FACULTAD DE DERECHO Y HUMANIDADES

ESCUELA PROFESIONAL DE DERECHO

Contribución de los medios tecnológicos en el delito informático de la suplantación de identidad en las telecomunicaciones, Jaén 2022

TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE:

Abogado

AUTORES:

Flores Machuca, Moises Alcides (orcid.org/0000-0003-3617-1154)

Uriarte Perez, Greyci Sheraldine (orcid.org/0000-0003-0787-6999)

ASESOR:

Dr. Rios Sánchez, Wilfredo (orcid.org/0000-0003-4569-3771)

LÍNEA DE INVESTIGACIÓN:

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

LÍNEA DE RESPONSABILIDAD SOCIAL UNIVERSITARIA:

Desarrollo económico, empleo y emprendimiento

TRUJILLO – PERÚ

2023

Dedicatoria

La presente tesis está dedicada a Dios, ya que gracias a él, logré concluir mi carrera, a mis padres, porque ellos estuvieron pendientes brindándome su apoyo para poder lograr este objetivo, a mi hermana también, por sus buenos deseos y a toda aquellas personas que de una u otra manera han contribuido para el logro de este objetivo.

Greyci.

Dedicada en primer lugar a Dios, por bendecirme todos los días, por iluminar mis caminos y permitirme llegar hasta esta etapa de mi vida, logrando tener tan buena experiencia dentro de mi Universidad.

A mis padres Jorge y Blanca quienes me han conducido con amor, paciencia, consejos, sacrificio y apoyo incondicional y así mismo han formado de mí una persona de bien y por darme todo lo que han podido.

A mis hermanas, por ser parte de mi vida y partícipes de mis sueños.

A mí esposa e hijos quienes constantemente han estado impulsándome día a día quienes han dado razón a mi vida para seguir adelante.

Moises.

Agradecimiento

El principal agradecimiento es a Dios quien me ha guiado todo este tiempo para poder seguir adelante.
A mi familia por su comprensión y estímulo constante, además de su apoyo a lo largo de mis estudios.
Y a todas las personas que de una u otra manera apoyaron en la realización de este trabajo.

A Dios, por permitirme la vida y la salud de todos los días, para formarme como profesional, de manera especial, a mis padres y hermanas por su apoyo, amor y sacrificio que demostraron día a día y por el profundo cariño que les profeso.
Especialmente agradezco a mi madre por su gran apoyo, por estar conmigo en momentos significativos y por su amor.
Y por último, gracias a mis amigos por su apoyo y cariño.

Índice de contenidos

Resumen

El desarrollo de investigación surge de la problemática, que se observó que en Jaén como en el Perú, el ciberdelito de suplantación de identidad teniendo como herramienta o mecanismo el uso de medios tecnológicos, no está regulado específicamente y tiene vacíos normativos, pues no están acordes a la nuevas modalidades de estos innovadores ciberdelitos, porque están complementadas con normas genéricas; así como también, se encontró que las denuncias por el delito de suplantación de identidad no proceden y son archivadas, porque existen escasos policías, profesionales y fiscales especialistas en casos de materia del ciberdelito de suplantación de identidad; por lo tanto, la investigación tiene como objetivo general, la de determinar cómo contribuyen los medios tecnológicos en el delito informático de la suplantación de identidad en las telecomunicaciones, Jaén 2022.

Para alcanzar el objetivo de estudio, se utilizó el enfoque de investigación cualitativa, de tipo básica, mediante el diseño de la teoría fundamenta, que mediante las técnicas de la revisión documental y las entrevistas realizadas a experimentados participantes, se obtuvo información relevante que ayudó a llegar a confirma el supuesto general, “los medios tecnológicos si contribuyen en el delito informático de la suplantación de identidad en las telecomunicaciones, Jaén 2022”.

Palabras clave: Delitos Informáticos, Suplantación de Identidad, Sistemas Informáticos, TIC, Phishing, Protección al Usuario.

Abstract

The development of research arises from the problem, which was observed that in Jaén as in Peru, the cybercrime of identity theft having as a tool or mechanism the use of technological means, is not specifically regulated and has regulatory gaps, since they are not in accordance to the new modalities of these innovative cybercrimes, because they are complemented with generic norms; as well as, it was found that the complaints for the crime of identity theft do not proceed and are archived, because there are few police officers, professionals and prosecutors specialized in cases of cybercrime of identity theft; Therefore, the research has as a general objective, to determine how technological means contribute to the computer crime of identity theft in telecommunications, Jaén 2022.

To achieve the objective of the study, the qualitative research approach was used, of a basic type, through the design of the fundamental theory, which through the techniques of documentary review and the interviews carried out with experienced participants, relevant information was obtained that helped to Getting to confirms the general assumption, "the technological means do contribute to the computer crime of identity theft in telecommunications, Jaén 2022".

Keywords: Computer Crimes, Identity Theft, Computer Systems, TIC, Phishing, User Protection.

I. INTRODUCCIÓN

La identidad es un derecho otorgado por el Estado para cada ciudadano, por ende, el Estado mediante la emisión y el acceso de documentos oficiales acredita el derecho a la identidad única a la población, pero en la actualidad, este derecho ha sido vulnerado por la delincuencia, que abusando la buena fe, inocencia y confianza de población, y haciendo uso indebido de la tecnología telefónica, incurre en el delito de la suplantación de identidad; este procedimiento ilegal sucede cuando a través de los medios tecnológicos telefónicos, el ciudadano acepta proporcionar información personal y confidencial a solicitud del operador telefónico, sin prever plenamente que se puede tratar de un individuo que utilice dicha información personal y confidencial para hacerse de beneficios económicos y patrimoniales, fruto del esfuerzo del ciudadano (Colectivo ARCIÓN, 2015).

La usurpación de identidad (suplantación de un titular), es una modalidad por la cual un individuo suplanta a otra persona o usuario, con el propósito de beneficiarse ilegalmente de la titularidad de un derecho u obtener beneficios por la obtención de un bien o una prestación de un servicio; el delito de suplantación de identidad se ha visto incrementado por el uso fraudulento de la información a través de los medios tecnológicos, pues las redes móviles se han convertido en una de las fuentes de alto riesgo para esta modalidad de fraude tecnológico (Gabaldón & Pereira, 2008).

Las Tecnologías de la Información y Comunicaciones (en adelante TIC) a través de la redes telefónicas móviles (redes sociales), permite a los jóvenes comunicarse de manera más rápida y oportuna; sin embargo, esta herramienta tecnológica puede usarse de manera inadecuada e imprudencial para dañar y suplantar a otras personas; la ciber victimización se presenta y se mide mediante la denigración y suplantación de identidad, con el propósito de dañar social y emocionalmente a otros individuos; pues mediante la suplantación de identidad el usuario mal intencionado puede; enviar mensajes amenazantes a otras personas haciéndose pasar por otra persona, como también publicar vídeos o imágenes denigrantes de personas, publicar burlas de otras personas, información comprometedora y confidencial haciéndose pasar por otras personas (Valdés, et al., 2018).

La criminalidad informática son actos ilícitos relativamente recientes, y que busca innovadoras formas y métodos día a día para cometer estos delitos , por lo que el derecho penal informático debe estar en permanente adaptación a este tipo de crímenes tecnológicos, pues el uso de nuevas tecnologías varían constantemente; por lo que la mayoría de las naciones en su legislación penal han incorporado normas para el uso correcto y administración de los medios tecnológicos, con el fin de reprimir las actividades mal intencionadas, ilegales y fraudulentas en el uso de los sistemas tecnológicos; el Perú ha suscrito un relevante convenio internacional en materia para combatir los ciberdelitos, que es el convenio de Budapest (2004), por lo que se promulgó la Ley Nro. 30096, la cual fue modificada mediante la Ley Nro. 30171 “Ley de Delitos Informáticos” (en adelante Ley Nro. 30171), normas legislativas incorporadas al sistema penal peruano con el propósito de que exista un ordenamiento jurídico y se adecue a los estándares internacionales estipulados en el “convenio de Budapest”; por ello en la Ley Nro. 30171 se tipificaron los delitos informáticos como ejemplo: la interceptación de datos informáticos, los atentados a la integridad de datos informáticos, la suplantación de la identidad, etc. (Leyva, 2021).

Además en el Perú se ha incrementado con más frecuencia dos (2) tipos de ciberdelitos, que son los fraudes informáticos y la suplantación de la identidad, pues un investigador egresado de la Universidad del Pacifico manifiesta que, en América latina, usuarios que utilizan medios tecnológicos digitales, se han visto expuestos al delito de suplantación de identidad en sus transacciones bancarias, según las entidades pertenecientes al sistema financiero, los tipos de ataques más frecuentes utilizados contra los clientes del sistema bancario son el phishing (modalidad de suplantación de identidad) por correo electrónico, el phishing por mensaje de texto, el phishing por llamada de voz y la infección con software malintencionados o malware (Vargas, 2021).

Según el Sistema de Denuncias de la Policía (SIDPOL), hasta julio del 2022, se vienen registrando más de 1,300 denuncias por casos de suplantación de identidad, cifra que supera las denuncias equivalentes al período de años anteriores, pues pese a que este tipo de denuncias hoy en día tienen mucha incidencia, la gran mayoría son denuncias archivadas por falta de profesionales especialistas en el caso, así como del

desconocimiento de los policías y fiscales sobre la materia de ciberdelitos (suplantación de identidad y fraudes tecnológicos); por otro lado, los suplantados deben lidiar con los perjuicios económicos, morales y sociales, porque las entidades responsables de su protección no les brindan soluciones. (Morales, 2022)

Por lo que, el problema que se encontró y la razón de realizar la presente investigación, es que se observó que en Jaén como en el Perú, el ciberdelito o delito informático de suplantación de identidad mediante el uso de medios tecnológicos (como mecanismo para cometer dichos delitos informáticos) no está regulado específicamente y tiene vacíos normativos, pues no están acordes a la nuevas modalidades de los ciberdelitos, porque están complementadas con normas genéricas; así como también se encontró que las denuncias por el delito de suplantación de identidad no proceden y son archivadas, porque existen escasos fiscales, profesionales y policías especialistas en casos de materia del ciberdelito de suplantación de identidad, y por último, se encontró también que existen deficiencias en las medidas de protección normativa de los usuarios consumidores de las telecomunicaciones frente al delito de suplantación de identidad en la ciudad de Jaén, 2022.

Por ello, se establece la siguiente interrogante como problema principal de investigación: ¿Cómo contribuyen los medios tecnológicos en el delito informático de la suplantación de identidad en las telecomunicaciones, Jaén 2022?; y como problemas específicos las siguientes incógnitas, (1) ¿ Cómo ayudan los medios informáticos en el delito de la suplantación de identidad en las telecomunicaciones, Jaén 2022?, (2) ¿De qué forma contribuyen las TIC en el delito informático de la suplantación de identidad en las telecomunicaciones, Jaén 2022?, (3) ¿Qué medidas de protección normativa tienen los usuarios de la telefonía móvil, frente al delito informático de la suplantación de identidad en las telecomunicaciones, Jaén 2022?.

Por lo que, el estudio de investigación relacionado a la problemática se justifica teóricamente, por lo que se busca generar mayor conocimiento teórico en relación al delito informático de suplantación de identidad a la población científica de investigación del derecho, así como también a la población en general, buscando generar conocimientos relacionados a las teorías modernas sobre el derecho penal y proceso

penal del delito informático y la tipificación legislativa de la suplantación de identidad digital, teorías que aportan a la generación de seguridad de la intimidad e información personal informática de las personas naturales y jurídicas ante el uso inadecuado de los medios tecnológicos; también se justifica prácticamente, pues se indagarán sobre las modalidades más comunes utilizadas por los ciberdelincuentes para ejecutar el delito informático de suplantación de identidad, para tomar conocimiento de ello y así no ser víctimas de dichos delitos, para que posteriormente teniendo conocimiento legal de sus derechos y conocimiento operativo del delito, el usuario informado pueda brindar recomendaciones y tomar medidas judiciales de amparo ante el delito de suplantación de identidad.

Por ende, el objetivo general a investigar, es la de determinar cómo contribuyen los medios tecnológicos en el delito informático de la suplantación de identidad en las telecomunicaciones, Jaén 2022; y como objetivos especificados, se tendrá en cuenta tres (3) metas, (1) Determinar cómo ayudan los medios informáticos en el delito de la suplantación de identidad en las telecomunicaciones, Jaén 2022, (2) Diagnosticar de qué forma contribuyen las TIC en el delito informático de la suplantación de identidad en las telecomunicaciones, Jaén 2022, y (3) Analizar las medidas de protección normativa que tienen los usuarios de la telefonía móvil, frente al delito informático de la suplantación de identidad en las telecomunicaciones, Jaén 2022.

De esta forma corroborar el siguiente supuesto general, “Los medios tecnológicos si contribuyen en el delito informático de la suplantación de identidad en las telecomunicaciones, Jaén 2022”; así como corroborar los siguientes supuestos específicos: (1) Los medios informáticos ayudan en el delito de la suplantación de identidad en las telecomunicaciones, Jaén 2022; (2) Las TIC contribuyen en el delito informático de la suplantación de identidad en las telecomunicaciones, Jaén 2022, y (3) Las medidas de protección normativa de los usuarios de la telefonía móvil son deficientes, frente al delito informático de la suplantación de identidad en las telecomunicaciones, Jaén 2022.

II. MARCO TEÓRICO

Internacionalmente se citó como antecedentes, a publicaciones científicas escritas en lengua hispana como extranjeras (de preferencia inglés), que a su vez fueron publicadas en diversas revistas indexadas, así como también se citó trabajos de investigación científica publicadas por diferentes universidades, las cuales procedemos a enunciarlas.

