjeta SIM puede usarse para crear perfiles falsos en bancos, redes sociales o servicios digitales, esto permite la suplantación de identidad, estafas bancarias y phishing masivo.

   - *Objetivo:* Obtener una explicación técnica sobre la conexión entre ambas prácticas.

2. **¿Qué modalidades de fraude informático (como phishing o smishing) son más comunes en los casos vinculados a SIMs ilegales?**

Phishing (Vishing) Telefónico: llamadas desde números con SIM ilegales para hacerse pasar por bancos, operadores o autoridades.

   - *Objetivo:* Profundizar en el modus operandi de los ciberdelincuentes.

3. **¿Qué obstáculos enfrentan al investigar delitos que involucran tarjetas SIM no registradas legalmente?**

Las SIM cards ilegales suelen estar a nombre de terceros (identidades robadas, falsificadas o inventadas), Tal información al pedir es a los operadores Telefónicos quienes deberían dar la información.

   - *Objetivo:* Conocer los retos operativos y legales en la investigación policial.

4. **¿Considera que las sanciones legales actuales (artículo 222-B del Código Penal) son suficientes para disuadir el comercio ilegal de SIMs?**

No, las sanciones no son actualmente suficientes para disuadir el comercio ilegal de SIM cards, baja aplicación real, escasa fiscalización y debil percepción de riesgo entre los involucrados.

   - *Objetivo:* Recoger una valoración crítica sobre la normativa vigente.

5. **¿Qué estrategias o mejoras propone para prevenir el uso del comercio ilegal de SIMs en delitos cibernéticos?**

Implementar leyes severas en el ambito informatico, Registro obligatorio con verificación biometrica, Aplicar sistemas de rastreabilidad de Tarjeta SIM.

   - *Objetivo:* Recabar propuestas desde el enfoque técnico y policial para aportar a las conclusiones.

CamScanner

UPN UNIVERSIDAD PRIVADA DEL NORTE

MATRIZ PARA EVALUACIÓN DE EXPERTOS

Título de la investigación:	EL COMERCIO ILEGAL DE SIMS CARDS Y SU INFLUENCIA EN LA COMISIÓN DE DELITO DE FRAUDE INFORMATICO REGISTRADOS EN LA DIVINDAT 2019-2022
Línea de investigación:	Tecnologías emergentes
Apellidos y nombres del experto:	
El instrumento de medición pertenece a la variable:	Guía de Entrevista

Mediante la matriz de evaluación de expertos, Ud. tiene la facultad de evaluar cada una de las preguntas marcando con una "x" en las columnas de SÍ o NO. Asimismo, le exhortamos en la corrección de los ítems, indicando sus observaciones y/o sugerencias, con la finalidad de mejorar la coherencia de las preguntas sobre la variable en estudio.

Items	Preguntas	Aprecia		Observaciones
		SÍ	NO	
1	¿El instrumento de medición presenta el diseño adecuado?	X		
2	¿El instrumento de recolección de datos tiene relación con el título de la investigación?	X		
3	¿En el instrumento de recolección de datos se mencionan las variables de investigación?	X		
4	¿El instrumento de recolección de datos facilitará el logro de los objetivos de la investigación?	X		
5	¿El instrumento de recolección de datos se relaciona con las variables de estudio?	X		
6	¿La redacción de las preguntas tienen un sentido coherente y no están sesgadas?	X		
7	¿Cada una de las preguntas del instrumento de medición se relaciona con cada uno de los elementos de los indicadores?	X		
8	¿El diseño del instrumento de medición facilitará el análisis y procesamiento de datos?	X		
9	¿Son entendibles las alternativas de respuesta del instrumento de medición?	X		
10	¿El instrumento de medición será accesible a la población sujeto de estudio?	X		
11	¿El instrumento de medición es claro, preciso y sencillo de responder para, de esta manera, obtener los datos requeridos?	X		

Sugerencias:

Firma del experto:

SA - 315[illegible]5618
MANUEL A. REYES BOLOVICH
S1 PNP

UPN UNIVERSIDAD PRIVADA DEL NORTE

PROTOCOLO DE CONSENTIMIENTO INFORMADO PARA ENCUESTAS

La finalidad de este protocolo en Ciencias Sociales, es informarle sobre el proyecto de investigación y solicitare su consentimiento. De aceptar, los investigadores y usted se quedarán con una copia.

