*Lucerna Iuris Et Investigatio*
n.º 4 - 2023, pp. 27 - 47
https://doi.org/10.15381/lucerna.n4.26638

Print ISSN: 2788-6689
Online ISSN: XXXX-XXXX
Facultad de Derecho y Ciencia Política UNMSM

INVESTIGACIONES NACIONALES

# Imperceptibilidad de la cibercriminalidad en la suplantación de identidad mediante huellas dactilares de silicona. Análisis del caso Julio César Flores

## Imperceptibility of cybercrime in identity theft using silicone fingerprints. Analysis of the Julio César Flores case

***Bertho Arturo Menacho Ortega***[1]

**Universidad Privada del Norte, Perú**

menachoortegaarturo@gmail.com

https://orcid.org/0000-0002-7370-6747

Presentado: 12/09/2022 - Aceptado: 14/12/2022- Publicación: 31/08/2023

**Resumen**

La cibercriminalidad centró su actividad delictiva en la suplantación de identidad mediante la tarjeta SIM valiéndose de las vulnerabilidades que posibilitan las empresas de telefonía móvil, las entidades bancarias y el desconocimiento de los internautas sobre las modalidades del ciberfraude. El objetivo de este artículo es establecer si es posible suplantar la identidad de una persona a través de huellas dactilares de silicona y disponer del patrimonio de las cuentas bancarias. Se utilizó la metodología de investigación de tipo socio jurídica, con propósito básico, cuyo enfoque fue cualitativo, nivel exploratorio y diseño de estudio de casos. A partir del suceso de Julio César Flores se estableció que es posible suplantar la identidad de las personas mediante sus huellas dactilares artesanales y disponer del patrimonio de las cuentas bancarias asociadas al número de SIM por medio de la captación de información y el apoderamiento de la línea móvil. Los cibercriminales aprovechan la venta ambulante de chip y el acceso a la base de datos de RENIEC para extraer la información personal de las cibervíctimas, reportar las líneas telefónicas, reponerlas y duplicarlas para disponer del dinero, solicitar créditos o adquirir servicios.

**Palabras clave:** ciberfraude, SIM-Swap, ciberdelincuencia, ciberespacio y patrullaje virtual.

**Abstract**
The cyberdelinquency SIM centred his criminal activity on the forgery of identity by means of the card using of the vulnerabilities that there make possible the companies of mobile telephony, the banking institutions and the ignorance of the Net users on the forms of the cyberfraud. The target of this article is to establish if it is possible to supplant the identity of a person across fingerprints of silicone and to have the patrimony of the bank accounts. Associate used the methodology of investigation of type juridical, with basic intention, which approach was qualitative, an exploratory level and design of study of cases. From the event of Julio César Flores, it was established that it is possible to supplant the identity of the persons by means of his handmade fingerprints and to have the patrimony of the bank accounts associated with the number of SIM by means of the reception of information and the authorization of the mobile line. The cybercriminals make use of the ambulant selling of chip and the access to the database of RENIEC to extract the personal information of the cybervictims, to bring the telephone lines, to restore them and to duplicate them to have the money, to request credits or to acquire services.

**Keywords:** cyberfraud, SIM-Swap, cybercrime, cyberspace and virtual patrol.

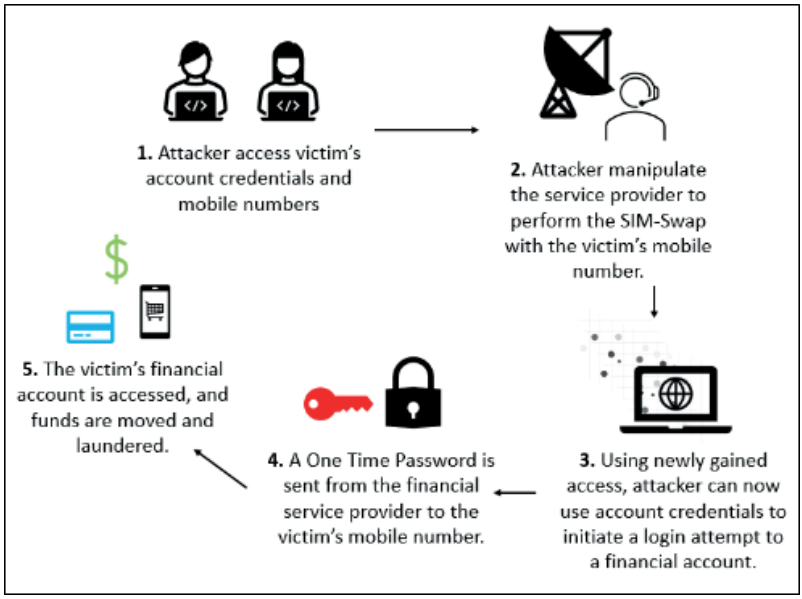
## I. Introducción

Los esfuerzos por robustecer los sistemas de seguridad en las transacciones de dinero electrónico fueron intensas y arduas, una clara materialización es la incorporación del sistema de reconocimiento biométrico a través de la huella dactilar, lo que permite validar la información personal de un sujeto para realizar un trámite ante el Estado o un ente particular.

Del mismo modo, se pueden comentar sobre diversos casos en los que se incluye el phishing, la ingeniería social y la ciberseguridad que giran en torno al intercambio de las tarjetas SIM. El impulso esencial para cometer estos delitos es la descomunal ganancia percibida por el atacante. Los casos más conocidos a nivel internacional convocan a Ortiz y Freeman, quienes realizaron el pirateo de las cuentas de Coinbase en donde sus víctimas tenían euros convertidos en criptomonedas por los montos de $ 5 y $ 2 millones, consecutivamente (Nicholls et al., 2016).

En el presente estudio importa centrar nuestros esfuerzos en el análisis de esta ingeniosa, pero perjudicial forma de comisión de delitos informáticos en la que no solo existe responsabilidad de las autoridades y las empresas que brindan los servicios de telefonía o banca móvil, sino que también están involucradas las víctimas, tal y como se aprecia en el siguiente organizador visual.

**Figura 1**
*Diagrama del proceso de SIM-Swap*




*Nota.* Obtenido de "*Ciberdelincuencia financiera: una encuesta exhaustiva de enfoques de aprendizaje profundo para abordar el panorama de la delincuencia financiera en evolución*", Nicholls et al., 2016, p. 13.