Pons (2017), manifestó que, según la Agencia Europea para la Seguridad de las Redes y de la Información (ENISA), existen 15 (quince) amenazas más relevantes utilizadas por los delincuentes cibernéticos, dentro de las cuales se tiene por ejemplo: el Malware, el uso inapropiado de las aplicaciones web, el robo de la identidad, la violación de los datos informativos, el ciber espionaje, etc.; también llego a la conclusión que, con la llegada del ciberespacio, el ambiente delincuencial se ha incrementado exponencialmente, pues con la aparición de la era de la información virtual se han visto multiplicados las oportunidades para los delincuentes cibernéticos, que buscan causar daños humanos, sociales y económicos, pues el reto esta que las naciones deben determinar estos nuevos delitos y sus penas, y que la legislación relacionada a estos delitos deben estar atentos a sus permanentes cambios tecnológicos que tienen día a día, porque de no hacerlo los delincuentes cibernéticos sacarían gran provecho de ello; deducciones que llego el autor gracias el uso de la investigación de enfoque cualitativo, utilizando el diseño de la investigación de la teoría fundamentada.

Ortiz (2019), argumentó que, el uso del internet desde dispositivos móviles hace la vida más fácil a los usuarios, pero esas facilidades se vuelven peligrosas, cuando delincuentes informáticos haciendo uso de las TIC como herramienta, infiltran programas maliciosos en sitios web o aplicaciones (en adelante APP), con el propósito sacar beneficios ilícitos o simplemente dañar a los usuarios consumidores de esos servicios; alegato que determinó la investigadora en mérito al uso del enfoque de investigación científica cualitativa, mediante la utilización de la técnica de la revisión bibliográfica; por último la autora también concluyó que, por motivo de la incompatibilidad de las leyes a nivel mundial así como la inasistencia de leyes en algunos países, y por la transnacionalización de los delitos informáticos, es decir, el

delincuente informático realiza el crimen en un país, mientras que el afectado o víctima del delito se encuentra en otro país, han generado dificultadas para combatir dichos delitos cibernéticos, generando pérdidas millonarias a los estados, empresas y usuarios.

Acosta, et al., (2020), manifestaron que, las causas principales en la activación de los delitos informáticos o ciberdelitos, están el descuido de los usuarios consumidores, las nubes de información, los e-mails y las redes sociales, siendo las más notorias el descuido y las redes sociales, las cuales están interconectadas con los dos delitos informáticos más recurrentes, que son el espionaje electrónico (que genera las acciones ilícitas como el robo de la identidad y el robo de los fondos bancarios) y los sabotajes informáticos (que generan acciones ilícitas como la interrupción de las líneas telefónicas, mediante el uso de virus); concluyeron también que, la impunidad en relación a los delitos informáticos, se da por los vacíos legales en materia de estos delitos, pues las leyes actuales carecen de relevancia y no son suficientes para atribuirles responsabilidad judicial a los infractores que comenten estos delitos cibernéticos; expresiones que llegaron los autores por el uso de la investigación cualitativa, a través del método de la revisión documentaria especializada.

Saltos (2021), argumentó que los delitos informáticos, son actitudes ilícitas cometidos por usuarios mediante el uso de medios tecnológicos, que conlleva a delitos como fraude, engaño, extorción, robo, sustitución de identidad, y otros; también concluyó que, las leyes en su país (ecuador) en relación a los delitos informáticos es generalizada, por lo que, necesita una reforma legislativa, mediante leyes específicas acorde a cada tipo de ciberdelito, las cuales deben estar en constante actualización por los cambios veloces que se producen en la tecnología y en la sociedad, con el propósito de generar seguridad a los usuarios tecnológicos que consumen redes móviles; argumentos que llego el investigador gracias al uso del método Inductivo-Deductivo, basada en la observación del fenómeno a investigar, mediante el uso de la técnica la revisión bibliográfica.

Domínguez y Vera (2022), expresaron que, en el sector de las telecomunicaciones se ejecutan la mitad de los delitos contra la propiedad intelectual

de las personas (naturales y jurídicas) en el mundo, afectándoles mayormente en el sector financiero; argumento que llego el autor mediante el uso de la metodología de investigación cuantitativa, aplicando el diseño no experimental comparativo; además el autor concluyó también que, la pandemia ha generado el uso frecuente de las TIC, por lo que, debe existir medidas orientadas la protección de las personas que encuentran en las telecomunicaciones como un espacio de emancipación económica, por ello, es crucial y fundamental fortalecer los marcos legislativos en relación a los delitos informáticos, con el propósito de generar seguridad virtual a los frecuentes consumidores de las telecomunicaciones.

Por otra parte, en cuanto a los antecedentes nacionales, se citó a los siguientes trabajos investigación científica.

Villavicencio (2014), en su estudio científico, fundamentó que, el uso de las TIC facilitan el delito de suplantación de identidad de organismo institucional o de una persona natural, como por ejemplo, crear usuarios o perfiles falsos atribuidos a personas, empresas, instituciones, mediante las redes sociales, con el propósito de defraudar, desprestigiar y/o perjudicar a los mismo o a terceros; también dentro de sus conclusiones manifestó que el delito cibernético de la suplantación de identidad esta normada en el artículo 9° de la Ley Nro 30096, la cual la tipifica como un delito de resultado, porque no basta con realizar la acción de suplantar la identidad del usuario o empresa, sino es necesario que se origine o cause un perjuicio como resultado del delito; expresiones que llego en su investigación mediante el método de investigación básica – cualitativa, utilizando la técnica de la revisión documentada.

Aldecoa (2020), argumentó que en el Perú, el delito de suplantación de identidad se ubica regulado dentro de los delitos informáticos, reconociéndose así, porque hace uso de la tecnología informática y de las telecomunicaciones para cometer el delito de la suplantación de identidad de una persona natural o jurídica, cometiendo perjuicios económicos y morales; la autora también concluyó que, el delito de suplantación de identidad en los últimos años no ha tenido regularización y modificación alguna, siendo en estos últimos años uno de delitos más ejecutados, por lo que en el Perú existe una incertidumbre legal sobre la regularización de la participación de los medios informáticos en el delito de la suplantación de identidad;

alegatos que llego la autora en su investigación, mediante el uso del método de investigación cualitativa, de tipo básica, de diseño de investigación de la teoría fundamentada, utilizando la técnica de la observación y la revisión bibliografía.

Riega, (2021), en su investigación cualitativa, de tipo descriptiva, utilizando la técnica de la revisión bibliográfica, manifestó que, en el artículo 49° del Reglamento de Conducta de Mercado del Sistema Financiero, aprobado por la Resolución SBS Nro. 3274-2017 y sus modificatorias, establece que, es responsabilidad de la empresa financiera de implementar medidas adecuadas para mitigar riesgos de delitos informáticos, con el propósito de garantizar todas la etapas del contrato electrónico celebrado entre el cliente y la empresa financiera, por lo que, las compañías financieras restringen severamente el envío de e-mails a sus usuarios, para evitar ataques con correos falsos, y estos sean suplantados, pero los delincuentes que innovan día a día sus métodos, suplantando los sitios web de las entidades financieras, con el propósito de tener acceso ilegal a las cuentas financieras y a las tarjetas de crédito de los clientes financieros; así mismo concluyeron también que, en el 2019, el Congreso de la Republica del Perú (en adelante CRP), aprobó el Convenio de Budapest, como una medida contra la ciberdelincuencia, si bien existe regularizaciones contra estos tipos de delitos, estos no están siendo completamente suficientes y eficaces para proteger a las personas (naturales y/o jurídicas) que tengan contratos electrónicos, pues el Perú está en la posición 78 de 160 estados, que tienen desarrollo digital e implementación de ciberseguridad.

Vinelli (2021), en su investigación expresó que, la comisión de una delito mediante la utilización de los medios tecnológicos (hardware o software) no configura en su totalidad un delito informático, pues para que sea catalogado un delito informático tiene que establecerse ciertas características, de lo contrario, se estaría adjudicando un delito de forma inadecuada, por ejemplo, los insultos mediante las redes sociales no es catalogado como delito informático, por otra parte, en el phishing, el delincuente suplanta la identidad de una institución financiera, copiando su página web y sus logos, con el propósito de acceder a los datos personales de la víctima, como la contraseña de acceso a su sistema financiero, y así sacar provecho y tener disposición de sus activos financieros del sujeto victima; también el investigador

concluyó que, para tener una lucha más eficiente contra los delitos informáticos, es necesario convocar a diversos Estados, con el propósito de suscribir un nuevo convenio internacional, que proponga nuevas herramientas y que estén acordes a las nuevas modalidades delictivas informáticas, pues las organizaciones criminarles están en constante evolución y perfeccionamiento; argumentos que llego el investigador, mediante el uso de la técnica de la revisión bibliográfica, enfocando la investigación cualitativamente.

Ramírez, et al., (2022), investigando a los estudiantes universitarios peruanos, argumentaron que el COVID-2019, ha obligado a los estudiantes y a las personas de todas las naciones la utilización de los medios informáticos y las TIC, de las cuales un aproximado del 16% de personas carecen de habilidades en ellas, utilizándolas de forma básica, por ello, con la expansión de la tecnología a través medios informáticos han generado ambientes ideales para múltiples maneras o formas de ejecución de ciberdelitos; a la vez los autores manifiestan también que, los delincuentes informáticos han desarrollado o evolucionado sus mecanismos delictivos tan igual o mayor al avance tecnológico, a través del uso del internet y teniendo como herramienta los medios tecnológicos, es por ello, que se convierten en amenazas, porque los delincuentes cibernéticos desafían a los derechos legales existentes, porque no están acordes a la tecnológica emergente.

De lo anterior, y basándose en los argumentos y deducciones citadas por los investigadores y/o autores nacionales e internacionales en la presente investigación, se podría acotar que, la problemática del delito informático de la sustitución de identidad, es que no se enfoca el problema en conjunto, es decir, los usuarios, los consumidores, las empresas, las organizaciones, las instituciones, y dentro de ellas la más relevante, los gobiernos, no coordinan ni trabajan todos en forma conjunta, para tomar medidas sociales y más que todo legales, para contrarrestar la amenaza creciente e innovadora de la sustitución de identidad informática, así como también, dentro de las leyes que existen y que están vigentes, se argumenta que no son suficientes y eficaces, para el tratamiento judicial contra la lucha ante los delitos informáticos, por lo que se alega también que, no hay legislación que sea resultado

del trabajo en conjunto de las Naciones y de los usuarios (personas naturales y jurídicas) que interactúan en las telecomunicaciones.

Por motivos de la pandemia del Coronavirus, en estos últimos años, los delitos con mayor auge y mayor repercusión de ejecución, han sido los delitos informativos, que se definen como, actos cometidos por usuarios con amplio manejo de los medios tecnológicos, que vulneran virtualmente el patrimonio de las personas, así como su identidad (Villavicencio, 2014).

Los delitos informáticos también se definen como, el conjunto de acciones ilícitas o desarrollo de crímenes a través de los sistemas informáticos, es decir, utilizan los medios tecnológicos para extender y desarrollar de manera exponencial sus actos criminales, así también, hacen uso de la tecnología para su evolución delictiva constante (Núñez & Carhuancho, 2020).

Es por ello, se dice que, la evolución de la cantidad y metodologías utilizadas en los delitos informáticos es proporcional al aumento de los usuarios que consumen o se afilian a los servicios que proporcionan los medios tecnológicos.

Los delitos informáticos se caracterizan:

- Solo un número específico de individuos con ciertos conocimientos técnicos puede cometer los delitos.
- Se realizan cuando la persona está laborando o ejecutando un trabajo.
- Aprovechan una ocasión creada en el campo de las funciones y organizaciones del sistema tecnológico y económico.
- Provocan déficit económico a las personas.
- Pueden cometerse en milésimas de segundos y sin estar presentes físicamente.
- Los autores del delito actúan de forma anónima.
- Son sofisticados y relativamente frecuentes en el ámbito militar.
- Existe dificultad para su comprobación.
- Son dolosos o intencionales, así como culposos o imprudenciales.
- Se comenten mayormente a los menores de edad.
- Proliferación.
- Se repiten continuamente en el tiempo, se perfeccionan con la acción u omisión.
- Puede afectar a varios bienes jurídicos y a varios sujetos pasivos.

- Son transfronterizos, pueden tener efecto en varios países. (Espinoza, 2018).

En los delitos informáticos, existe 2 (dos) tipos de usuarios, el sujeto activo, que es cualquier persona con dominio de los medios tecnológicos (medios informativos, TIC, medios audiovisuales), y el sujeto pasivo, que también es cualquier persona natural o jurídica (entidades gubernamentales o privadas), la cual es la víctima del hecho delictivo (Espinoza, 2018).

Los delitos informativos, inicialmente se encontraban tipificados en el Capítulo I, del Título V (delitos contra el patrimonio), en el artículo 186°, inciso 3 del Código Penal Decreto Legislativo Nro 635, publicado y emitido el año 1991, siendo considerado como un agravante del delito de hurto (hurto electrónico), la que sería corregida el año 2009 mediante la Ley Nro 27309, ley que modificó el Título V, insertando el Capitulo X, denominado “Delitos Informáticos” introduciendo 4 (cuatro) artículos.