La presente investigación se titula: EL COMERCIO ILEGAL DE SIMS CARDS Y SU INFLUENCIA EN LA COMISIÓN DE DELITO DE FRAUDE INFORMATICO REGISTRADOS EN LA DIVINDAT 2019-2022

Y es dirigido por los estudiantes Paulo Edgardo Huaman Miraval y Diego Alonso Merino Flores, investigadores de la UNIVERSIDAD PRIVADA DEL NORTE.

El propósito de la investigación es:

Analizar la influencia del Comercio Ilegal de Tarjetas SIM en la comisión de Delitos de Fraude Informatico, según los Registros de la DIVINDAT durante el Periodo 2019-2022

Para ello, se le invita a participar en una encuentras que le tomará 10 minutos de su tiempo.

Su participación en la investigación es completamente voluntaria y anónima. Usted puede decidir interrumpirla en cualquier momento, sin que ello le genere ningún perjuicio. Si tuviera alguna inquietud y/o duda sobre la investigación, puede formularla cuando crea conveniente.

Al concluir la investigación, usted será informado de los resultados a través del WhatsApp 982800832 o 950861802. Si desea, también para escribir a los correos N00183304@upm.pe o N00184094@upn.pe para recibir más información.

Si está de acuerdo con los puntos anteriores, complete sus datos a continuación:

Nombre: MAY DAP Pierre Ruiz Contreras.

Fecha: 16/05/25 Correo electrónico: divindat.mesadepartes@policia.gob.pe.

Firma del participante (*): _____

Firma del investigador: Paulo H.M Diego M. Flores

(*) La firma de la presente es la voluntad libre y expresa del consentimiento informado para la realización de la encuesta para el estudio de la investigación.

UPN UNIVERSIDAD PRIVADA DEL NORTE

Preguntas para los INFORMÁTICOS (peritos, policías, expertos)

1. **¿Cómo facilita el comercio ilegal de tarjetas SIM la comisión de delitos de fraude informático?**

   ACTIVADOS A TERCERAS PERSONAS PARA COMETER FRAUDES, SUPLANTACION, Y EXTORSIONAR.

   - *Objetivo:* Obtener una explicación técnica sobre la conexión entre ambas prácticas.

2. **¿Qué modalidades de fraude informático (como phishing o smishing) son más comunes en los casos vinculados a SIMs ilegales?**

   PHISHING ES LO MAS COMUN VINCULADOS A LOS SIM CARDS ILEGALES.

   - *Objetivo:* Profundizar en el modus operandi de los ciberdelincuentes.

3. **¿Qué obstáculos enfrentan al investigar delitos que involucran tarjetas SIM no registradas legalmente?**

   QUE LAS PERSONAS SUPLANTADAS SON DE PROVINCIAS Y PERSONAS DE LA TERCERA EDAD.

   - *Objetivo:* Conocer los retos operativos y legales en la investigación policial.

4. **¿Considera que las sanciones legales actuales (artículo 222-B del Código Penal) son suficientes para disuadir el comercio ilegal de SIMs?**

   NO SON LO SUFICIENTE AREMADOS PARA COMBATIR LA COMERCIALIZACION ILEGAL DE SIM CARD ACTIVADAS.

   - *Objetivo:* Recoger una valoración crítica sobre la normativa vigente.

5. **¿Qué estrategias o mejoras propone para prevenir el uso del comercio ilegal de SIMs en delitos cibernéticos?**

   QUE LAS BANCARIAS TIENEN QUE SER MAS RIGUROSAS, YA QUE NO ES UNA BUENA DEFENSA.

   - *Objetivo:* Recabar propuestas desde el enfoque técnico y policial para aportar a las conclusiones.

CamScanner

UPN UNIVERSIDAD PRIVADA DEL NORTE

MATRIZ PARA EVALUACIÓN DE EXPERTOS

Título de la investigación:	EL COMERCIO ILEGAL DE SIMS CARDS Y SU INFLUENCIA EN LA COMISIÓN DE DELITO DE FRAUDE INFORMATICO REGISTRADOS EN LA DIVINDAT 2019-2022
Línea de investigación:	Tecnologías emergentes
Apellidos y nombres del experto:	
El instrumento de medición pertenece a la variable:	Guía de Entrevista

Mediante la matriz de evaluación de expertos, Ud. tiene la facultad de evaluar cada una de las preguntas marcando con una "x" en las columnas de SÍ o NO. Asimismo, le exhortamos en la corrección de los ítems, indicando sus observaciones y/o sugerencias, con la finalidad de mejorar la coherencia de las preguntas sobre la variable en estudio.