Sobre las fases de ejecución del SIM-swap, partiendo desde que el atacante obtiene las credenciales de la cuenta, así como los números de celular de sus víctimas, continúa por la manipulación del proveedor de servicio de telefonía para iniciar sesión de la cuenta vinculada, culminando su actuación delictiva con el envío del token o contraseña por parte del operador de servicios financieros y la disposición de los fondos (Nicholls et al., 2016).

Puede anotarse que, el problema que se pretende esclarecer consiste en si ¿Es posible suplantar la identidad de una persona a través de huellas dactilares de silicona y disponer del patrimonio de las cuentas bancarias? A su vez, en busca de aportar una reflexión consistente se trazó como objetivo «Establecer si es posible suplantar la identidad de una persona a través de huellas dactilares de silicona y disponer del patrimonio de las cuentas bancarias».

El artículo presentado aborda la exposición y vulnerabilidad que vienen atravesando las personas que utilizan el aplicativo de banca móvil en el sistema bancario y telefónico del Perú, a propósito del caso Julio César Flores. La relevancia viene dada por el incremento de casos reportados

por diferentes personas a quienes se les sustrajo el saldo disponible de sus cuentas bancarias.

Este trabajo pretende develar la actuación de los cibercriminales en la sustracción de caudales económicos ajenos, así como la nueva forma de comisión de delitos informáticos como el acceso ilícito a la consulta en línea de Reniec, la suplantación de identidad ante las empresas de telefonía móvil y la banca por internet del Banco de la Nación u otra entidad bancaria.

## II. Planteamiento del problema

La búsqueda de nuevas herramientas innovativas para satisfacer diversas necesidades humanas ha propiciado que las invenciones tecnológicas como la 'banca móvil' no solo sea utilizada conforme a lo previsto por su creador, puesto que existen organizaciones criminales con finalidad lucrativa, dedicadas a la comisión de delitos informáticos, comúnmente llamados ciberdelincuentes o cibercriminales.

Estos sujetos inescrupulosos aprovechan su 'camuflaje intermitente' para suplantar la identidad de las personas, utilizando a su favor el mecanismo de reconocimiento biométrico de huella dactilar, el cual fue incorporado como sistema de seguridad por las compañías que prestan el servicio de telefonía móvil a nivel nacional.

En ese orden de ideas, se puede brindar una aproximación preliminar al lector sobre los delitos informáticos que presuntamente se estarían cometiendo, entre ellos, el acceso ilícito y la suplantación de identidad. Los cibercriminales habrían obteniendo información de sus víctimas en las fuentes de acceso público y las bases de datos de información personal distribuida en mercados negros virtuales o presenciales.

Ahora bien, luego de la obtención de los datos básicos se extraía la información complementaria de la 'consulta en línea' de Reniec, incluyendo la huella dactilar digital. Consecuentemente, se procedía con la fabricación artesanal de huellas dactilares en silicona, la cancelación y reposición del número afiliado a la banca por internet y la disposición del dinero de las cuentas de las víctimas, directamente o por medio de cuentas bancarias de testaferros, denominados por la doctrina como muleros.

## III. Estado de la cuestión

La cuestión en torno al tema propuesto remarca la nueva forma de ejecución de esta clase de delitos informáticos, su incremento tiene un campo extenso de acaparamiento en nuestro país, principalmente por la gran acogida que tienen los emporios comerciales tecnológicos de Polvos Azules y El Hueco.

El fraude de intercambio de SIM se considera una estafa ingeniosa en la que los ciberdelincuentes sustraen el número de teléfono celular de un usuario de banca en línea para extraer la contraseña válida de un solo uso, conocida como «One Time Password», así como los mensajes de seguridad que la entidad bancaria enviará al titular de la cuenta asociada al número de celular durante el desarrollo de las transacciones bancarias con el fiel objetivo de disponer el monto de las tarjetas (Jordaan y Von Solms, 2011).

Los cibercriminales aprovechan que la autentificación empleada por las entidades bancarias se concentra en la generación de tokens que persiguen el número signado al usuario, lo cual es insuficiente para la ejecución de transacciones seguras, mientras que la experiencia internacional propone como alternativa implementar la autenticación del usuario basada en la identidad del dispositivo contenido en el IMEI (Hassan y Shukur, 2021).

Luego de un agudo patrullaje virtual y consecuente seguimiento de geolocalización, la División de Investigación de Delitos de Alta Tecnología de la Policía Nacional del Perú descubrió que se utilizaban los establecimientos descritos en el párrafo anterior como centros de operación de los cibercriminales para la realización de sus delitos informáticos (América Noticias, 2021a).

Merece la pena subrayar la alerta difundida por el Organismo Supervisor de Inversión Privada en Telecomunicaciones, en adelante Osiptel, sobre la nueva modalidad denominada 'SIM swapping' o 'Suplantación de la tarjeta SIM' (Osiptel, 2021).

Esta nueva forma se suma a la enorme lista que posibilita el comportamiento delictivo en el ciberespacio para la suplantación de identidad en medios informáticos, podemos referirnos a los más conocidas, estos son, el Phishing, Smishing, Vishing y Pharming.

Con el ánimo de brindar un acercamiento académico sobre el phishing, se puede indicar que son:

> Técnicas de engaño, desde las más simples hasta las más complejas y creativas, son ejecutadas y modificadas a diario, buscando localizar puntos de ataque que permitan un mayor grado de éxito en las víctimas. Este tipo de actividad, tanto por el incremento de usuarios conectados a internet, así como también por el aumento en la utilización del sistema financiero en línea, brindan cada vez mayor cantidad de potenciales víctimas para los delincuentes informáticos dedicados a la recolección ilegítima de información privada. (Anzit et al., 2010)

A partir de ello, se infiere que es una terminación informática que confiere una modalidad de abuso informático y que para su consumación es necesaria la aplicación de un tipo de ingeniería social, cuya característica primigenia es extraer información íntima o confidencial de manera fraudulenta, entre lo más usual encontramos las contraseñas, el detalle de las tarjetas de débito o crédito y en general la información bancaria (Salvi, 2019).

En efecto, la criminalidad organizada conformada por cibercriminales intenta captar a sus víctimas mediante el envío de mensajes de correo electrónico confeccionados para engañarlos e inducirlos a consignar sus datos personales, así como el de sus cuentas bancarias.