- Articulo N° 207-A: Interferencia, acceso o copia ilícita contenida en base de datos.
- Articulo N° 207-B: Alteración, daño o destrucción de base de datos.
- Articulo N° 207-C: Circunstancias cualificantes agravantes.
- Articulo N° 207-D: Tráfico ilegal de datos. Codigo Penal D.L. N° 635 (1991)

Las tipificaciones realizadas a los delitos informáticos en el Código Penal Decreto Legislativo Nro 635 del año 1991, fueron derogadas el 22 de octubre del 2013, mediante la Ley Nro 30096, “Ley de Delitos Informáticos” (en a delante Ley Nro 30096), la que actualiza la tipificación e incorpora nuevos delitos informáticos, ley que a su vez fue modificada mediante la Ley Nro 30171, con el propósito de adecuar el ordenamiento jurídico peruano a los estándares normativos internacionales estipulados en el Convenio de Budapest.

Ahora bien, no es objetivo del presente trabajo de investigación tratar, estudiar y analizar la problemática de todos los delitos informáticos que están regulados en el ordenamiento jurídico peruano, si no se tratara, estudiara y analizara un delito en particular, el delito informático denominado “Suplantación de Identidad”, la cual se encuentra tipificado en el artículo 9° de la Ley Nro 30096.

El delito de suplantación de identidad, es cuando mediante el uso de los medios tecnológicos, un usuario se hace pasar o usurpar la identidad de otra persona o

institución, acto ilícito que puede ocasionar problemas a una víctima, como perjudicarla económicamente, moralmente y socialmente, CRP, Ley Nro 30096, (2013).

El delito de suplantación de identidad, también conocido como usurpación de identidad, se define también como una modalidad por la cual un individuo suplanta a otra persona o usuario, con el propósito de beneficiarse ilegalmente de la titularidad de un derecho u obtener beneficios por la obtención de un bien o una prestación de un servicio; el delito de suplantación de identidad se ha visto incrementado por el uso fraudulento de los medios tecnologías de información, pues las redes móviles se han convertido en una de las fuentes de alto riesgo para esta modalidad de fraude tecnológico (Gabaldón & Pereira, 2008).

Los ciberdelitos que pueden ser derivados de la suplantación de identidad, y que pueden ser realizados por los delincuentes informáticos son:

- Clonación de tarjetas de débito y crédito.
- Falsificación y alteración de documentos.
- Trata de personas.
- Tráfico de indocumentados.
- Tráfico de menores.
- Fraude especifico.
- Evasión a la Justicio.
- Usurpación de funciones.
- Terrorismo Colectivo, ARCIÓN (2015).

Por ello, si se usurpa la identidad mediante medios tecnológicos de una organización institucional o de persona natura, con el fin de dañarlo, económicamente, socialmente y moralmente, por la comisión del delito se sancionaría con pena privativa de libertad no menor a tres ni mayor a cinco años.

En el párrafo anterior, se menciona como fuente de delito a los medios tecnológicos, que se definen como, recursos o fuentes que hacen uso de la tecnología o la informática, para poder cumplir un propósito o tarea estipulada por un usuario (Flores, 2020).

Pues a finales de los sesenta del siglo pasado, para ser preciso en el año 1969, con la creación del internet, se dio a inicio a una revolución tecnológica que ha

abarcado y seducido su consumo a diferentes usuarios de todo el mundo, en especial a los adolescentes y jóvenes, promoviendo así el desarrollo y la masificación de nuevos e innovadores aparatos tecnológicos, como teléfonos inteligentes, tablets, computadoras personales, etc, generando una interacción global de comunicación e intercambio de datos entre usuarios a través de los medios tecnológicos (Arab & Díaz, 2015).

Los medios tecnológicos tienen diferentes clasificaciones por diferentes autores, pero para efectos de la investigación solo tomaremos 2 (dos) clasificaciones, los medios informáticos (sistemas informáticos) y las tecnologías de la información y comunicación (TIC).

Cuando se habla de los medios informáticos o sistemas informativos, se hace referencia a los procesadores de cómputo, sus programas y softwares, porque son un conjunto de dispositivos que forman parte de un sistema de cómputo o de dispositivos móviles, capaces de realizar de manera automática e intangible una serie de operaciones, así como procesos a tiempo real o diferido (Sepúlveda, et al., 2008).

Por otro lado, las TIC están relacionadas estrechamente al uso del internet, y se definen como, un conjunto de instrumentos, fuentes de procedimientos y técnicas para el proceso, almacenamiento y transmisión de la información, con el propósito de optimizar la comunicación humana (Pinargote & Cevallos, 2020).

Uno de los métodos de estafa cibernética relacionada a la suplantación de identidad, es el phishing, que es una modalidad de ingeniera social, que utilizan los delincuentes cibernéticos para obtener información confidencial de las personas de manera fraudulenta y así usurpar la identidad de estos usuarios; por ejemplo, dentro de los métodos usados por los cibercriminales para ejecutar el phishing están, el envió de e-mails maliciosos, el envió de SMS maliciosos, descarga de APPs maliciosas, mensajes maliciosos en WhatsApp, ataque a las redes sociales, etc, acciones que hacen los cibercriminales, mayormente con el propósito de acceder a información confidencial financiera, para vaciar las cuentas de las víctimas y robar el dinero que tienen (Dextre, 2022).

Una nueva modalidad de suplantación de identidad informática es el SIM Swapping, donde el delincuente informático busca la forma de duplicar la tarjeta SIM

de un usuario, con el propósito de suplantar su identidad y acceder a sus cuentas bancarias y redes sociales vinculadas a su dispositivo móvil; por lo que, para prevenir dicha modalidad de delito informático, las personas no deben de proporcionar datos personales en llamadas, e-mails o SMS, no deben de vincular sus cuentas bancarias a sus dispositivos móviles, no deben de brindar el código PIN a nadie, no deben de descargar APPs de dudosa procedencia y deben de borrar redes sociales que no utilicen (Redacción Gestión, 2022).

Por ello, el Estado para contrarrestar el avance y el crecimiento del delito informático de la suplantación de identidad, ha tomado muchas medidas, dentro de las cuales están las normas que protegen al usuario consumidor, las cuales se definen como, el conjunto de medidas normativas y legislativas que el Estado adopta, con el propósito de proteger a los usuarios consumidores, cautelando la capacidad adquisitiva de ellos, así como también, el de velar la seguridad frente a las contrataciones de bienes y servicios que realicen con el propósito de satisfacer sus necesidades (Durand, 2010).

III. METODOLOGÍA

La investigación cualitativa, no hace uso de las variables como en las investigaciones cuantitativas, la investigación cualitativa se centra en el estudio del porque o del como ocurre el fenómeno de investigación, a través del análisis de los significados, definiciones, percepciones, pensamientos y experiencias, la investigación cualitativa acopia datos informativos mediante fotografías, observaciones, entrevistas y revisiones bibliográficas. (Loayza, 2020)

Por ello, el enfoque de investigación que tuvo el presente estudio, fue cualitativo, pues mediante la técnica de la revisión bibliográfica y la técnica de ejecución de entrevistas, se realizó un análisis legal sobre el porqué de la problemática formulada, con el propósito de determinar normativamente cómo contribuyen los medios tecnológicos en el delito informático de la suplantación de identidad en las telecomunicaciones, Jaén 2022.

3.1. Tipo y diseño de investigación

En el presente estudio, se adoptó el tipo de investigación básica, pues la investigación básica o investigación pura, teórica o dogmática, tiene con fin primordial y general el de incrementar los conocimientos científicos, sin constatarlos con ningún aspecto práctico (Muntané, 2010).

Por lo tanto, el diseño de investigación acopiado fue la de la Teoría Fundamentada, por lo que se requiere fundamentos teóricos del planteamiento del problema y posibles soluciones, por ello, necesariamente se requiere la revisión bibliográfica del marco teórico previo (Páramo, 2015).

3.2. Categorías, subcategorías y matriz de categorización

Para efectos de aplicación de la presente investigación se plantío como categoría (1) al **delito informático de la suplantación de identidad,** que es una modalidad por la cual un individuo suplanta a otra persona o usuario, con el propósito de beneficiarse ilegalmente de la titularidad de un derecho u obtener beneficios por la obtención de un bien o una prestación de un servicio; el delito de suplantación de identidad se ha visto incrementado por el uso fraudulento de los medios tecnologías

de información, pues las redes móviles se han convertido en una de las fuentes de alto riesgo para esta modalidad de fraude tecnológico (Gabaldón & Pereira, 2008).

Como consecuencia de la categoría (1), se derivaron dos subcategorías, el Phishing y las normas de protección a los usuarios, que conceptualmente se describen como:

El Phishing se define como, una modalidad de ingeniera social, que utilizan los delincuentes cibernéticos para obtener información confidencial de las personas de manera fraudulenta y así usurpar la identidad de estos usuarios; acciones que realizan los cibercriminales, mayormente con el propósito de acceder a información confidencial financiera, para vaciar las cuentas de las víctimas y robar el dinero que tienen (Dextre, 2022).

Normas de protección al usuario, que se define como, el conjunto de medidas normativas y legislativas que el Estado adopta, con el propósito de proteger a los usuarios consumidores, cautelando la capacidad adquisitiva de ellos, así como también, el de velar la seguridad frente a las contrataciones de bienes y servicios que realicen con el propósito de satisfacer sus necesidades (Durand, 2010).

Por otra parte, se tomó como categoría (2) a los **medios tecnológicos**, que son recursos o fuentes que hacen uso de la tecnología o la informática, para poder cumplir un propósito o tarea estipulada por un usuario (Flores, 2020); y que dentro de sus amplias clasificaciones tiene a los medios informáticos y las TICs; por lo tanto, a dichas clasificaciones se consideraron como subcategorías de la categoría (2) las cuales teóricamente se definen como:

Los medios informáticos o sistemas informativos, se hace referencia a los procesadores de cómputo, sus programas y softwares, porque son un conjunto de dispositivos que forman parte de un sistema de cómputo o de dispositivos móviles, capaces de realizar de manera automática e intangible una serie de operaciones, así como procesos a tiempo real o diferido (Sepúlveda, et al., 2008).

Las TIC están relacionadas estrechamente al uso del internet, y se definen como, un conjunto de instrumentos, fuentes de procedimientos y técnicas para el proceso, almacenamiento y transmisión de la información, con el propósito de optimizar la comunicación humana (Pinargote & Cevallos, 2020).

3.3. Escenario de estudio

El escenario de estudio, donde se realizó la investigación fue en la región de Cajamarca, provincia y distrito de Jaén, donde radican los especialistas que con su amplia experiencia participarán en la presente investigación mediante la técnica de la entrevista, de los cuales se recopiló información relevante que ayudo a resolver la problemática de estudio; ¿Cómo contribuyen los medios tecnológicos en el delito informático de la suplantación de identidad en las telecomunicaciones, Jaén 2022?; cabe aclarar que la institución más relevante donde se aplicó la mayoría de los instrumentos de investigación, fue en las instalaciones del Ministerio Publico – Fiscalía de la Provincia de Jaén, ambiente de estudio donde se aplicó la técnica de investigación de la entrevista a participantes con años de experiencia que conozcan sobre el tema relacionado a las categorías de la presente investigación, con el propósito de corroborar el supuesto propuesto, así también se aplicó la técnica de la entrevista en las instalaciones de la Policía Nacional del Perú, con el propósito ya explícito en líneas anteriores.

3.4. Participantes

La población de investigación será no probabilística, puesto que es de enfoque cualitativo, por ende, la población será finita, pues la población finita, es el conjunto de personas, donde se preestablece el número exacto de participantes, que aportan información empírica y documental del universo de estudio de investigación (Cabezas, et al., 2018).

Por lo cual, en la investigación la población fue determinada de manera intencional y finita, pues se consideró la cantidad exacta de ocho (8) participantes y/o especialistas, seis (6) participantes de profesión de abogacía y dos (2) participantes que tienen la profesión de ingenieros de sistemas; escogidos como participantes de investigación, porque cuentan con experiencia en la rama del derecho penal (abogados) y en casos de delitos informáticos (abogados e ingenieros) en la ciudad de Jaén y zonas aledañas, de los cuales se recolectó información pertinente y relevante que están relacionados a los objetivos y supuestos de investigación.

- Entrevistado 1, de profesión Abogado, Fiscal Provincial Penal, con más de 10 años de experiencia.
- Entrevistado 2, de profesión Abogado, Estudio Jurídico Rodríguez & Flores, con 25 años de experiencia.
- Entrevistado 3, de profesión Abogado, Estudio Jurídico Barrantes, con 22 años de experiencia.
- Entrevistado 4, de profesión Abogado, Asesoría y Consultoría Mego & Abogados EIRL, con 18 años de experiencia.
- Entrevistado 5, de profesión abogado, Estudio Jurídico Valera & Ortiz, con 10 años de experiencia.
- Entrevistado 6, de profesión abogado, Asesora Jurídica, con 6 años de experiencia.
- Entrevistado 7, de profesión Ingeniero Informático y de Sistemas, Unidad de Sistemas y Soporte Tecnológico, con 14 años de experiencia.
- Entrevistado 8, de profesión Ingeniero de Sistemas, Oficina de Tecnologías de la Información, con 10 años de experiencia.

Además se tomó lo siguientes criterios:

Criterios de Inclusión

- Profesión : Abogados e Ingenieros, con experiencia y/o relación en derecho penal y en delitos informáticos.
- Experiencia : Con experiencia superior a los cinco (5) años
- Nacionalidad : peruana.

Criterios de Exclusión

- Especialidad : No tengan experiencia y/o relación en derecho penal y en Delitos informáticos.
- Experiencia : No cuente con experiencia relevante en el tema de estudio superior a los cinco años

- Nacionalidad : personas de otra nacionalidad

3.5. Técnicas e instrumentos de recolección de datos

La entrevista es un técnica ventajosa para los estudios de investigación cualitativo – descriptivo, que consiste en un dialogo o conversación, donde interactúa la realización de interrogantes y la manifestación de respuestas, que tiene como objetivo primordial la de recopilar información relevante de los participantes, fundamentadas en sus percepciones (Fernández, 2018), por ende se aplicó dicha técnica, mediante el instrumento de la guía de entrevista, para lo cual se utilizó herramientas como: grabadoras, filmadoras, celulares, lápiz, lapiceros y papel.