Items	Preguntas	Aprecia		Observaciones
		SÍ	NO	
1	¿El instrumento de medición presenta el diseño adecuado?	X		
2	¿El instrumento de recolección de datos tiene relación con el título de la investigación?	X		
3	¿En el instrumento de recolección de datos se mencionan las variables de investigación?	X		
4	¿El instrumento de recolección de datos facilitará el logro de los objetivos de la investigación?	X		
5	¿El instrumento de recolección de datos se relaciona con las variables de estudio?	X		
6	¿La redacción de las preguntas tienen un sentido coherente y no están sesgadas?	X		
7	¿Cada una de las preguntas del instrumento de medición se relaciona con cada uno de los elementos de los indicadores?	X		
8	¿El diseño del instrumento de medición facilitará el análisis y procesamiento de datos?	X		
9	¿Son entendibles las alternativas de respuesta del instrumento de medición?	X		
10	¿El instrumento de medición será accesible a la población sujeto de estudio?	X		
11	¿El instrumento de medición es claro, preciso y sencillo de responder para, de esta manera, obtener los datos requeridos?	X		

Sugerencias:

Firma del experto:

.....
QA-347136
PIERRE RUIZ CONTRERAS
MAYOR PNP

UPN UNIVERSIDAD PRIVADA DEL NORTE

PROTOCOLO DE CONSENTIMIENTO INFORMADO PARA ENCUESTAS

La finalidad de este protocolo en Ciencias Sociales, es informarle sobre el proyecto de investigación y solicitare su consentimiento. De aceptar, los investigadores y usted se quedarán con una copia.

La presente investigación se titula: EL COMERCIO ILEGAL DE SIMS CARDS Y SU INFLUENCIA EN LA COMISIÓN DE DELITO DE FRAUDE INFORMATICO REGISTRADOS EN LA DIVINDAT 2019-2022

Y es dirigido por los estudiantes Paulo Edgardo Huaman Miraval y Diego Alonso Merino Flores, investigadores de la UNIVERSIDAD PRIVADA DEL NORTE.

El propósito de la investigación es:

ANALIZAR LA INFLUENCIA DEL COMERCIO ILEGAL DE TARJETAS SIMS EN LA COMISION DE DELITOS DE FRAUDE INFORMATICO, SEGÚN REGISTROS DE LA DIVINDAT DURANTE EL PERIODO 2019 - 2022

Para ello, se le invita a participar en una encuentras que le tomará 10 minutos de su tiempo.

Su participación en la investigación es completamente voluntaria y anónima. Usted puede decidir interrumpirla en cualquier momento, sin que ello le genere ningún perjuicio. Si tuviera alguna inquietud y/o duda sobre la investigación, puede formularla cuando crea conveniente.

Al concluir la investigación, usted será informado de los resultados a través del WhatsApp 982800832 o 950861802. Si desea, también para escribir a los correos N00183304@upm.pe o N00184094@upn.pe para recibir más información.

Si está de acuerdo con los puntos anteriores, complete sus datos a continuación:

Nombre: Julio Enrique Farfan Chuan

Fecha: 14 MAYO 2025 Correo electrónico: jefarfanch@outlook.com

Firma del participante (*):

Firma del investigador:

(*) La firma de la presente es la voluntad libre y expresa del consentimiento informado para la realización de la encuesta para el estudio de la investigación.

UPN UNIVERSIDAD PRIVADA DEL NORTE

Preguntas para los INFORMÁTICOS (peritos, policías, expertos)

1. **¿Cómo facilita el comercio ilegal de tarjetas SIM la comisión de delitos de fraude informático?**

   Hace que sea más accesible el acceso a la red de internet a través de la activación ilegal de tarjetas SIM.

   - *Objetivo:* Obtener una explicación técnica sobre la conexión entre ambas prácticas.

2. **¿Qué modalidades de fraude informático (como phishing o smishing) son más comunes en los casos vinculados a SIMs ilegales?**

   Realizan transferencias fraudulentas, compras de pasajes aéreos o débitos en diferentes páginas que brindan servicio electrónico

   - *Objetivo:* Profundizar en el modus operandi de los ciberdelincuentes.

3. **¿Qué obstáculos enfrentan al investigar delitos que involucran tarjetas SIM no registradas legalmente?**

   El acceso a la información de la titularidad de los SIM por parte de los operadores de telefonía

   - *Objetivo:* Conocer los retos operativos y legales en la investigación policial.