La doctrina hace una distinción bastante atractiva. De un lado, encontramos el phishing propiamente dicho, el cual se encuentra direccionado a personas específicas, es decir, a sujetos con mayor vulnerabilidad por razones de ubicación y conocimientos informáticos. De otro lado, se puede ubicar el Spear phishing, el cual se puede diferenciar del anterior en la medida que su envío es practicado de forma genérica, sin hacer un diagnóstico previo.

En concordancia con lo descrito previamente, existe una clasificación del Phishing, esto son, el Vishing y Smishing. Ambos supuestos, exigen la intervención de un tercero que mediante el uso de las tecnologías de la información y comunicación intentan contactar a las presuntas víctimas para extraer sus datos personales y acceder a sus cuentas.

El primer escenario es el que se ejecuta a través de llamadas telefónicas, mientras que el segundo fomenta la emisión de mensajes de texto o WhatsApp, ambos tienen la finalidad de sustraer información sobre cuentas bancarias para que posteriormente de suplante la identidad de los sujetos victimados y se disponga de su patrimonio (América Noticias, 2021b).

La obtención de las claves de acceso no solo se practica por medio del phishing, sino que existe una alternativa en la que el usuario entrega su información de manera voluntaria, pero sin consentimiento. La aproximación más clara sobre el pharming fue desarrollada por (Fernández, 2011) cuando explica que:

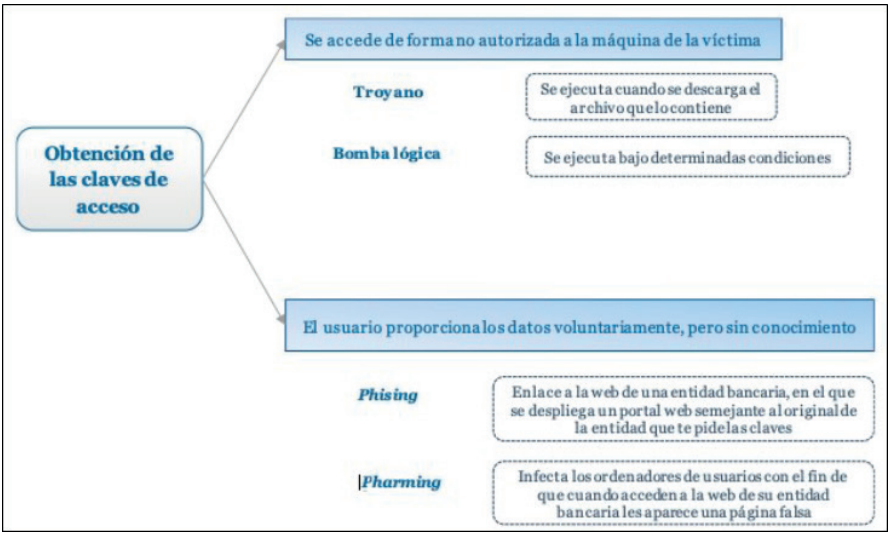
> Es una modalidad del anterior en la cual lo que se hace es infectar los ordenadores de los usuarios, con el fin de que cuando acceden a la web de su entidad bancaria les aparece la página falsa, de forma que al introducir las claves surge en la interfaz un mensaje de error y a partir de ese momento las claves del usuario ya han pasado a manos ajenas. (p. 36)

La infección que ocasiona esta última modalidad refleja una realidad cibernética alterada, induciendo a la víctima a situarse en una página oficial

aparente, lo que posibilita que con seguridad y sin desconfianza ingrese el número de tarjeta, el código de tres dígitos de la parte inferior de la tarjeta, la fecha de vencimiento y la clave secreta. Acto seguido, la página arroja un error sobre los datos ingresados y comienza la sustracción de dinero. Para mayor detalle, se agregó el siguiente organizador visual.

**Figura 2**

*La obtención autorizada sin conocimiento o no autorizada de las claves de acceso*




Nota. Información obtenida de "Los Ciberfraudes II: Análisis Avanzado de la Ciberdelincuencia Económica y Empresarial", Universidad Internacional de La Rioja, 2021, p. 13.

Conviene mencionar que, en nuestro país contamos con legislación especializada para que nuestras autoridades, principalmente la Unidad Fiscal Especializada en Ciberdelincuencia y la División de Investigación de Delitos de Alta Tecnología de la Policía Nacional del Perú, puedan enfrentar las nuevas modalidades de delitos informáticos.

El gobierno del Perú ratificó el convenio de Budapest, conocido tradicionalmente como el convenio de la ciberdelincuencia, por medio del Decreto Supremo N.° 010-2019-RE, del 10 de marzo de 2019. Se publicó en el Diario Oficial El Peruano, el 22 de setiembre de 2019 y se planteó una *vacatio legis* hasta el 1 de diciembre del mismo año (Ministerio Público Fiscalía de la Nación, 2020)

Bajo el mismo tenor, se empezaron a expedir instrumentos normativos que pretendían coadyuvar en la lucha directa y efectiva contra la cibercriminalidad, se consideró necesario incorporar al presente estudio una

tabla detallada con las normas más relevantes sobre el fenómeno objeto de análisis.

**Tabla 1**
*Instrumentos normativos nacionales e internacionales sobre ciberdelincuencia*

| Instrumento normativo | Contenido regulatorio | |
|---|---|---|
| Convenio sobre ciberdelincuencia | Artículo 2. Acceso ilícito<br>Cada parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno el acceso deliberado e ilegítimo a todo o parte de un sistema informático. Las partes podrán exigir que el delito se cometa infringiendo medidas de seguridad, con la intención de obtener datos informáticos u otra intención delictiva, o en relación con un sistema informático conectado a otro sistema informático. | |
| Ley n.º 30096 – Ley de delitos informáticos | Artículo 2. Acceso ilícito<br>El que accede sin autorización a todo o parte de un sistema informático, siempre que se realice con vulneración de medidas de seguridad establecidas para impedirlo, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días multa. Será reprimido con la misma pena el que accede a un sistema informático excediendo lo autorizado. | Artículo 9. Suplantación de identidad<br>El que, mediante las tecnologías de la información o de la comunicación suplanta la identidad de una persona natural o jurídica, siempre que de dicha conducta resulte algún perjuicio, material o moral, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años. |
| Ley n.° 30171 – Ley que modifica la Ley 30096, Ley de delitos informáticos | Artículo 2. Acceso ilícito<br>El que deliberada e ilegítimamente accede a todo o en parte de un sistema informático, siempre que se realice con vulneración de medidas de seguridad establecidas para impedirlo, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días-multa. Será reprimido con la misma pena, el que accede a un sistema informático excediendo lo autorizado. | |

*Nota*. Información obtenida del Convenio de Budapest, la Ley n.° 30096 y la Ley 30171.