Por otro lado, la revisión bibliográfica es un método que acerca al investigador científico a conocer un tema en general o especifico en investigación, pues es una búsqueda o indagación bibliográfica (artículos, documentos, escritos) de publicaciones manifestada alrededor del mundo. (Goris, 2015), por ello, también se aplicó la técnica de la revisión bibliográfica, mediante el instrumento del análisis documental, para lo cual se analizó publicaciones en: revistas indexadas, tesis de investigación de pregrado y posgrado, normas legislativas y periódicos de renombre; análisis documental que se ejecutó de acuerdo a los objetivos de la presente investigación, por ello, se utilizará herramientas como: internet y repositorios documentales.

3.6. Procedimiento

Los procedimientos de acopio de información estarán relacionados al tipo de investigación escogido en la presente estudio científico, que es de enfoque cualitativo, de tipo básico, de diseño de la teoría fundamenta, y a su vez estará también, relacionado a la problemática propuesta, por lo que primero se utilizó la técnica de revisión bibliográfica, con el propósito de recolectar información de publicaciones científicas internacionales y nacionales (priorizando publicaciones de los últimos siete años), donde se acopió teorías, definiciones, objetivos, antecedentes, argumentos y conclusiones de artículos de revistas indexadas, tesis de investigación, normas y leyes, que ayudaron a fundamentar y aclarar los objetivos y supuesto de la presente tesis investigación.

Se desarrolló también, la técnica de la entrevistas, mediante la guía de entrevistas, las cuales antes de aplicarse, fueron validadas por expertos relacionados al tema de investigación, posteriormente fueron aplicadas en los participantes, con el propósito de captar información importante y optima que facilite determinar y argumentar el supuesto de investigación, es decir, corroborar si los medios tecnológicos contribuyen en el delito informático de la suplantación de identidad en las telecomunicaciones, Jaén 2022.

3.7. Rigor científico

El presente estudio cualitativo cumplirá con varias criterios de investigación como, **credibilidad**, porque se acopió manifestaciones y argumentos confiables de investigadores científicos, así como también, se recolectó acotaciones relevantes de los participantes de la investigación en merito a su experiencia laboral y a sus capacidades; asimismo se tuvo en cuenta también que, la información que se acopio cumpla con el criterio de **imparcialidad**, porque se recolectó y analizó la información, así también, se determinó conclusiones y recomendaciones relacionadas a la realidad problemática y al planteamiento del problema sin alusiones o beneficios personales de los investigadores (Arias & Giraldo, 2011).

Por otro lado, también se cumplió con el criterio de **validez,** porque las fuentes de información, las técnicas e instrumentos de investigación son auténticas, y fueron validados por expertos de la rama del tema a investigar (Plaza, Uriguen, & Bejarano, 2017); por lo tanto, también se cumplió con el criterio de **confiabilidad,** porque las técnicas e instrumentos utilizados al ser validados, proporcionan que los resultados, conclusiones y recomendaciones de la investigación generen mayor confianza (Manterola, et al., 2018).

Por último, para el análisis de dato, se cumplió con el criterio de **triangulación**, porque mediante la comparación e interpretación de las diferentes fuentes de información, se tuvo una síntesis conjunta de todos los datos recolectados (Okuda & Gómez, 2005).

3.8. Método de análisis de datos

El análisis de datos de una investigación cualitativa se caracteriza por su forma cíclica, a comparación de forma lineal que adopta el análisis de información de una investigación cuantitativa. (Spradley, 1980)

El análisis de datos cualitativos, son procedimientos en el cual se analiza e interpreta teorías, se manifiesta conclusiones de los datos recolectados de las fuentes de información, las cuales fueron estructuradas para dicho propósito. (Rodríguez, et al., 2005).

El análisis de contenido, es una técnica que mediante el instrumento de codificación o categorización de un meta-texto analítico, se puede sintetizar los procesos de información (Fernández, 2002).

Por lo tanto, la presente investigación utilizó para el análisis de datos de la información recopilada en las entrevistas como en la revisión bibliográfica, la técnica de análisis de contenido, por lo cual se usó el instrumento de categorización, mediante el cuadro de convergencia y divergencias.

3.9. Aspectos éticos

El presente estudio de investigación científica se redactó en mérito a los parámetros estipulados en la “Guía de Elaboración de Productos de Investigación de Fin de Programas” de la Universidad Cesar Vallejo”, la cual fue aprobada el 05 de abril del 2022, en el ARTÍCULO PRIMERO de la RESOLUCIÓN DE VICERRECTORADO DE INVESTIGACIÓN N° 110-2022-VI-UCV; también se respetara los derechos de creación intelectual, es decir, los derechos de autor, los cuales se citaron mediante paráfrasis y de acuerdo a las Normas APA Séptima Edición, por lo cual para constatar que no existe plagio, la presente investigación se filtrara mediante el software TURNITIN; además, se tendrá el criterio ético de la conformidad, pues al momento de interpretar la información recolectada, para que posteriormente generar la discusión de investigación, se respetara la originalidad las fuentes de investigación.

IV. RESULTADOS Y DISCUSIÓN

Los resultados recolectados en el presente estudio de investigación científico, se analizaron y trabajaron con el fin de absolver el problema y la realidad problemática de investigación, como también, la finalidad de absolver el objetivo general y los objetivos específicos de investigación; los resultados hallados, están fundamentados en datos informativos recopilados mediante la herramienta cualitativa guía de entrevista, aplicada a participantes profesionales expertos, que basados en sus experiencias en el derecho penal, procesal penal, sistemas de penas y medios tecnológicos, así como también, en sus experiencias de acuerdo a sus funciones laborales, se obtuvieron respuestas destacadas para comprobar el supuesto general.

Supuesto general: los medios tecnológicos si contribuyen en el delito informático de la suplantación de identidad en las telecomunicaciones, Jaén 2022.

Objetivo general: Determinar cómo contribuyen los medios tecnológicos en el delito informático de la suplantación de identidad en las telecomunicaciones, Jaén 2022.

Interrogantes y respuestas, relacionadas al Objetivo General: Determinar cómo contribuyen los medios tecnológicos en el delito informático de la suplantación de identidad en las telecomunicaciones, Jaén 2022.

Por lo que se efectuó las siguientes interrogantes:

1. ¿Conoce usted que es el delito de suplantación de identidad?, comente su respuesta**.**

Del análisis de contenido, a través del instrumento de categorización detallado en la Matrix de Convergencias y Divergencias, se destacan los siguientes argumentos convergentes.

Entrevistado 1 (2023), argumentó que, es un delito mediante el cual el sujeto activo se apropia de la identidad de una persona natural o jurídica, se comete utilizando las tecnologías.

Entrevistado 2 (2023), argumentó que, es un delito donde un individuo suplanta el derecho de identidad de otra, causándole perjuicio económico y moral, está regulado en el Código Penal.

Entrevistado 3 (2023), argumentó que, es un delito donde una persona usa las tecnologías para hacerse pasar por otra persona.

Entrevistado 4 (2023), argumentó que, es un delito por el cual se suplanta la identidad de una persona natural o jurídica, siempre que dicha conducta resulte en algún perjuicio.

Entrevistado 5 (2023), argumentó que, es un delito que consiste en usurpar la identidad de una persona, ocasionándole daños, utiliza los sistemas informativos.

Entrevistado 6 (2023), argumentó que, es un delito que radica en hacerse pasar por otra persona, este tipo de delitos estarían normados en el Código Penal Peruano, existen delito de suplantación de identidad tanto en materia electoral como en materia informática, Artículo 9 de la Ley Nº 30096.

Entrevistado 7 (2023), argumentó que, es un delito donde las acciones de una persona tiene el fin de apropiarse de la identidad de otro individuo, para obtener beneficios ilícitos de dicho acto; por lo general estos tipos de actos se realizan digitalmente, mediante el uso de la tecnología.

Entrevistado 8 (2023), argumentó que, es un delito que consiste en utilizar la identidad de otra persona sin su autorización y con fines ilícitos.

Por ende, y sintetizando las respuestas de los participante de investigación, se deduce primariamente que, la suplantación de identidad es el delito donde un usuario activo realiza o ejecuta acciones para apropiarse del derecho de la identidad de otra persona natural o jurídica (usuario pasivo) sin su autorización, con el fin de obtener beneficios ilícitos por dicho acto, así también generando al suplantado, perjuicios económicos y/o morales, por lo general estos tipos de delitos se realizan digitalmente, mediante el uso de la tecnología informática, además este tipo de delitos esta normados en el Código Penal Peruano, Artículo 9 de la Ley Nº 30096.

2. ¿En el ámbito de su experiencia profesional, conoce que modalidades más comunes ejecutan los delincuentes para cometer el delito de suplantación de identidad?, comente su respuesta**.**

Entrevistado 1 (2023), argumentó que, los delitos de suplantación más frecuentes son, el Fraude en el sistema financiero, como compras online, y transferencias bancarias; el ciberbullying y el grooming, que consiste en ganar la confianza de un menor y cometer abuso sexual y acoso sexual contra la persona.

Entrevistado 2 (2023), argumentó que, los delitos de suplantación más frecuentes son, la suplantación en el uso de las redes sociales y la suplantación en el teléfono celular.

Entrevistado 3 (2023), argumentó que, el delito de suplantación más frecuente es, la suplantación del usuario en las telecomunicaciones.

Entrevistado 4 (2023), argumentó que, los delitos de suplantación más frecuentes son, el fraude financiero (compras en línea, transferencias bancarias, etc), el acoso sexual y la estafa.

Entrevistado 5 (2023), argumentó que, los delitos de suplantación más frecuentes son, la suplantación de tarjetas bancarias (débito o crédito), el envió de links, para extraer información del sujeto agraviado, para posteriormente sacar dinero de las cuentas bancarias o hacer compras en línea.

Entrevistado 6 (2023), argumentó que, el delito de suplantación más frecuente es, la creación de cuentas falsas en redes sociales.

Entrevistado 7 (2023), argumentó que, el delito de suplantación más frecuente es, el phishing, a través emails recepcionados, ingresos a páginas peligrosas y/o llamadas telefónicas, donde roban información personal y financiera para suplantar.

Entrevistado 8 (2023), argumentó que, los delitos de suplantación más frecuentes son, el SIM swapping, o la suplantación de la tarjeta SIM del móvil, para fraudes telefónicos y el phishing, fraude en línea, robo de identidad en redes sociales, entre otros.

Del análisis de contenido, a través del instrumento de categorización detallado en la Matrix de Convergencias y Divergencias, se destacan los siguientes argumentos convergentes y divergentes.

- El phishing, delito de suplantación de identidad, haciendo uso del internet, a través del envió de emails malintencionados, ingreso a paginas peligrosas, envió de link maliciosos y llamadas telefónicas, con el propósito de extraer datos de sujeto agraviado, para suplantación de tarjetas de débito y crédito, compras online, transferencias financieras, robo de identidad en las redes sociales, etc (Entrevistado 1, 4, 5, 7 y 8).
- El swanpping, suplantación y duplicación de la tarjeta SIM del celular móvil, con la finalidad de realizar fraudes telefónicos, suplantación en las redes sociales, acceso a la información de la banca móvil de los celulares, para fraudes financieros (Entrevistado 2, 3 y 8).
- El grooming, delito por el cual se adopta la identidad de otra persona, para cometer acoso sexual y abuso sexual a terceros, mayormente a menores de edad. (Entrevistado 1 y 4).
- El ciberbullying (Entrevistado 1).

En consecuencia, y sintetizando las respuestas de los entrevistados, se deduce que, los ciberdelitos de suplantación de identidad más comunes en la provincia de Jaén y zonas aledañas, son el phishing y el swanpping, delitos que hacen uso frecuente de sistemas informáticos y las TIC, con el propósito de cometer fraudes financieros, suplantación en redes sociales, desfalco de tarjetas financieras, etc; otros delitos comunes, pero en menor escala, son el grooming y el ciberbullying, que también hacen uso frecuente de los medios tecnológicos; delitos realizados a través del mal uso del internet, mediante el envió de emails malintencionados, ingreso a páginas web peligrosas, envió de link maliciosos, así también, a través de la clonación de tarjetas SIM móviles, llamadas telefónicas falsas, etc.

6. ¿Mencione usted a su criterio profesional, si los medios tecnológicos contribuyen a cometer el delito informático de suplantación de identidad?, comente su respuesta**.**

Entrevistado 1 (2023), argumentó que, sí, porque muchas los medios tecnológicos permiten la encriptación de información personal y no se puede identificar el dominio o IP responsable de los hechos delictivos.

Entrevistado 2 (2023), argumentó que, los medios tecnológicos no, sino que es la mala voluntad del ser humano al querer enriquecerse y aprovechar de los medios tecnológicos para su beneficio.

Entrevistado 3 (2023), argumentó que, sí, porque utilizan generalmente el escáner para los documentos (medios o sistemas informáticos).

Entrevistado 4 (2023), argumentó que, sí, porque permiten a los delincuentes tener acceso con facilidad a la información personal, así también, se ha convertido en una ayuda importante para la celeridad de los usuarios.

Entrevistado 5 (2023), argumentó que, sí, debido a que nuestra sociedad actualmente funciona por los medios tecnológicos, estos se han convertido en las actuales herramientas para cometer actos delictivos.

Entrevistado 6 (2023), argumentó que, sí, en el ámbito tecnológico (TIC) existen muchas facilidades de que se creen cuentas falsas atribuyendo hechos o efectuando adquisiciones a nombre de terceros.