4. **¿Considera que las sanciones legales actuales (artículo 222-B del Código Penal) son suficientes para disuadir el comercio ilegal de SIMs?**

   No, considero que debería incrementarse para mermar este fenómeno delictivo en la sociedad

   - *Objetivo:* Recoger una valoración crítica sobre la normativa vigente.

5. **¿Qué estrategias o mejoras propone para prevenir el uso del comercio ilegal de SIMs en delitos cibernéticos?**

   Activar mayores mecanismos de validación (doble autenticación o detección facial, envío de token digitales)

   - *Objetivo:* Recabar propuestas desde el enfoque técnico y policial para aportar a las conclusiones.

CamScanner

UPN UNIVERSIDAD PRIVADA DEL NORTE

MATRIZ PARA EVALUACIÓN DE EXPERTOS

Título de la investigación:	EL COMERCIO ILEGAL DE SIMS CARDS Y SU INFLUENCIA EN LA COMISIÓN DE DELITO DE FRAUDE INFORMATICO REGISTRADOS EN LA DIVINDAT 2019-2022
Línea de investigación:	Tecnologías emergentes
Apellidos y nombres del experto:	Farfan Chiun Julio Enrique
El instrumento de medición pertenece a la variable:	Guía de Entrevista

Mediante la matriz de evaluación de expertos, Ud. tiene la facultad de evaluar cada una de las preguntas marcando con una "x" en las columnas de SÍ o NO. Asimismo, le exhortamos en la corrección de los ítems, indicando sus observaciones y/o sugerencias, con la finalidad de mejorar la coherencia de las preguntas sobre la variable en estudio.

Items	Preguntas	Aprecia		Observaciones
		SÍ	NO	
1	¿El instrumento de medición presenta el diseño adecuado?	X		
2	¿El instrumento de recolección de datos tiene relación con el título de la investigación?	X		
3	¿En el instrumento de recolección de datos se mencionan las variables de investigación?	X		
4	¿El instrumento de recolección de datos facilitará el logro de los objetivos de la investigación?	X		
5	¿El instrumento de recolección de datos se relaciona con las variables de estudio?	X		
6	¿La redacción de las preguntas tienen un sentido coherente y no están sesgadas?	X		
7	¿Cada una de las preguntas del instrumento de medición se relaciona con cada uno de los elementos de los indicadores?	X		
8	¿El diseño del instrumento de medición facilitará el análisis y procesamiento de datos?	X		
9	¿Son entendibles las alternativas de respuesta del instrumento de medición?	X		
10	¿El instrumento de medición será accesible a la población sujeto de estudio?	X		
11	¿El instrumento de medición es claro, preciso y sencillo de responder para, de esta manera, obtener los datos requeridos?	X		

Sugerencias:

Firma del experto:

DNI - 36[illegible]123
JULIO ENRIQUE FARFAN CHIUN
MAY S. PNP

UPN UNIVERSIDAD PRIVADA DEL NORTE

PERÚ | Ministerio de Educación | Superintendencia Nacional de Educación Superior Universitaria | Dirección de Documentación e Información Universitaria y Registro de Grados y Títulos

REGISTRO NACIONAL DE GRADOS ACADÉMICOS Y TÍTULOS PROFESIONALES

SCOTT ARENAZA, EDWARD IVAN **DNI 09585000**	ABOGADO **Fecha de diploma: 07/05/2013** Modalidad de estudios: -	UNIVERSIDAD INCA GARCILASO DE LA VEGA ASOCIACIÓN CIVIL ***PERU***
SCOTT ARENAZA, EDWAR IVAN **DNI 09585000**	BACHILLER EN ADMINISTRACION Y CIENCIAS POLICIALES **Fecha de diploma: 09/07/2013** Modalidad de estudios: - Fecha matrícula: Sin información (***) Fecha egreso: Sin información (***)	ESCUELA DE OFICIALES DE LA POLICÍA NACIONAL DEL PERÚ ***PERU***
SCOTT ARENAZA, EDWARD IVAN **DNI 09585000**	BACHILLER EN DERECHO Y CIENCIAS POLITICAS **Fecha de diploma: 29/12/2010** Modalidad de estudios: - Fecha matrícula: Sin información (***) Fecha egreso: Sin información (***)	UNIVERSIDAD INCA GARCILASO DE LA VEGA ASOCIACIÓN CIVIL ***PERU***
SCOTT ARENAZA, EDWARD IVAN **DNI 09585000**	LICENCIADO EN ADMINISTRACION Y CIENCIAS POLICIALES **Fecha de diploma: 24-12-2014** Modalidad de estudios: -	ESCUELA DE OFICIALES DE LA POLICÍA NACIONAL DEL PERÚ ***PERU***
SCOTT ARENAZA, EDWARD IVAN **DNI 09585000**	MAESTRO EN ADMINISTRACIÓN Y CIENCIAS POLICIALES CON MENCIÓN EN CRIMINALÍSTICA **Fecha de diploma: 24/05/23** Modalidad de estudios: PRESENCIAL Fecha matrícula: 17/12/2021 Fecha egreso: 30/12/2022	ESCUELA DE POSGRADO DE LA POLICÍA NACIONAL DEL PERÚ ***PERU***