Al haber asentado la consecución de ideas que respaldan el estado general de la suplantación y el acceso ilícito. Conviene exponer lo que se entiende por 'Suplantación de la tarjeta SIM', esta nueva modalidad utilizada por organizaciones criminales conformadas por delincuentes informáticos expone que se busca intensivamente "acceder a los códigos de verificación que empresas, plataformas y entidades bancarias suelen enviarnos a nuestros dispositivos móviles" (Albors, 2020, párr. 2).

En concordancia con lo anterior, "El SIM swapping es un tipo de fraude que permite a los criminales robar tu identidad mediante el secuestro del número de teléfono al obtener un duplicado de tu tarjeta SIM" (Albors, 2020, párr. 1). En nuestro país, se ha comenzado a poner en práctica dicha suplantación, esto debido a la falta de control por parte de las empresas de

telefonía al otorgar autorizaciones para la activación y reactivación de chips en lugares de dudosa procedencia.

En la misma medida, accedían a las consultas de Reniec para obtener los datos personales de las víctimas, así como sus huellas dactilares para replicarlas en silicona y comenzar con la suplantación de identidad en sus cuentas bancarias. Recientemente, se ha puesto en conocimiento de la ciudadanía que:

> ...los malhechores recopilan información personal de las víctimas (a través del phishing, apps fraudulentas, señales de wifi falsas, entre otras) como su número telefónico, y se apoderan de la línea móvil notificando a la empresa operadora de una supuesta pérdida o robo del equipo, para luego solicitar la reposición del servicio en otro chip móvil. (Osiptel, 2021, párr. 2)

Sobre la marcha, nuestras autoridades y los ciudadanos deben estar preparados para combatir conjuntamente esta nueva modalidad. Es incipiente el conocimiento que se tiene frente a las múltiples denuncias interpuestas hasta el momento. No obstante, esta situación no puede ser entendida como un obstáculo para continuar investigando y reforzando los conocimientos de las potenciales víctimas.

## IV. Metodología

El método es el camino que persigue el indagador durante el desarrollo de la investigación mediante un procedimiento elocuente con el ánimo de producir hallazgos de relevancia académica sobre un problema tangible e identificable en la sociedad (Martínez y Benítez, 2016). En relación al tipo de investigación, se denomina como socio jurídica porque expresa un fenómeno real con relevancia jurídica, tiene como principal centro de atención el funcionamiento legal e imparcial (Tantaleán, 2016).

En ese orden de ideas, se eligió el propósito básico, expresando que son consideradas ciencias puras que permiten realizar estudios profundos para la comprensión de nuevos fenómenos contenidos en las variables o categorías (Baena, 2017). En ese tenor, estas investigaciones se dirigen a revelar los cimientos básicos a través de los conceptos científicos, sirve de sostén para comenzar el análisis de los aspectos fácticos de los fenómenos (Escudero y Cortez, 2018).

Ahora bien, cabe reseñar que el enfoque elegido fue el cualitativo, en tanto que se centra en el aspecto fenomenológico por encima de la generalización, es así que su tratamiento procura ser intensivo y comprensivo (Chávez et al., 2013). A su vez, debe precisarse que este enfoque revisa la realidad dentro de su contexto real y sin condicionamiento con la intención de dotar de sentido

interpretativo a los materiales seleccionados (Rodríguez, Gil y Garcés, 1999), como se citó en (Cruz et al., 2014).

Esclarecido el escenario anterior, corresponde indicar que el diseño es el estudio de casos, esto exige que se analicen casos particulares en los que se haya plasmado el fenómeno para describirlo y detallarlo desde la perspectiva objetiva y subjetiva (Pimienta y De la Orden, 2017). En consecuencia, el nivel exploratorio "Se enfoca en descubrir información sobre un objeto de estudio desconocido" (Fernández et al., 2015). En concordancia con lo anterior, se emplea la inmersión para abordar la problemática que carece de investigaciones previas o teniéndolas no analizaron completamente dicho problema (Altuna, 2018).

## V. Resultados

La posición que hemos adoptado devela que en la actualidad existen plataformas virtuales exclusivas del Estado y excepcionalmente utilizadas por empresas privadas debidamente acreditadas, con las que se puede obtener información de la base de datos general de Reniec, la cual por ninguna razón puede ser divulgada en espacios no autorizados que pongan en peligro la seguridad informática de cada sujeto.

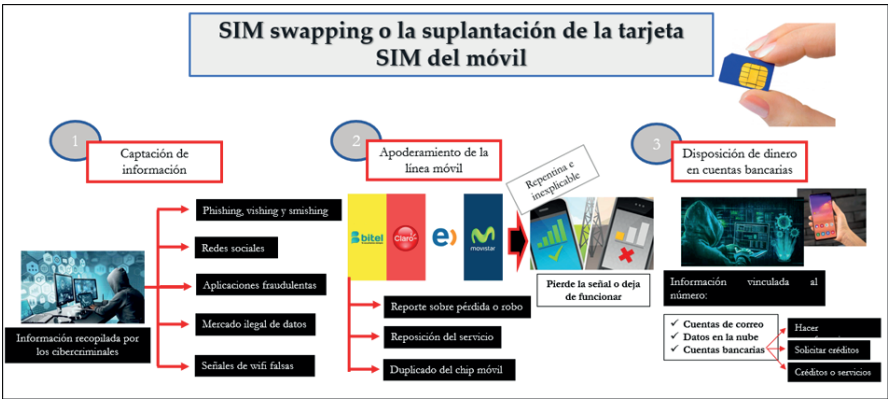
Pese a ello, en la práctica la información recopilada de fuentes de acceso abierto como lo son las redes sociales y páginas web termina siendo vendida en mercados informales y en el peor de los escenarios en la Deep Web. Situándonos en el contexto nacional, en el Centro de Lima se encuentran los puntos de venta de accesorios de cómputo en general.