Entrevistado 7 (2023), argumentó que, sí, por lo general se hace por medio de computadoras, celulares, vía telefónica, skimmer para tarjetas de banco, dispositivo tipo POS para leer chip de tarjetas por acercamiento, entre otros (medios o sistemas informativos).

Entrevistado 8 (2023), argumentó que, sí, los medios tecnológicos pueden contribuir significativamente, en particular, los avances en la tecnología de la información y la comunicación han hecho que sea más fácil para los delincuentes suplantar la identidad de otra persona y cometer fraudes, por ejemplo, los correos electrónicos falsos y las páginas web falsas pueden ser creadas para hacer que el destinatario crea que está interactuando con una persona o entidad legítima, cuando en realidad es un delincuente que está intentando obtener información personal o financiera; además, los delincuentes utilizan el phishing para engañar a las personas para que revelen información confidencial, como contraseñas o números de tarjetas de crédito; también existen aplicaciones y herramientas en línea que pueden ser

utilizadas para suplantar la identidad de una persona, por ejemplo, las aplicaciones de falsificación de llamadas pueden hacer que una llamada parezca que proviene de un número de teléfono diferente, lo que puede permitir que los delincuentes realicen fraudes telefónicos.

Del análisis de contenido, a través del instrumento de categorización detallado en la Matrix de Convergencias y Divergencias, se destacan los siguientes argumentos similares o convergentes relacionados a la contribución de los medios tecnológicos al delito de suplantación de identidad.

- Sí, a través de la encriptación de información personal (Entrevistado 1).
- Sí, porque utilizan generalmente el escáner (Entrevistado 3).
- Sí, porque permiten a los delincuentes tener acceso con facilidad a la información personal (Entrevistado 4).
- Sí, debido a que nuestra sociedad actualmente funciona por los medios tecnológicos (Entrevistado 5).
- Sí, a través de las TIC, existen muchas facilidades de que se creen cuentas falsas (Entrevistado 6).
- Sí, a través de los medios o sistemas informativos (Entrevistado 7).
- Sí, contribuyen significativamente, en particular, los avances en la tecnología de la información y la comunicación han hecho que sea más fácil para los delincuentes suplantar la identidad de otra persona y cometer fraudes (Entrevistado 8).

Por lo tanto, y sintetizando las respuestas de los entrevistados, se deduce que, los medios tecnológicos, a través del mal uso de los medios o sistemas informáticos y las TIC, contribuyen y facilitan a los delincuentes a suplantar el derecho de identidad de otra persona, ejecutándose a través de la encriptación de información personal, llamadas telefónicas falsas, uso de escáners, uso de lectoras POS, facilidad al acceso digital de la información personal en la redes sociales, creación de correos cuentas falsas, etc.

Por último, y en relación al objetivo general de la presente tesis de investigación, se deduce que, los medios tecnológicos, a través del mal uso de los medios o sistemas informáticos y las TIC, contribuyen y facilitan a los delincuentes a suplantar el derecho

de identidad de otras personas, pues en Jaén y en zonas aledañas, los delitos más frecuentes son el phishing y el swanpping, que son modalidades de delitos de suplantación que se ejecutan con el propósito de cometer fraudes financieros, suplantación en redes sociales, desfalco de tarjetas financieras, etc; así también, se tienen otros delitos frecuentes, pero en menor escala, que son el grooming (delito por el cual se adopta la identidad de otra persona, para cometer acoso sexual y abuso sexual a terceros) y el ciberbullying; delitos realizados a través del mal uso del internet, mediante el envió de emails malintencionados, ingreso a páginas web peligrosas, envió de link maliciosos, encriptación de información personal, facilidad al acceso digital de la información personal en la redes sociales, creación de correos cuentas falsas; así también, a través de la clonación de tarjetas SIM móviles, llamadas telefónicas falsas, etc.

Interrogantes y respuestas, relacionadas al Objetivo General y al Objetivo Especifico 1: Determinar cómo ayudan los medios informáticos en el delito de la suplantación de identidad en las telecomunicaciones, Jaén 2022.

Por lo que se efectuó las siguientes interrogantes:

4. ¿En el ámbito de su experiencia profesional, ha tenido casos relacionados al delito informático del phishing, y cuál fue su tratamiento?, comente su respuesta.

Entrevistado 1 (2023), argumentó que, en casos de phishing se solicita que la entidad bancaria en la cual se ha sufrido la afectación proporcione la investigación interna y a partir de la misma se logre determinar si realmente se sufrió de una vulneración los datos privados financieros.

Entrevistado 2 (2023), argumentó que, no ha tenido ningún caso relacionado al delito informático, más tiene conocimiento de ello, ya que el delito informático del phishing es la suplantación de identidad de las personas, ya sea por medio de los sistemas informáticos, o por medio de los correos electrónicos y sitios web y así mismo lo realizan con las empresas.

Entrevistado 3 (2023), argumentó que, el delito de phinsing, por lo general son archivados, porque es difícil de demostrar, y no se tiene profesionales expertos en la región (Cajamarca).

Entrevistado 4 (2023), argumentó que, si ha tenido caso de phishing, pero en realidad nada o poco se puede hacer, porque en la ciudad de Jaén, no se cuenta con los medios tecnológicos que permitan llegar a la verdad y son archivados.

Entrevistado 5 (2023), argumentó que, si ha tenido caso de phishing, pero en la mayoría de casos, debido a que no se logra encontrar a las personas responsables, se terminaban archivando.

Entrevistado 6 (2023), argumentó que, no, ha tenido casos.

Entrevistado 7 (2023), argumentó que, no, ha tenido casos ese tipo de delito.

Entrevistado 8 (2023), argumentó que, si ha tenido casos de phishing, pues uno de los delitos más comunes, de los que llegan a través de correo electrónico, sin embargo, en la empresa se cuentan con herramientas de seguridad, tanto a nivel interno y externo (proveedores de Internet) que detectan a tiempo este tipo de ataques, en la mayoría de los casos, el contar con este tipo de herramientas y con una certificación en Seguridad de la Información (SGSI ISO 27001) nos ha permitido mitigar los riesgos que conllevan este tipo de ataques, y sobre todo prevenirlos, que es lo más importante. Los diferentes controles aplicados por medio del SGSI ayudan a mantenernos actualizados y alertas contra todo tipo de ataques y vulnerabilidades, además de mantener siempre informados y capacitados a los usuarios de la empresa.

Del análisis de datos, se destacaron los siguientes argumentos divergentes y convergentes detallados en la Matrix de Convergencias y Divergencias, relacionados al delito informático del phishing y su tratamiento.

- En la ciudad de Jaén, por lo general son archivados, porque son difíciles de demostrar, porque no se cuenta con los profesionales expertos en relación del delito y no se cuenta con los medios tecnológicos e informáticos en relación al delito (Entrevistado 3,4 y 5).
- No han tenido casos (Entrevistado 2, 6 y 7).

- Phishing, se comete por medio de los sistemas informáticos o por medio de los correos electrónicos y los sitios web (Entrevistado 2 y 8).
- En casos de phishing, se solicita que la entidad bancaria en la cual se ha sufrido la afectación proporcione la investigación interna y a partir de la misma se logre determinar si realmente se sufrió de una vulneración los datos privados financieros (Entrevistado 1).
- Las empresas deben contar con controles y herramientas de seguridad, tanto a nivel interno y externo (proveedores de Internet) que detecten a tiempo este tipo de ataques, en la mayoría de los casos, el contar con ese tipo de herramientas y con una certificación en Seguridad de la Información (SGSI ISO 27001) permiten mitigar los riesgos que conllevan a ese tipo de ataques, y sobre todo prevenirlos (Entrevistado 8).

Por lo tanto, y sintetizando las respuestas de los participantes entrevistados, se deduce que, el phishing, normalmente es cometido mediante el uso de sistemas o medios informáticos, complementados mediante el acceso a correos electrónicos falsos y sitios web peligrosos, en la ciudad de Jaén y zonas aledañas, el de delito de phishing, por lo general son archivados, porque son delitos difícil de demostrar, porque no se cuenta los profesionales expertos en relación del delito, y tampoco se cuenta con los medios tecnológicos e informáticos en relación al delito; por ello, las empresas deberían de contar con controles y herramientas tanto a nivel interno como externo, para detectar y prevenir este tipos de delito, y así apoyar a la criminalización del mismo.

8. ¿Mencione usted a su criterio profesional, si cree que los sistemas informáticos, ayudan a los delincuentes a cometer el delito del phishing?, comente su respuesta.

Entrevistado 1 (2023), argumentó que, sí, los sistemas informáticos ayudan a facilitar el delito de phishing.

Entrevistado 2 (2023), argumentó que, sí, los medios informáticos si ayudan a los delincuentes a delinquir de esa manera (phishing), sabiendo aún que los

delincuentes son personas que estudian y se capacitan detalladamente en todo el proceso en sí y como se generan estos dentro de los medios tecnológicos.

Entrevistado 3 (2023), argumentó que, sí, los delincuentes jaquean siempre información, a través de las computadoras (medios informáticos).

Entrevistado 4 (2023), argumentó que, sí, a través de los medios informáticos, se puede acceder con facilidad a la información personal de los usuarios.

Entrevistado 5 (2023), argumentó que, sí, los medios informativos sirven como un conducto para que los delincuentes puedan apropiarse de datos personales de terceros de manera más fácil, pues se aprovechan de la ingenuidad de personas que aún están aprendiendo a manejar los medios tecnológicos o se aprovechan de un descuido para lograr obtener su cometido.

Entrevistado 6 (2023), argumentó que, sí, porque a través de las redes informáticas se puede acceder a datos almacenados de los clientes y al no contar con la seguridad informática estos pueden ser vulnerados.

Entrevistado 7 (2023), argumentó que, depende del tipo de seguridad que manejen los sistemas y ordenadores, ya que por lo general el phishing, cosiste en engañar al usuario para que éste brinde la información que ellos necesitan para cometer el delito.

Entrevistado 8 (2023), argumentó que, sí, los sistemas informáticos pueden ayudar a los delincuentes a cometer el delito de phishing de varias maneras, al igual que las TIC, por eso es importante que las empresas que desarrollan software se encuentren reguladas o cuenten con adecuados mecanismos de seguridad.

Del análisis de datos, se destacaron los siguientes argumentos convergentes y divergentes detallados en la Matrix de Convergencias y Divergencias, otorgados por los participantes de investigación entrevistados.

- Los sistemas o medios informáticos, si ayudan y facilitan a los delincuentes a cometer el delito del phishing (Entrevistado 1, 2, 4, 5 y 8).
- Mediante los medios o sistemas informáticos, se puede acceder a información confidencial personal de terceros, para delinquir (Entrevistado 4, 5 y 6).

- Los delincuentes, se aprovechan de la ignorancia, descuido e ingenuidad de los usuarios, que desconocen y que no manejan los medios informáticos y tecnológicos, para cometer los delitos de suplantación de identidad (Entrevistado 5 y 7).
- Los delincuentes que cometen phishing, son personas estudiosas y capacitadas en informática y medios tecnológicos para cometer dichos delitos (Entrevistado 2).
- Los delincuentes hackean información a través de las computadoras (Entrevistado 3).
- Las empresas que desarrollan software, deben estar reguladas y contar y garantizar adecuados mecanismos de seguridad (Entrevistado 8).

Por lo tanto, en la síntesis y análisis de las respuestas de los participantes, se deduce que, Los sistemas o medios informáticos, si ayudan y facilitan a cometer el delito de phishing, pues los delincuentes que cometen esta modalidad de suplantación de identidad, son personas estudiosas y capacitadas en informática y medios tecnológicos, para poder ingresar mediante computadoras a distintos ordenadores y softwares y así poder hackear información, accediendo con facilidad a información personal de terceros, información recopilada a veces aprovechándose de la ingenuidad, descuido e ignorancia de los usuarios que no manejan los medios informáticos y tecnológicos; por lo tanto, una forma para remediar estos tipos de delitos, es que las empresas que desarrollan software, deben estar reguladas y contar y garantizar adecuados mecanismos de seguridad.

Para complementar, así también absolver y demostrar el objetivo general y el objetivo específico Nro 1, se tomó en cuenta la pregunta Nro 6, **¿Mencione usted a su criterio profesional, si los medios tecnológicos contribuyen a cometer el delito informático de suplantación de identidad?**, que anteriormente ya se analizó y diagnosticó y se dedujo lo siguiente.

Los medios tecnológicos, a través del mal uso de los medios o sistemas informáticos y las TICs, contribuyen y facilitan a los delincuentes a suplantar el derecho de identidad de otra persona, ejecutándose a través de la encriptación de información personal, llamadas telefónicas falsas, uso de escaners, uso de lectoras POS, facilidad

al acceso digital de la información personal en la redes sociales, creación de correos cuentas falsas, etc.

Entonces, y en relación al objetivo Nro 1 de la presente tesis de investigación, se deduce que, el mal uso de los medios o sistemas informáticos, contribuyen y facilitan a los delincuentes a suplantar el derecho de la identidad de un tercero, mediante la modalidad del phishing; los delincuentes que cometen estos tipos de delitos, son personas capacitadas en informática y medios tecnológicos, asimilando habilidades que mediante el uso de escáners, lectoras POS, clonación de tarjetas SIM, computadoras, hackeos de softwares, páginas y ordenadores, etc, acceden a información confidencial personal de usuarios en sus redes sociales y su banca personal, con el propósito de sacar beneficios ilícitos a favor del suplantador; los delitos relacionados a la suplantación de identidad en la ciudad de Jaén y zonas aledañas, por lo general son archivadas, porque dichos delitos son difíciles de demostrar, porque no cuentan con los profesionales expertos, y tampoco cuentan con los medios tecnológicos e informáticos en relación probatoria al delito; por lo tanto, una forma para remediar estos tipos de delitos, es que las empresas de telecomunicaciones y las que desarrollan software, deben estar reguladas y contar y garantizar adecuados mecanismos de seguridad.