Paulo Edgardo Huaman Miraval

EL COMERCIO ILEGAL DE SIMS CARDS Y SU INFLUENCIA EN LA COMISIÓN DE DELITO DE FRAUDE INFORMATICO REGIST...

Quick Submit

Quick Submit

Asesores

Detalles del documento

Identificador de la entrega
trn:oid:::1:3275414665

Fecha de entrega
12 jun 2025, 11:23 p.m. GMT-5

Fecha de descarga
12 jun 2025, 11:44 p.m. GMT-5

Nombre de archivo
TESIS_11_DE_JUNIO.docx

Tamaño de archivo
10.1 MB

88 Páginas

13.540 Palabras

76.281 Caracteres

17% Similitud general

El total combinado de todas las coincidencias, incluidas las fuentes superpuestas, para ca...

Filtrado desde el informe

- Bibliografía
- Texto citado
- Texto mencionado
- Coincidencias menores (menos de 8 palabras)

Exclusiones

- N.º de fuentes excluidas

Fuentes principales

15% Fuentes de Internet
3% Publicaciones
8% Trabajos entregados (trabajos del estudiante)

Marcas de integridad

N.º de alertas de integridad para revisión

No se han detectado manipulaciones de texto sospechosas.

Los algoritmos de nuestro sistema analizan un documento en profundidad para buscar inconsistencias que permitirían distinguirlo de una entrega normal. Si advertimos algo extraño, lo marcamos como una alerta para que pueda revisarlo.

Una marca de alerta no es necesariamente un indicador de problemas. Sin embargo, recomendamos que preste atención y la revise.

turnitin Página 2 of 100 - Descripción general de integridad Identificador de la entrega trn:oid:::1:3275414665

N	PRODECENCIA	NUMERO DE GUIA	FECHA		DENUNCIADOS	DELITO	ESPECIES	INSTRUCTOR
1	ACTA DE INTERVENCION	057-25	8/01/2025	FLAGRANCIA	MANUEL HUAMAN POZO	DELITO INFORMATICO-ACCESO ILICITO, DELITO CONTRA LA FE PUBLICA, SUPLANTACION DE IDENTIDAD, ABUSO DE MECANISMOS Y DISPOSITIVOS INFORMATICOS, DELITO CONTRA EL PATRIMONIO-RECEPTACION AGRAVADA	-CIENTO CINCO(105) SIM CARDS--- DOS (02) LECTORAS BIOMETRICAS-- CINCO (05) TELEFONOS--- DOS MIL QUINIENTOS SETENTA Y OCHO (2578)	S3 TEJADA
2	ACTA DE INTERVENCION	1652-25	19/03/2025	FLAGRANCIA	EVA CHUMBILE FLORES	DELITO CONTRA EL PATRIMONIO-RECEPTACION	SIETE (07)TARJETAS LINEA 1-- UN (01) CELULAR-- UN (01) SIMCARDS-- DOS (02) CHIPS GNV-- CIENTO CINCUENTA Y TRES (153) SOLES	S3 QUISPE QUISPE
3	ACTA DE INTERVENCION	2932-24	6-Nov-24	FLAGRANCIA	Nilo FIGUEROA CRISOSTOMO, Ana ACUÑA VASQUEZ	DELITO CONTRA LA PROPIEDAD INDUSTRIAL-POSESION ILEGITIMA DE SIM CARDS,DELITO CONTRA LA FE PUBLICA-SUPLANTACION DE IDENTIDAD, DELITO DE ABUSO DE MECANISMOS Y DISPOSITIVOS INFORMATICOS	-CINCO (05) CELULARES, CINCUENTRA Y CUATRO (54) SIMCARD, OCHO (08) LECTORAS , CUARENTA (40) SOLES.	S3 MAMANI SANTOS

CIP. N° 3094036
Wilfredo CRUZADO MALCA
SS/PNP

OA-347136
PIERRE RUIZ CONTRERAS
MAYOR PNP