Particularmente, hay jaladores que ofrecen la venta de base de datos con información pormenorizada de ciudadanos peruanos, los cuales desconocen que se ha exhibido y difundido ilegítimamente sus datos personales. Salta a la vista un amplio mercado con alta demanda de consumidores, lo que deja en evidencia la falta de cultura informática y el debido cuidado que merece nuestra intimidad.

Igualmente, para el caso de las empresas que prestan el servicio de telefonía a nivel nacional, los ciberdelincuentes han identificado diversas vulnerabilidades que han aprovechado para sacar el máximo provecho empelando la suplantación de identidad para aplicar el 'SIM swapping'.

Los cibercriminales cada vez logran sofisticar sus acciones en el ciberespacio, dejando una gran duda a la comunidad sobre el trabajo que realizan nuestras autoridades para enfrentar esta problemática. Merece tomarnos el tiempo para explicar cómo es que operan estos delincuentes informáticos, siendo ello así, se integró el siguiente organizador visual.

**Figura 3**
*Las etapas de la suplantación de la tarjeta SIM en el caso Julio César Flores*




*Nota*. Información obtenida de la "*Suplantación de identidad mediante huellas dactilares de silicona*", (Menacho, 2021)

### 5.1. Captación de información

El esquema de desarrollo de la suplantación de la tarjeta SIM, involucra tres etapas para su iniciación y consumación. Es ideal para ellos, captar toda la información que se encuentre registrada en las fuentes de acceso abierto, ya que la gente difunde no solo los acontecimientos importantes, sino aquellos que contienen información que pertenece a la esfera íntima o reservada.

Como se mencionó al inicio de la redacción del presente artículo, el phishing resulta el segundo mecanismo de captación más importante para que los integrantes de la organización cibercriminal puedan obtener los datos de las tarjetas de débito o crédito, así como el nombre completo del titular de la línea y el número vinculado a la banca online.

La información mencionada previamente también puede extraerse de las redes sociales, dado que no es extraño que la vida diaria se difunda y publique en Facebook e Instagram. Desde la proporción más mínima, hasta el conjunto de datos personales que posibiliten la individualización de la presunta víctima.

A esto debe sumarse, la descarga de aplicaciones de dudosa procedencia. Por lo general, son aquellas que se brindan en formato crack, aparentemente se pueden descargar de manera gratuita y utilizar funciones premium. Los mercados de venta ilegal de datos son los más visitados, al vulnerar los equipos inteligentes, los ciberdelincuentes acceden al almacenamiento interno y externo, en donde tradicionalmente se alojan los datos relevantes sobre usuarios y contraseñas de toda clase.

Para culminar la primera etapa, es conveniente señalar que las señales de wifi falsas se suman a las alternativas que utilizan los cibercriminales para ingresar a sus dispositivos móviles y aprovechan el tiempo de conexión para supervisar el ingreso a sus aplicativos de banca móvil por internet. Una vez que lo detectan, extraen usuarios, contraseñas e información relevante para usurpar su identidad.

### 5.2. Apoderamiento de la línea móvil

La segunda acción que realizan los ciberdelincuentes está relacionada al apoderamiento de la línea móvil. Para su ejecución identifican el número de celular de la víctima y generan el reporte de pérdida o robo.

Es conocido que los integrantes de la organización criminal cuentan con conexiones que les permite tener facilidad de acceso para reponer el servicio de una línea, gracias a los centros de reparación de celulares que fungen como fachada para cometer estos delitos informáticos.

Al tener todo listo, simplemente se comunican con la operadora de la empresa de telefonía móvil correspondiente y solicitan la reposición del servicio para proceder con la reactivación en uno de los chips nuevos con los que cuentan en el almacén.

Previamente, han realizado la réplica de la huella dactilar mediante la fabricación en silicona y sencillamente colocan el aparado de reconocimiento biométrico el dedo y debajo la huella dactilar de silicona con lo que consiguen el duplicado y reactivación de la línea.

Mientras esto sucede, la víctima afronta la pérdida de la señal o problemas con el funcionamiento del equipo, ambos son indicaciones claves que presuntamente se estaría cometiendo la suplantación de tarjeta SIM en el móvil, en tanto que los códigos de las transacciones o movimientos financieros llegarían al equipo en el que se encuentra insertado el nuevo chip.

### 5.3. Disposición de patrimonio de la banca móvil

El paso final del procedimiento empleado por los cibercriminales se circunscribe a la disposición del efectivo contenido en las cuentas de la víctima. Para que esto sea posible, el número de celular tiene que estar afiliado a la banca por internet, pues no se debe olvidar que la entidad bancaria confirma cada disposición de dinero mediante un código único e irrepetible que solo le llega al titular de la línea.

Confirmado el requisito anterior, el delincuente informático realiza una revisión sistemática sobre la información almacenada en la nube, cuentas de correo electrónico y blog de notas para acceder a cuentas y contraseñas,

ya que es muy común que los usuarios utilicen como ayuda de memoria sus dispositivos móviles.

Luego de ingresar a sus cuentas bancarias afiliadas con su número telefónico, comienzan a realizar transferencias a cuentas de testaferros, llamados por la doctrina como "Los Burros", quienes previamente han sido captados y se les ha ofrecido una suma económica para que faciliten sus números de cuenta y en ocasiones entreguen la tarjeta de débito.

Adicionalmente, pueden solicitar crédito a través de la banca por internet, sin necesidad de acudir presencialmente a la entidad bancaria. Esto se debe a la simplificación administrativa incluida por algunas de las más conocidas entidades bancarias, hasta el momento ya se han presentado casos en los que ha ocurrido lo que se intenta reseñar en la presente indagación.

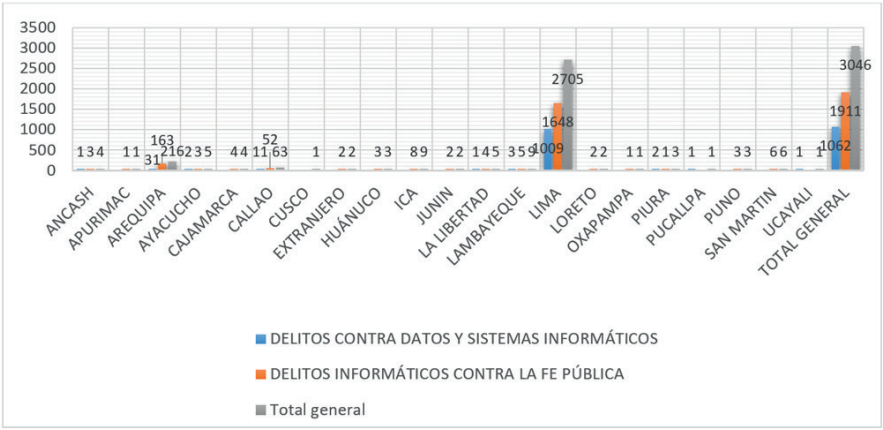
Es común que también realicen compras de bienes o servicios por medio de las plataformas virtuales, pues como se conoce al contar con el acceso a la banca por internet tenemos un sin número de posibilidades de actuar en perjuicio de la víctima. Una de las restricciones superables es el tiempo, los delincuentes informáticos podrán disponer del dinero hasta que el titular se percate y proceda a realizar la cancelación inmediata de sus tarjetas y el chip vinculado a las mismas.