Interrogantes y respuestas, relacionadas al Objetivo General y al Objetivo Especifico 2: Diagnosticar de qué forma contribuyen las TIC en el delito informático de la suplantación de identidad en las telecomunicaciones, Jaén 2022.

Por lo que se efectuó las siguientes interrogantes:

9. ¿Mencione usted a su criterio profesional, si cree que las TIC, ayudan a los delincuentes a cometer el delito del phishing?, comente su respuesta.

Entrevistado 1 (2023), argumentó que, sí, las Tecnología de la Información contribuyen a la realización del phishing, puesto que remiten datos de identificación de información básicos que permiten identificar información sensible de los agraviados a través de sus redes sociales, como principal medio de escape o difusión.

Entrevistado 2 (2023), argumentó que, si ayudan a cometer el delito del phishing, ya que las TIC se pueden usar para cosas buenas o malas.

Entrevistado 3 (2023), argumentó que, claro que sí.

Entrevistado 4 (2023), argumentó que, sí, los delincuentes utilizan las TIC para engañar a la población, asumiendo sus identidades.

Entrevistado 5 (2023), argumentó que, sí, las TIC son herramientas que aprovechan los delincuentes para poder engañar a los ciudadanos y lograr que entreguen su información personal.

Entrevistado 6 (2023), argumentó que, sí, porque a través del internet y la redes sociales, los delincuentes captan información para suplantar a terceros.

Entrevistado 7 (2023), argumentó que, sí, porque hoy en día todo se maneja mediante dispositivos tecnológicos, para la administración y distribución de la información de forma digitalizada. Las así llamadas TIC nos brindan un sinfín de beneficios. Esto también es utilizado por los delincuentes para cometer el phishing, así como otro tipo de delitos informáticos.

Entrevistado 8 (2023), argumentó que, en efecto que sí, y se debe en gran medida también al acceso a Internet sin restricción o sin los adecuados controles de seguridad, por lo tanto cualquier persona que quiera hacer daño y cuente con los conocimientos pueden utilizar la tecnología para cometer el delito del phishing de varias maneras, como por ejemplo:

Los delincuentes pueden enviar correos electrónicos fraudulentos y crear sitios web falsos que parecen auténticos. Los delincuentes pueden utilizar técnicas de ingeniería social para engañar a los usuarios para que revelen información confidencial, como contraseñas y números de tarjetas de crédito. Estos correos electrónicos y sitios web falsos pueden ser muy convincentes, utilizando logos y diseños similares a los sitios web legítimos.

Los delincuentes pueden enviar correos electrónicos de phishing a gran escala utilizando sistemas informáticos comprometidos como "bots" o "zombies". Los delincuentes pueden acceder a información personal y financiera de los usuarios a través de software malicioso o malware. Este software malicioso puede ser enviado a través de correos electrónicos o descargado desde sitios web infectados. Una vez que

se instala en el sistema de un usuario, el malware puede recopilar información confidencial y enviarla a los delincuentes.

En resumen, las TIC pueden ser utilizadas por los delincuentes para cometer el delito del phishing de varias maneras, por lo tanto, es importante que los usuarios estén conscientes de estas amenazas y tomen medidas para proteger su información en línea. Además, es importante que los sistemas informáticos estén protegidos por software de seguridad actualizado para evitar la infección por malware.

Del análisis de datos, se destacaron las siguientes manifestaciones convergentes y divergentes detalladas en la Matrix de Convergencias y Divergencias, otorgadas por las experiencias de los participantes de investigación.

- Las TIC contribuyen a realizar el delito del phishing, puesto que proporcionan herramientas como el internet y las redes sociales a los delincuentes cibernéticos, para captar información personal de terceros (Entrevistado 1, 2, 3, 6, 7 y 8).
- Los delincuentes a través de las TIC, engañan a la población, para que entreguen información confidencial de ellos y así poder suplantarlos (Entrevistado 4 y 5).
- Los delincuentes a través de correos electrónicos y páginas web falsas, así también, utilizando métodos de ingeniería social, pueden captar información confidencial de terceros, como contraseñas de sus redes sociales, de sus correos electrónicos y de sus finanzas, para sacar beneficio de ello (Entrevistado 8).
- Los delincuentes también pueden acceder a información personal y financiera de terceros a través de softwares maliciosos o malware, enviados a traes de correos electrónicos o links (Entrevistado 8).

Por ende, de la síntesis y análisis de las respuestas expresadas por las experiencias de los participantes investigación, se deduce que, el mal uso de las TIC, contribuyen a realizar el delito del phishing, puesto que proporcionan herramientas como las redes sociales y el internet sin restricciones y controles, es decir, los delincuentes informáticos, a través del malware y métodos de ingeniería social, utilizando correos electrónicos y páginas webs falsas y links peligroso, pueden captar información confidencial de terceros, como contraseñas de redes sociales, correos

electrónicos y financieros, para suplantar la identidad de los usuarios y sacar provecho de ello.

10. ¿Mencione usted a su criterio profesional, cree que los proveedores de sistemas informáticos y TIC, deben tener responsabilidad directa en el delito informático de suplantación de identidad, frente al usuario consumidor?, comente su respuesta.

Entrevistado 1 (2023), argumentó que, los proveedores de las TIC, tiene responsabilidad siempre y cuando haya de por medio un beneficio económico con la transmisión de información que identifique al usuario.

Entrevistado 2 (2023), argumentó que, sí, porque los proveedores de los medios tecnológicos son conocedores de toda la información personal de los usuarios.

Entrevistado 3 (2023), argumentó que, sí, pero si se aplica el sistema biométrico no podrán suplantar no podrán hacer nada.

Entrevistado 4 (2023), argumentó que, directamente no, porque la responsabilidad es indirecta, la responsabilidad debe caer en los terceros civiles, dado que deben tener el cuidado debido.

Entrevistado 5 (2023), argumentó que, sí, pero en algunos casos, como por ejemplo, cuando el proveedor sea una entidad bancaria, en esos casos el banco también debe tener responsabilidad frente al agraviado, pues ellos deberían haber tenido un procedimiento riguroso para hacer operaciones bancarias de retiro de dinero o compras con tarjeta de débito.

Entrevistado 6 (2023), argumentó que, los proveedores de los sistemas informáticos si deberían ser responsables solidarios a efectos de que en proceso eventual puedan resarcir el daño ocasionado.

Entrevistado 7 (2023), argumentó que, el usuario consumidor es el encargado de proteger su información personal; asimismo los proveedores de sistemas y TIC, tienen responsabilidad si se ha vulnerado o robado la información de sus sistemas informáticos o bases de datos.

Entrevistado 8 (2023), argumentó que, en general, los proveedores de sistemas informáticos y TIC no tienen una responsabilidad directa en el delito

informático de suplantación de identidad, ya que ese delito es cometido por terceros que utilizan las tecnologías de manera ilegal.

Sin embargo, los proveedores de sistemas informáticos y TIC sí tienen la responsabilidad de garantizar que sus productos y servicios sean seguros y estén protegidos contra los ataques de suplantación de identidad y otros delitos informáticos; esto incluye la implementación de medidas de seguridad adecuadas, la actualización constante del software y la capacitación del personal para detectar y responder a amenazas de seguridad.

Además, en algunos casos, los proveedores de sistemas informáticos y TIC pueden ser responsables si se demuestra que han actuado negligentemente y han contribuido a la comisión del delito de suplantación de identidad; por ejemplo, si un proveedor de servicios de correo electrónico no implementa medidas de seguridad adecuadas para proteger las cuentas de sus usuarios, y como resultado se produce una violación de seguridad que permite a los delincuentes robar información personal de los usuarios, el proveedor de servicios de correo electrónico podría ser considerado responsable de la violación.

Del análisis de datos, se sintetizaron los siguientes argumentos convergentes detallados en la Matrix de Convergencias y Divergencias, las cuales fueron proporcionadas por los entrevistados.

- En general, los proveedores de sistemas informáticos y TIC no tienen una responsabilidad directa en el delito informático de suplantación de identidad, ya que este delito es cometido por terceros que utilizan las tecnologías de manera ilegal (Entrevistado 4 y 8).
- Los proveedores de sistemas informáticos y TIC, tienen acceso a la información confidencial de las personas, por ende, tienen la responsabilidad de garantizar que sus productos y servicios sean seguros y estén protegidos contra los ataques de suplantación de identidad y otros delitos informáticos; esto incluye la implementación de sistemas biométricos y medidas de seguridad adecuadas, la actualización constante del software y la capacitación del personal para detectar y responder a amenazas de seguridad (Entrevistado 2, 3, 6 y 8).

- Los proveedores de sistemas informáticos y TIC pueden ser responsables si se demuestra que han actuado negligentemente y han contribuido a la comisión del delito de suplantación de identidad (7 y 8).

Por lo tanto, de la síntesis y análisis de las respuestas expresadas por los entrevistados, se deduce que, los proveedores de las TIC no tienen una responsabilidad directa en el delito informático de suplantación de identidad, ya que este delito es cometido por terceros que utilizan las tecnologías de manera ilegal, por otra parte, dichos proveedores, si tienen acceso a la información confidencial de las personas, por ende, tienen la responsabilidad de garantizar que sus productos y servicios sean seguros y estén protegidos contra los ataques de suplantación de identidad; esto incluye implementación de sistemas biométricos y medidas de seguridad adecuadas, la actualización constante del software y la capacitación del personal para detectar y responder a amenazas de seguridad; los proveedores de las TIC, pueden ser responsables si se demuestra que han actuado negligentemente y han contribuido a la comisión del delito de suplantación de identidad.

Entonces, y en relación al objetivo Nro 2 de la presente tesis de investigación, se deduce que, el mal uso de las TIC, contribuyen a realizar el delito de la suplantación del derecho de la identidad, puesto que proporcionan a los delincuentes informáticos, herramientas como las redes sociales y el internet sin restricciones y controles, para que a través de métodos de ingeniería social y el malware, insertados por correos electrónicos, páginas webs falsas y links peligroso, pueden captar información confidencial de terceros, como contraseñas de redes sociales, correos electrónicos y financieros, con el fin de suplantar la identidad de los usuarios y sacar provecho de ello; por otra parte, los proveedores de las TIC, dentro de sus ordenadores, tienen acceso a la información confidencial de las personas, por ende, tienen la responsabilidad de garantizar que sus productos y servicios sean seguros y estén protegidos contra los ataques de suplantación de identidad, mediante la implementación de sistemas biométricos y medidas de seguridad adecuadas, la actualización constante de los softwares y la capacitación constante del personal para detectar y responder a amenazas de seguridad.

Interrogantes y respuestas, relacionadas al Objetivo General y al Objetivo Especifico 3: Analizar las medidas de protección normativa que tienen los usuarios de la telefonía móvil, frente al delito informático de la suplantación de identidad en las telecomunicaciones, Jaén 2022.

Por lo que se efectuó las siguientes interrogantes:

3. ¿En el ámbito de su experiencia profesional, usted cree que se debe modificar el marco legislativo relacionado al delito de suplantación de identidad, y que modificaciones plantearía?, comente su respuesta.

Entrevistado 1 (2023), argumentó que, no está de acuerdo, porque los tipos penales de suplantación poseen aspectos básicos que permiten que el operador jurídico a través de una interpretación teológica, sancione la mayor cantidad de conductas posibles; más aún, si los delitos informáticos presentan a lo largo de los años nuevas modalidades de comisión. en lo que sí, está de acuerdo, es que se invierta más en presupuesto y se constituya a nivel regional fiscalías especializadas en delitos informáticos, puesto que las diligencias tienen un carácter especializado y de poco dominio común por parte de las fiscalías corporativas.

Entrevistado 2 (2023), argumentó que, sí debiera modificarse el marco legislativo respecto al delito de suplantación de identidad; las modificaciones que plantearía son, aumentar la pena privativa de libertad y las multas no debieran darse en este delito.

Entrevistado 3 (2023), argumentó que, sí, plantearía aumentar las penas, porque son penas muy cortas.

Entrevistado 4 (2023), argumentó que, sí, y las modificaciones que plantearía es que dote de equipos tecnológicos para la investigación del delito de suplantación, porque de lo contrario no se podría hallar los medios probatorios de los responsables.

Entrevistado 5 (2023), argumentó que, sí, primero, sería bueno que los delitos informáticos sean incorporados específicamente dentro del Código Penal, pues al encontrarse en una legislación separada, muy pocas personas conoces sobre este delito; segundo, en cuanto al delito de suplantación de identidad la norma debe especificar que la acción típica del delito consiste en adoptar, crear, apropiarse o

utilizar la identidad de una persona, en cualquier sistema informático, medio de comunicación o por cualquier otro medio.

Entrevistado 6 (2023), argumentó que, sí, debería tener penas más altas y que se deben implementar métodos de seguridad y confiabilidad que no permitan crear cuentas falsas.

Entrevistado 7 (2023), argumentó que, desconoce el marco legislativo, pero creo que se debería tener en cuenta el tipo de delito y el daño causado, ya que el término suplantación de identidad engloba un campo muy extenso.