## VI. Discusiones

De esta forma, se ha intentado brindar una explicación suficiente respecto al modo de actuación de los delincuentes del ciberespacio. Surgen algunas dudas sobre el nivel de especialización y actuación de nuestras autoridades, debido a que hasta el momento se desconocen cifras reales que revelen sentencias condenatorias por delitos informáticos relacionados a la suplantación de identidad, acceso ilícito o fraude informático. No cabe duda que, la Divindat está recibiendo las denuncias interpuestas por las víctimas, tal y como se muestra en la figura 4.

Los resultados demuestran que, hay un notable crecimiento de estos delitos informáticos, cuya concentración según el gráfico está situado en Lima. No debemos dejar pasar por desapercibido que las provincias también deben centrar sus esfuerzos en proteger y cautelar su información personal, tal y como se evidencia en Arequipa ya se han registrado casos con similares características a las que se ha abordado durante la redacción del artículo.

**Figura 4**
*Delitos de acceso ilícito y suplantación de identidad registrada*




*Nota*. Información obtenida de la División de Investigación de Delitos de Alta Tecnología - Divindat, 2021.

Las organizaciones cibercriminales pueden tener entre sus tribunas a hackers, quienes cuentan con conocimientos especializados en informática y que por lo general son utilizados para comprobar las vulnerabilidades de una página web. A diferencia de los crackers, pues estos últimos cuentan con los mismos o superiores conocimientos tecnológicos y tienen como principal objetivo la intrusión en sistemas informáticos.

> Estos delitos, como por ejemplo los fraudes en masa en el comercio y la banca electrónica, son llevados a cabo por bandas organizadas y tremendamente especializadas, que incorporan a sus filas a hackers con grandes conocimientos informáticos. Como es obvio, las posibilidades de delinquir se han trasladado para estas estructuras organizadas también a la red. (UNIR, 2021a, p. 29)

Los *attack vectors,* conocidos por su traducción en castellano como "vectores de ataque" son los conductos del ciberataque, dentro la protuberante lista ubicamos a la suplantación de identidad, medios extraíbles externos como es el caso de los desfasados USB, las cuentas de correo electrónico y diversas páginas web.

Surgen algunos cuestionamientos frente a la actuación del hacker en el ciberespacio, intentaremos abordar algunas reflexiones al respecto:

> Por ejemplo, un hacker que accede a un ordenador y no lleva a cabo ninguna otra conducta, sino, meramente mantenerse en el sistema, ¿podría entenderse que era esta conducta un mero descubrimiento

de secretos cuando el contenido no tenía esta consideración? ¿podría calificarse como delito contra la intimidad? (UNIR, 2021a, p. 20)

Sostenemos que el hacker antes de introducirse a un sistema informático u ordenador, debe contar con la autorización expresa de su creador o el propietario, ya que de no ser así estaríamos frente a la presunta comisión de un delito de intrusismo informático. Además, se estaría atentando la intimidad de la persona dueña del ordenador en el que se realiza la intromisión. Para entender con mayor detalle el flujo de obtención de información por parte de estos especialistas en informática, se decidió agregar el siguiente organizador visual.

**Figura 5**
*Modalidades empleadas para la captación de información*

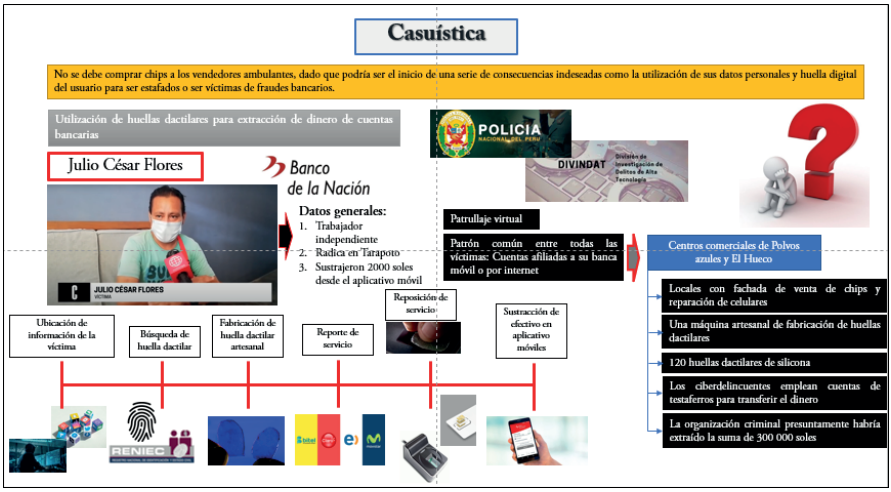

*Nota*. Información obtenida de "*Derecho Penal Informático y de la Ciberdelincuencia: El Derecho Penal Informático*", Universidad Internacional de La Rioja, 2021a, p. 20.

Como se puede observar, existe más de una forma eficiente de extraer información, así como una enorme responsabilidad por parte de los usuarios que la ventilan en fuentes de acceso abierto o llenan formularios que ofrecen algún curso gratuito o beneficio económico con la condición que se brinde la información personal del usuario.

Hagamos memoria y precisemos que para poder hacer la consulta en Reniec, es necesario que mínimamente se cuente con el número de DNI o los apellidos completos y cualquiera de los prenombres, estos son los datos que se exhiben indiscriminadamente en las redes sociales o sus semejantes.

Para demostrar nuestra postura y advertir a la ciudadanía sobre las consecuencias jurídico penales que acarrea la difusión indiscriminada de material con contenido personal, se ha analizado un caso que a nuestro criterio es emblemático porque permite describir de manera ordenada y secuencial cómo es la actuación cibercriminal, así como la respuesta de nuestras autoridades después de tomar conocimiento sobre el hecho. En esa línea de análisis, se incorporó la siguiente figura.

**Figura 6**
*Análisis del caso de suplantación de tarjeta SIM*




*Nota.* Información obtenida de la "*Suplantación de identidad mediante huellas dactilares de silicona*", (Menacho, 2021, p. 10).

El penoso episodio que afrontó el Sr. Julio Flores, probablemente refleje una situación equiparable a la de muchos otros peruanos que se percataron a tiempo y evitaron la sustracción de su patrimonio; y un grupo diferente que no logró identificarlo a tiempo y fue víctima de la suplantación de identidad del SIM.

Comencemos por explicar que, el señor Flores es un trabajador 'de a pie' como cualquier otro en nuestro país, actualmente radica en Tarapoto y se extrajeron 2000 soles de su banca móvil del Banco de la Nación. Después de haberse difundido la noticia y en paralelo la denuncia correspondiente, la

Divindat inició el patrullaje virtual para ubicar el centro de actuación de los cibercriminales.

Una de las principales características identificadas por la unidad especializada es que todas las presuntas víctimas tienen cuentas bancarias afiliadas a la banca por internet. Luego de una ardua búsqueda, se descubrieron los lugares de comisión cibercriminal, estos estaban situados en 'El Hueco' y 'Polvos Azules'.

Dichos espacios contaban con una fachada de venta de chips y reparación de dispositivos móviles, aprovechando que en esos lugares se cuenta con la máquina de reconocimiento biométrico y chips en los que se puede solicitar la reposición de la línea.

Por consiguiente, podemos contrastar las etapas de suplantación de la tarjeta SIM expuestas en párrafos precedentes, se ubicó la información del señor Flores, mediante las fuentes de acceso abierto, acto seguido se accedió ilícitamente a los servicios en línea de Reniec para realizar la búsqueda y obtener la huella dactilar.

Habiendo obtenido dicha huella se precedió a fabricarla artesanalmente para solicitar el reporte de pérdida o robo e inmediatamente la reposición del servicio, llevando a cabo todos los pasos anteriores, se dispuso por completo del patrimonio de la víctima, durante ese lapso no tuvo señal o se presentaron inconsistencias en el dispositivo móvil.

Este es uno de los tantos precedentes sobre la nueva modalidad de comisión de delitos de suplantación de tarjeta SIM. Es una obligación que los ciudadanos puedan informarse sobre las medidas de protección que deben adoptar durante la utilización de redes sociales. No debe olvidarse que en el caso que se presentó, no se aplicaron el phishing, smishing, vishing o pharming, simplemente utilizaron medios diferentes para consolidar la información obtenida de fuentes de acceso abierto.

## VII. Conclusiones

En el presente epígrafe se muestran las conclusiones arribadas por el autor, de acuerdo a la problemática identificada sobre la que se ha desarrollado la investigación. En efecto, se ha develado la nueva forma de suplantación de identidad mediante la fabricación artesanal de huellas dactilares de silicona, un acontecimiento que probablemente haya generado la duda de los lectores, pero con la integración de la casuística ha permitido contrastar la teoría con la práctica.

Es evidente que, no se puede abarcar el infinito mundo del ciberespacio y las nuevas formas de comisión de suplantación, pese a ello se ha intentado contribuir con la sociedad exponiendo la nueva conformación de las

organizaciones cibercriminales y la impunidad de su accionar debido a diferentes aspectos, principalmente las vulnerabilidades de sistemas informáticos como Reniec, la difusión indiscriminada de información personal en redes sociales y el descontrol en la reactivación de líneas por parte de las empresas prestadoras de servicios móviles.

**Primero:**

La suplantación de identidad mediante huellas dactilares de silicona se ha convertido en el nuevo medio de las organizaciones cibercriminales para la comisión de delitos informáticos, especialmente la suplantación de identidad, el acceso ilícito y el fraude informático. A su vez, se suma a la lista de los más posicionados y conocidos a nivel nacional e internacional, estos son, el phishing, vishing, smishing, pharming y el sim swapping.

**Segundo:**

La responsabilidad es atribuible tanto a las autoridades como a los usuarios, siempre que los primeros hayan realizado todas las medidas necesarias para informar y prevenir sobre las consecuencias delictivas que puede ocasionar la difusión indiscriminada de información personal. Asimismo, en el orden de ideas establecido, los segundos tendrán igual participación en caso no hayan actuado cautelosamente en aras de evitar colocarse en una situación de riesgo con la compra de chip de vendedores ambulantes o proliferando información innecesaria.

**Tercero:**

El acceso a la base de datos del Reniec es vulnerable y vulnerada por diversos usuarios con acceso directo o indirecto, quienes terminan facilitándolo a los ciberdelincuentes para que extraigan información de las víctimas y repliquen las huellas dactilares mediante la fabricación artesanal en silicona. Para ello, es suficiente con ubicar el número de DNI o un prenombre y apellidos de la persona seleccionada.

## VIII. Recomendaciones

Con el ánimo de contribuir a la optimización de algunos sistemas informáticos y brindar mayores alcances a la ciudadanía, se creyó pertinente incorporar algunas recomendaciones de naturaleza académica y práctica, las cuales permitirán reducir el índice de comisión de estos delitos y coadyuvarán a las autoridades en la lucha frontal contra la cibercriminalidad.

**Primero:**

La sociedad jurídica y el público en general deben conocer e internalizar los riesgos que supone difundir información personal en redes sociales o

fuentes de acceso abierto, en tanto que su información puede almacenarse en bases de datos informales y terminar en lugares de dudosa procedencia como son el mercado negro o la Deep Web.

**Segundo:**

El ingreso a la base de datos de Reniec, debe contar con un sistema de reconocimiento facial, similar al que se utiliza para solicitar el DNI por medio de la plataforma biofacial, de esa manera lograríamos disminuir el uso descontrolado de dicha plataforma de identificación nacional, con lo que tendríamos el reporte de los usuarios que han accedido, así como la información que han solicitado como búsqueda en el sistema informático.