Entrevistado 8 (2023), argumentó que, sí, se debe revisar y actualizar el marco legislativo de la Ley Nº 30096, Ley de Delitos Informáticos, para abordar adecuadamente estas amenazas emergentes, sobre todo si se trata de temas relacionados a las TIC que cambian constantemente, la modificación que plantearía sería en definir claramente los delitos relacionados con la suplantación de identidad en el ámbito digital en sus diferentes modalidades, incluyendo SIM swapping, el phishing y el fraude en línea, aunque este último fue actualizado en la Ley N° 30171, Ley que modifica la Ley 30096; sin embargo, no sólo se debe quedar en un marco legal, también debe haber un seguimiento continuo para ser efectivo el cumplimiento de las definiciones establecidas, y para lograrlo es importante fomentar la cooperación internacional, para perseguir a los delincuentes que comenten delitos de suplantación de identidad a través de Internet, ya que este tipo de delito a menudo tiene implicaciones transfronterizas, también se debería, proporcionar más recursos a las autoridades encargadas de investigar y perseguir los delitos relacionados con la suplantación de identidad, incluyendo la formación en tecnología y la colaboración con expertos en ciberseguridad, así como también, educar a la población sobre cómo proteger su información personal y financiera y cómo reconocer y evitar los intentos de suplantación de identidad.

Del análisis de datos, se tomaron en cuenta las manifestaciones más relevantes entre convergentes y divergentes, detalladas en la Matrix de Convergencias y Divergencias, las cuales fueron proporcionadas por los entrevistados.

- Sí, debe tener penas más altas, además se deben implementar métodos de seguridad y confiabilidad que no permitan adoptar, crear, apropiar o utilizar la identidad de una persona (Entrevistado 2, 3, 5 y 6).
- Se debe Invertir más presupuesto y constituir a nivel regional fiscalías especializadas en delitos informáticos, incluyendo formación en tecnología con la colaboración de expertos en ciberseguridad, puesto que las diligencias tienen un carácter especializado y de poco dominio común por parte de las fiscalías corporativas, y así tener acceso a medios probatorios más acordes a la realidad actual de las TIC (Entrevistado 1, 4 y 8).
- Sí, se debe revisar y actualizar el marco legislativo de la Ley Nº 30096, Ley de Delitos Informáticos, para abordar adecuadamente estas amenazas emergentes, sobre todo si se trata de temas relacionados a las TIC que cambian constantemente, pues se debe definir claramente los delitos de suplantación de identidad en el ámbito digital en sus diferentes modalidades, como el SIM swapping, el phishing y el fraude en línea, aunque este último fue actualizado en la Ley N° 30171, Ley que modifica la Ley 30096 (Entrevistado 8).
- Educar a la población sobre cómo proteger su información personal y financiera y cómo reconocer y evitar los intentos de suplantación de identidad (Entrevistado 8).

Por cuanto, de la síntesis y análisis de las respuestas expresadas por los entrevistados, se deduce que, sí se debe revisar y actualizar el marco legislativo de la Ley Nº 30096, Ley de Delitos Informáticos, para abordar adecuadamente las nuevas amenazas emergentes, sobre todo si se trata de temas relacionados a las TIC que cambian constantemente y son usadas en el delito digital de suplantación de identidad en sus modalidad de SIM swapping, phishing y fraudes en línea, aunque este último ya fue actualizado en la Ley N° 30171, Ley que modifica la Ley 30096; también se debe aumentar las penas relacionadas al delito de suplantación digital; otros cambios, pero no relacionados al marco legislativo, se debe Invertir más presupuesto y constituir a nivel regional fiscalías especializadas en delitos informáticos, incluyendo formación en tecnología con la colaboración de expertos en ciberseguridad, puesto que las

diligencias tienen un carácter especializado y de poco dominio común por parte de las fiscalías corporativas.

5. ¿En el ámbito de su experiencia profesional, usted, cree que existen falencias en las normas de protección al usuario en relación al delito de suplantación de identidad?, comente su respuesta.

Entrevistado 1 (2023), argumentó que, no, puesto que las normas de protección al usuario tienen cláusulas de no divulgación de información, que si son puesta al servicio de particulares contiene una sanción para la empresa, en donde, si puede haber una vulneración es a través de los sistemas informáticos.

Entrevistado 2 (2023), argumentó que, si existen falacias en las normas de protección al usuario en relación al delito de suplantación de identidad, las cuales debieran modificarse a favor del usuario, ya que lamentablemente esta protección al usuario solo es un saludo a la bandera.

Entrevistado 3 (2023), argumentó que, sí, tiene falencias, porque para que se haga efectivo, normalmente se tiene que comprar paquetes prepago o postpago de un seguro digital.

Entrevistado 4 (2023), argumentó que, sí, lamentablemente lo teórico no coincide con la realidad, pues si bien la norma establece que existe pena aplicable al autor (es), sin embargo los medios con los que se cuenta la autoridad que investiga son deficientes y por ello el caso sale impune.

Entrevistado 5 (2023), argumentó que, sí, pero más que todo el usuario no conoce todos sus derechos.

Entrevistado 6 (2023), argumentó que, las diligencias de la policía cibernética deben ser más céleres.

Entrevistado 7 (2023), argumentó que, sí, porque existen a diario casos de víctimas de robos cibernéticos, estafas, entre otras y usuarios que denuncian pero que no obtienen solución alguna.

Entrevistado 8 (2023), argumentó que, sí, una de las principales falencias en la regulación es que la suplantación de identidad puede ser difícil de detectar y prevenir, especialmente en línea y en las plataformas digitales, para hacerse pasar por

otra persona y obtener información personal o cometer fraudes; por ende, es necesario mejorar la regulación y la implementación de medidas de seguridad de las líneas digitales, para proteger a los usuarios de estos delitos; además, otra falencia en la regulación es que puede ser difícil procesar y castigar a los delincuentes que cometen suplantación de identidad, porque en algunos casos, puede ser difícil identificar al delincuente o recopilar pruebas suficientes para condenarlos; las leyes y los procesos penales deben ser mejorados para facilitar la investigación y el enjuiciamiento de los delitos de suplantación de identidad, en resumen, es necesario mejorar la regulación y la implementación de medidas de seguridad en línea y fortalecer los procesos penales para investigar y enjuiciar a los delincuentes que cometen este tipo de delitos.

Del análisis de datos, se tomaron en cuenta las manifestaciones más relevantes entre convergentes y divergentes, detalladas en la Matrix de Convergencias y Divergencias, las cuales fueron proporcionadas por los entrevistados.

- Sí, existe falencias en las normas de protección al usuario en relación al delito de suplantación de identidad (Entrevistado 2, 3, 4, 5 y 8).
- Los medios con los que cuentan las autoridades fiscalizadoras e investigadoras son deficientes, por ello, en algunos casos de delitos de suplencia, pueden ser difícil identificar al delincuente o recopilar pruebas suficientes para condenarlos y no hay solución alguna (Entrevistado 4, 7 y 8).
- No, puesto que las normas de protección al usuario tienen cláusulas de no divulgación de información, que si son puesta al servicio de particulares contiene una sanción para la empresa (Entrevistado 1).
- Para que se haga efectivo o eficiente las normas de protección al usuario, las empresas proveedoras de tecnológicas, ofrecen paquetes prepago o postpago de seguros digitales (Entrevistado 3).
- Sí, una de las principales falencias en la regulación, es que la suplantación de identidad es difícil de detectar y prevenir, especialmente en líneas y plataformas digitales (Entrevistado 8).

- Es necesario mejorar la regulación y la implementación de medidas de seguridad de las líneas digitales, para proteger a los usuarios de estos delitos. (Entrevistado 8).

En consecuencia, de la síntesis y análisis de las respuestas expresadas por los entrevistados, se deduce que, sí existe falencias en las normas de protección al usuario en relación al delito de suplantación de identidad, pues es necesario mejorarlas y además implementar medidas de seguridad de las líneas y plataformas digitales, porque el delito de suplantación de identidad es difícil de detectar y prevenir, puesto que, los medios con los que cuentan las autoridades fiscalizadoras e investigadoras son deficientes, por ello, en algunos casos de delitos de suplencia, es difícil identificar al delincuente o recopilar pruebas suficientes para condenarlos y al final no hay solución alguna.

7. ¿Mencione usted a su criterio profesional, si cree que se debe modificar el marco legislativo relacionado a los medios tecnológicos, con el propósito de evitar el delito de suplantación de identidad, y que modificaciones plantearía?, comente su respuesta.

Entrevistado 1 (2023), argumentó que, no sería necesario una modificación normativa.

Entrevistado 2 (2023), argumentó que, sí deben modificar el marco legislativo ya que la pena privativa de libertad es muy leve en esta clase de delitos, sabiendo que muchas veces el robo a través de estos medios tecnológicos son de sumas demasiadas altas las cuales ya no se pueden devolver.

Entrevistado 3 (2023), argumentó que, sí, porque toda persona para realizar un acto lo debe hacer a través de la huella digital, eso quiere decir que al momento de poner su huella en biométrico, le deben salir todos sus datos, para lo cual todos los biométricos deben estar vinculados a RENIEC.

Entrevistado 4 (2023), argumentó que, no, lo que se debe agregar es datos de los medios tecnológicos, para investigar los delitos tecnológicos.

Entrevistado 5 (2023), argumentó que, no, porque la palabra medios tecnológicos es un concepto amplio que abarca muchas modalidades de suplantación de identidad a través del uso de la tecnología.

Entrevistado 6 (2023), argumentó que, sí, las medidas de seguridad y las penas de cárcel deberían incrementarse.

Entrevistado 7 (2023), argumentó que, sí, fortaleciendo de la cooperación internacional, los delitos de suplantación de identidad digital a menudo cruzan las fronteras nacionales, por lo que es necesario fortalecer la cooperación internacional entre las autoridades encargadas de hacer cumplir la ley para investigar y enjuiciar a los delincuentes.

Entrevistado 8 (2023), argumentó que, sí, actualmente se cuenta con el Decreto Legislativo N.° 1412, que aprueba la Ley del Gobierno Digital, sin embargo esta ley no cuenta con lineamientos relacionado a los medios tecnológicos con el propósito de evitar el delito de suplantación de identidad, y la Ley Nº 30096, Ley de Delitos Informáticos, contempla la prevención y sanción de este tipo de delitos, pero no abarca medios tecnológicos, por lo que se observa que existe una brecha respecto a este tema que sería importante incluirlos en ambos marcos legislativos.

Algunas modificaciones que podrían ser consideradas en el marco legislativo para evitar el delito de suplantación de identidad podrían ser:

- Ampliación del ámbito de aplicación de la ley, pues debe abarcar no solo la suplantación de identidad, sino también cualquier las acciones que pueda contribuir al delito, como la elaboración, venta o distribución de software malicioso o herramientas de suplantación de identidad.
- Fortalecimiento de la responsabilidad de los proveedores de servicios en línea, pues deben ser responsables de proporcionar medidas de seguridad efectivas para prevenir la suplantación de identidad, además, deben tener la obligación de notificar a los usuarios si se produce una brecha de seguridad que pueda afectar su información personal.

- Aumento de las sanciones y penas, las sanciones y penas para los delitos de suplantación de identidad deben ser lo suficientemente severas para disuadir a los delincuentes de cometerlos.

Del análisis de datos, se tomaron en cuenta las manifestaciones más relevantes y relacionadas al tema de investigación, sobresalieron las opiniones divergentes y en menor escala las convergentes, las cuales se detallan en la Matrix de Convergencias y Divergencias.

- no se debe modificar el marco legislativo de suplantación de identidad, relacionado a los medios tecnológicos (Entrevistado 1, 4 y 5).
- Sí, se debe aumentar las sanciones y penas de cárcel, relacionadas al delito de suplantación de identidad, pues deben ser lo suficientemente severas para disuadir a los delincuentes de cometerlos (Entrevistado 2, 6 y 8).
- Sí, se debe implementar actividades con lectoras de huella, a través de biométricos, para tener los datos de las personas que realizan dichas actividades (Entrevistado 3).
- Sí, los delitos de suplantación de identidad digital a menudo cruzan las fronteras nacionales, por lo que es necesario fortalecer la cooperación internacional entre las autoridades encargadas de hacer cumplir la ley, y así investigar y enjuiciar a los delincuentes (Entrevistado 7).
- Si, actualmente contamos con el Decreto Legislativo N.° 1412, que aprueba la Ley del Gobierno Digital, sin embargo esta ley no cuenta con lineamientos relacionado a los medios tecnológicos con el propósito de evitar el delito de suplantación de identidad, y la Ley Nº 30096, Ley de Delitos Informáticos contempla la prevención y sanción de este tipo de delitos, pero no abarca específicamente a los medios tecnológicos, por lo que se observa que existe una brecha respecto a este tema que sería importante incluirlos en ambos marcos legislativos (Entrevistado 8).
- Sí, mediante la ampliación del ámbito de aplicación de la ley, pues debe abarcar no solo la suplantación de identidad, sino también, cualquier acción que pueda contribuir al delito, como la elaboración, venta o distribución de software malicioso o herramientas de suplantación de identidad (Entrevistado 8).

En consecuencia, de la síntesis y análisis de las respuestas expresadas por los entrevistados, se deduce que, actualmente se cuenta con el D.L. Nro 1412, Ley del Gobierno Digital, ley que no cuenta con lineamientos relacionados a los medios tecnológicos, para evitar el delitos de suplantación de identidad, también está la Ley Nro 30096, Ley de Delitos Informáticos, que contempla la prevención y sanción de este tipo de delitos, pero no abarca específicamente a los delitos por medios tecnológicos, por lo que, se observa que existe un vacío legal en el tratamiento de las nuevas modalidades de delito de suplantación de identidad; otra medida a modificar en el marco legislativo seria, la ampliación del ámbito de aplicación de la ley, pues debe abarcar no solo la suplantación de identidad, sino también, cualquier acción que pueda contribuir al delito, como la elaboración, venta o distribución de software malicioso o herramientas de suplantación de identidad.