**Tercero:**

Se debería restringir la venta ambulatoria de chips, para retomar el control sobre la validación dactilar en lugares autorizados que cuenten con todas las medidas necesarias que imposibiliten la suplantación de identidad, en tanto que en la práctica con las empresas con el ímpetu de incrementar las ventas y captación de usuarios, conceden autorizaciones para puntos de venta sin considerar que podrían estar contribuyendo con la suplantación de SIM.

**Cuarto:**

El uso de los aplicativos de banca móvil, debería exigir una seguridad en más de dos pasos, debido a que no basta con el código que llega al celular, sino que es necesario agregar una clave secreta creada por el titular de la cuenta bancaria, de esa manera se tendría un control más eficiente sobre las transacciones realizadas, es inevitable que exista una demora más extendida, pero considerando que está de por medio su seguridad informática, bajo una ponderación básica, es viable aplicarlo.

## Referencias bibliográficas

Albors, J. (30 de marzo de 2020). *SIM swapping: qué es y cómo funciona este fraude*. Welivesecurity. https://bit.ly/3DMUIPn

Altuna, M. (2018). *Guía de investigación científica 2018*. Universidad Privada del Norte. https://bit.ly/3xYOn2r

América Noticias. «Crímenes invisibles: Nueva modalidad de robo en la web | Cuarto Poder». Vídeo de YouTube, 10:31. Publicado el 23 de agosto de 2021a, https://www.youtube.com/watch?v=DqObK_CiPYM&t=6s

América Noticias. «Sujetos obtienen huellas digitales para suplantar identidades | Cuarto Poder». Vídeo de YouTube, 2:34. Publicado el 25 de noviembre de 2021b, https://www.youtube.com/watch?v=go-bjVcCsfM

Anzit, R., Tato, N., y Profumo, S. (2010). *El Derecho Informático - Aspectos fundamentales*. Cathedra Jurídica. https://bit.ly/33mtDWK

Baena, G. (2017). *Metodología de la Investigación*. (3a ed.). Grupo Editorial Patria. https://bit.ly/2WjnP7B

Chávez, G., Covarrubias, K., Uribe, A. (Coord). (2013). *Metodología de investigación en ciencias sociales: Aplicaciones prácticas*. Universidad de Colima. https://bit.ly/3u4Qe4p

Cruz, C., Olivares, S., y González, M. (Coord). (2014). *Metodología de la investigación*. Grupo Editorial Patria. https://bit.ly/3xYR97E

Escudero, C., y Cortez, L. (coord.). (2018). *Técnicas y Métodos cualitativos para la investigación científica*. Editorial UTMACH. https://bit.ly/3ng1SWy

Fernández, J. (2011). *Derecho penal e internet: especial consideración de los delitos que afectan a jóvenes y adolescentes*. Editorial Lex Nova.

Fernández, M., Urteaga, P., y Verona, A. (2015). *Guía de investigación en Derecho*. Pontificia Universidad Católica del Perú. https://bit.ly/3HUWjGj

Hassan, M., y Shukur, Z. (2022). Autenticación de usuario basada en la identidad del dispositivo en el sistema de pago electrónico para aplicaciones seguras de monedero electrónico. *Electronics*, 11(1). https://doi.org/10.3390/electronics11010004

Jordaan, L., y Von Solms, B. (2011). Una solución basada en biometría para combatir el fraude SIMSwap. *In Lecture Notes in Computer Science*, 6555, 70-87. https://doi.org/10.1007/978-3-642-19228-9_7

Ley 30096 de 2013. Por la cual se incorporan las normas que regulan los delitos informáticos. 22 de octubre de 2013. D. O. No. 505484. https://bit.ly/3ykN9yo

Ley 30171 de 2014. Por la cual se modifican las normas que regulan los delitos informáticos. 10 de marzo de 2014. D. O. No. 518568. https://bit.ly/3EMQMiT

Martínez, H., y Benítez, L. (Eds.). (2016). *Metodología de la investigación social I*. Cengage Learning Editores. https://bit.ly/3A7HgHI

Menacho Ortega, B., A. (2021, 10 de diciembre). *Suplantación de identidad mediante huellas dactilares de silicona* [Diapositivas de PowerPoint]. Menacho y Bernal Abogados. https://bit.ly/3rZ6UKE

Ministerio Público Fiscalía de la Nación. (2020). *"Convenio sobre la Ciberdelincuencia" permite a jueces y fiscales realizar requerimientos de cooperación internacional*. Plataforma digital única del Estado Peruano. https://bit.ly/3yiXZVh

Nicholls, J., Kuppa A., y Le-Khac, N. (2021). Ciberdelincuencia financiera: una encuesta exhaustiva de enfoques de aprendizaje profundo para abordar el panorama de la delincuencia financiera en evolución. *IEEE Access*, 9, 163965 - 163986. DOI: 10.1109/ACCESS.2021.3134076

Organismo Supervisor de Inversión Privada en Telecomunicaciones. «OSIPTEL alerta a usuarios sobre modalidad de robo de identidad y dinero usando el número móvil». Oficina de Comunicaciones y Relaciones Institucionales - OSIPTEL, 23 de agosto de 2021. https://www.osiptel.gob.pe/portal-del-usuario/noticias/osiptel-alerta-a-usuarios-sobre-modalidad-de-robo-de-identidad-y-dinero-usando-el-numero-movil/

Pimienta, J., y De la Orden, A. (2017). *Metodología de la Investigación*. (3a ed.). Pearson. https://bit.ly/3xVe2c7

Salvi, M. (2019). *El Phishing en la Argentina* [Tesis de licenciatura, Universidad Siglo 21]. Repositorio Institucional. https://repositorio.uesiglo21.edu.ar/handle/ues21/16066

Tantaleán, R. (2016). *Tipología de las investigaciones jurídicas*. Fundación Dialnet. https://dialnet.unirioja.es/servlet/articulo?codigo=5456267

Universidad Internacional de La Rioja. (2021). Los Ciberfraudes II: Análisis Avanzado de la Ciberdelincuencia Económica y Empresarial. *UNIR*. https://bit.ly/31WVbkw

Universidad Internacional de La Rioja. (2021a). Derecho Penal Informático y de la Ciberdelincuencia: El Derecho Penal Informático. *UNIR*. https://bit.ly/3pS25zQ

**Notas al final**

1 Abogado por la Universidad Privada del Norte, maestrante en Ciencias Penales por la Universidad Nacional Mayor de San Marcos y maestrante en Ciberdelincuencia por la Universidad Internacional de la Rioja - España. Lima-Perú.