Entonces, y en relación al objetivo Nro 3 de la presente tesis de investigación, se deduce que, se debe revisar y actualizar el marco legislativo relacionados a los delitos informáticos; actualmente se cuenta con el D.L. Nro 1412, Ley del Gobierno Digital y la Ley Nro 30096, Ley de Delitos Informáticos, que fue actualizada y modificada con la Ley N° 30171; normas legislativas que contemplan la prevención y sanción de los delitos informativos, pero que no abarcan específicamente a los delitos por medios tecnológicos, sobre todo si se trata de temas relacionados a las TIC que cambian constantemente y son usadas en el delito digital de suplantación de identidad en sus modalidad de SIM swapping, phishing y fraudes en línea, etc; por lo que, se observa que existen vacíos legales en el tratamiento de las nuevas modalidades de delito de suplantación de identidad; otra medida a modificar en el marco legislativo seria, la ampliación del ámbito de aplicación de la ley, pues debe abarcar no solo la suplantación de identidad, sino también, cualquier acción que pueda contribuir al delito, como la elaboración, venta o distribución de software malicioso o herramientas de suplantación de identidad; otros cambios, pero no relacionados al marco legislativo, es que se debe Invertir más presupuesto y constituir a nivel regional fiscalías especializadas en delitos informáticos, incluyendo formación en tecnología con la colaboración de expertos en ciberseguridad, puesto que las diligencias tienen un carácter especializado y de poco dominio común por parte de las fiscalías corporativas,

puesto que, los medios con los que cuentan las autoridades fiscalizadoras e investigadoras son deficientes, por ello, en algunos casos de delitos de suplencia, es difícil identificar al delincuente o recopilar pruebas suficientes para condenarlos y al final no hay solución alguna.

Siguiendo con la investigación, a continuación se realizó el análisis y comparación de los resultados conseguidos por medio de la guía de entrevistas realizada a los 8 participantes expertos del tema de estudio, con las fuentes documentales y teorías citadas, encontrando concordancias o convergencias.

Con relación al Objetivo General: Determinar cómo contribuyen los medios tecnológicos en el delito informático de la suplantación de identidad en las telecomunicaciones, Jaén 2022, se analizaron las siguientes fuentes documentales:

Por motivos de la pandemia del Coronavirus, en estos últimos años, los delitos con mayor auge y mayor repercusión de ejecución, han sido los delitos informativos, que se definen como, actos cometidos por usuarios con amplio manejo de los medios tecnológicos, que vulneran virtualmente el patrimonio de las personas, así como su identidad (Villavicencio, 2014).

El delito de suplantación de identidad se ha visto incrementado por el uso fraudulento de la información a través de los medios tecnológicos, pues las redes móviles se han convertido en una de las fuentes de alto riesgo para esta modalidad de fraude tecnológico (Gabaldón & Pereira, 2008).

La identidad es un derecho otorgado por el Estado para cada ciudadano, por ende, el Estado mediante la emisión y el acceso de documentos oficiales acredita el derecho a la identidad única a la población, pero en la actualidad, este derecho ha sido vulnerado por la delincuencia, que abusando la buena fe, inocencia y confianza de población, y haciendo uso indebido de la tecnología telefónica, incurre en el delito de la suplantación de identidad; este procedimiento ilegal sucede cuando a través de los medios tecnológicos telefónicos, el ciudadano acepta proporcionar información personal y confidencial a solicitud del operador telefónico, sin prever plenamente que

se puede tratar de un individuo que utilice dicha información personal y confidencial para hacerse de beneficios económicos y patrimoniales, fruto del esfuerzo del ciudadano (Colectivo ARCIÓN, 2015).

En América latina, usuarios que utilizan medios tecnológicos digitales, se han visto expuestos al delito de suplantación de identidad en sus transacciones bancarias, según las entidades pertenecientes al sistema financiero, los tipos de ataques más frecuentes utilizados contra los clientes del sistema bancario son el phishing (modalidad de suplantación de identidad) por correo electrónico, el phishing por mensaje de texto, el phishing por llamada de voz y la infección con software malintencionados o malware (Vargas, 2021).

El delito de suplantación de identidad, es cuando mediante el uso de los medios tecnológicos, un usuario se hace pasar o usurpar la identidad de otra persona o institución, acto ilícito que puede ocasionar problemas a una víctima, como perjudicarla económicamente, moralmente y socialmente, CRP, Ley Nro 30096, (2013).

De las entrevistas a los participantes expertos, se dedujo que, los medios tecnológicos, a través del mal uso de los medios o sistemas informáticos y las TIC, contribuyen y facilitan a los delincuentes a suplantar el derecho de identidad de otras personas, pues en Jaén y en zonas aledañas, los delitos más frecuentes son el phishing y el swanpping, que son modalidades de delitos de suplantación que se ejecutan con el propósito de cometer fraudes financieros, suplantación en redes sociales, desfalco de tarjetas financieras, etc; así también, se tienen otros delitos frecuentes, pero en menor escala, que son el grooming (delito por el cual se adopta la identidad de otra persona, para cometer acoso sexual y abuso sexual a terceros) y el ciberbullying; delitos realizados a través del mal uso del internet, mediante el envió de emails malintencionados, ingreso a páginas web peligrosas, envió de link maliciosos, encriptación de información personal, facilidad al acceso digital de la información personal en la redes sociales, creación de correos cuentas falsas; así también, a través de la clonación de tarjetas SIM móviles, llamadas telefónicas falsas, etc.

Por lo tanto, se concluye finalmente, que la deducción resultante de las entrevistas a los participantes, comparada con las manifestaciones teóricas de los autores citados en la presente investigación, se ha hallado concordancias en muchos

puntos, lo que fortalece la conclusión procedente de la entrevista; además, dicha conclusión comprueba afirmativamente el supuesto general de la presente tesis “Los medios tecnológicos si contribuyen en el delito informático de la suplantación de identidad en las telecomunicaciones, Jaén 2022”.

Con relación el Objetivo Especifico 1: Determinar cómo ayudan los medios informáticos en el delito de la suplantación de identidad en las telecomunicaciones, Jaén 2022, se analizaron las siguientes fuentes documentales:

Los delitos informáticos también se definen como, el conjunto de acciones ilícitas o desarrollo de crímenes a través de los sistemas informáticos, es decir, utilizan los medios tecnológicos para extender y desarrollar de manera exponencial sus actos criminales, así también, hacen uso de la tecnología para su evolución delictiva constante (Núñez & Carhuancho, 2020).

En los delitos informáticos, existe 2 (dos) tipos de usuarios, el sujeto activo, que es cualquier persona con dominio de los medios tecnológicos (medios informativos, TIC, medios audiovisuales), y el sujeto pasivo, que también es cualquier persona natural o jurídica (entidades gubernamentales o privadas), la cual es la víctima del hecho delictivo (Espinoza, 2018).

Según el Sistema de Denuncias de la Policía (SIDPOL), hasta julio del 2022, se vienen registrando más de 1,300 denuncias por casos de suplantación de identidad, cifra que supera las denuncias equivalentes al período de años anteriores, pues pese a que este tipo de denuncias hoy en día tienen mucha incidencia, la gran mayoría son denuncias archivadas por falta de profesionales especialistas en el caso, así como del desconocimiento de los policías y fiscales sobre la materia de ciberdelitos (suplantación de identidad y fraudes tecnológicos); por otro lado, los suplantados deben lidiar con los perjuicios económicos, morales y sociales, porque las entidades responsables de su protección no les brindan soluciones (Morales, 2022).

El COVID-2019, ha obligado a los estudiantes y a las personas de todas las naciones la utilización de los medios informáticos y TIC, de las cuales un aproximado del 16% de personas carecen de habilidades en ellas, utilizándolas de forma básica, por ello, con la expansión de la tecnología a través medios informáticos han generado

ambientes ideales para múltiples maneras o formas de ejecución de ciberdelitos; así también, los delincuentes informáticos han desarrollado o evolucionado sus mecanismos delictivos tan igual o mayor al avance tecnológico, a través del uso del internet y teniendo como herramienta los medios tecnológicos, es por ello, que se convierten en amenazas, porque los delincuentes cibernéticos desafían a los derechos legales existentes, porque no están acordes a la tecnológica emergente (Ramírez, et al., 2022).

Una nueva modalidad de suplantación de identidad informática es el SIM swapping, donde el delincuente informático busca la forma de duplicar la tarjeta SIM de un usuario, con el propósito de suplantar su identidad y acceder a sus cuentas bancarias y redes sociales vinculadas a su dispositivo móvil; por lo que, para prevenir dicha modalidad de delito informático, las personas no deben de proporcionar datos personales en llamadas, e-mails o SMS, no deben de vincular sus cuentas bancarias a sus dispositivos móviles, no deben de brindar el código PIN a nadie, no deben de descargar APPs de dudosa procedencia y deben de borrar redes sociales que no utilicen (Redacción Gestión, 2022).

De las entrevistas a los participantes expertos, se dedujo que, el mal uso de los medios o sistemas informáticos, contribuyen y facilitan a los delincuentes a suplantar el derecho de la identidad de un tercero, mediante la modalidad del phishing; los delincuentes que cometen estos tipos de delitos, son personas capacitadas en informática y medios tecnológicos, asimilando habilidades que mediante el uso de escáners, lectoras POS, clonación de tarjetas SIM, computadoras, hackeos de softwares, páginas y ordenadores, etc, acceden a información confidencial personal de usuarios en sus redes sociales y su banca personal, con el propósito de sacar beneficios ilícitos a favor del suplantador; los delitos relacionados a la suplantación de identidad en la ciudad de Jaén y zonas aledañas, por lo general son archivadas, porque dichos delitos son difíciles de demostrar, porque no cuentan con los profesionales expertos, y tampoco cuentan con los medios tecnológicos e informáticos en relación probatoria al delito; por lo tanto, una forma para remediar estos tipos de delitos, es que las empresas de telecomunicaciones y las que desarrollan software, deben estar reguladas y contar y garantizar adecuados mecanismos de seguridad.

Por lo tanto, se concluye finalmente que la deducción resultante de las entrevistas a los participantes, comparada con las manifestaciones teóricas de los autores citados, relacionados al objetivo específico 1 de la presente tesis, se ha hallado concordancias en muchos puntos, lo que fortalece la conclusión procedente de la entrevista; además, dicha conclusión comprueba afirmativamente el supuesto especifico Nro 1 (uno) “Los medios informáticos ayudan en el delito de la suplantación de identidad en las telecomunicaciones, Jaén 2022”.

Con relación el Objetivo Especifico 2: Diagnosticar de qué forma contribuyen las TIC en el delito informático de la suplantación de identidad en las telecomunicaciones, Jaén 2022, se analizaron las siguientes fuentes documentales:

Las TIC a través de la redes sociales, permite a los jóvenes comunicarse de manera más rápida y oportuna; sin embargo, esta herramienta tecnológica puede usarse de manera inadecuada e imprudencial para dañar y suplantar a otras personas; pues mediante la suplantación de identidad el usuario mal intencionado puede; enviar mensajes amenazantes a otras personas haciéndose pasar por otra persona, como también publicar vídeos o imágenes denigrantes de personas, publicar burlas de otras personas, información comprometedora y confidencial haciéndose pasar por otras personas, con el propósito de dañar social y emocionalmente a otros individuos (Valdés, et al., 2018).

El uso del internet desde dispositivos móviles hace la vida más fácil a los usuarios, pero esas facilidades se vuelven peligrosas, cuando delincuentes informáticos haciendo uso de las TIC como herramienta, infiltran programas maliciosos en sitios web o APPs, con el propósito sacar beneficios ilícitos o simplemente dañar a los usuarios consumidores de esos servicios; por otro lado, la incompatibilidad de las leyes a nivel mundial así como la inasistencia de leyes en algunos países, y por la transnacionalización de los delitos informáticos, han generado dificultadas para combatir dichos delitos cibernéticos, generando pérdidas millonarias a los estados, empresas y usuarios (Ortiz, 2019).

El uso de las TIC facilitan el delito de suplantación de identidad de organismo institucional o de una persona natural, como por ejemplo, crear usuarios o perfiles falsos atribuidos a personas, empresas, instituciones, mediante las redes sociales, con el propósito de defraudar, desprestigiar y/o perjudicar a los mismo o a terceros; el delito cibernético de la suplantación de identidad esta normada en el artículo 9° de la Ley Nro 30096, la cual la tipifica como un delito de resultado, porque no basta con realizar la acción de suplantar la identidad del usuario o empresa, sino es necesario que se origine o cause un perjuicio como resultado del delito (Villavicencio, 2014).

Uno de los métodos de estafa cibernética relacionada a la suplantación de identidad, es el phishing, que es una modalidad de ingeniera social, que utilizan los delincuentes cibernéticos para obtener información confidencial de las personas de manera fraudulenta y así usurpar la identidad de estos usuarios; por ejemplo, dentro de los métodos usados por los cibercriminales para ejecutar el phishing están, el envió de e-mails y SMS maliciosos, descarga de APPs maliciosas, mensajes maliciosos en WhatsApp, ataque a las redes sociales, etc, acciones que hacen los cibercriminales, mayormente con el propósito de acceder a información confidencial financiera, para vaciar las cuentas de las víctimas y robar el dinero que tienen (Dextre, 2022).

De las entrevistas a los participantes expertos, se dedujo que, el mal uso de las TIC, contribuyen a realizar el delito de la suplantación del derecho de la identidad, puesto que proporcionan a los delincuentes informáticos, herramientas como las redes sociales y el internet sin restricciones y controles, para que a través de métodos de ingeniería social y el malware, insertados por correos electrónicos, páginas webs falsas y links peligroso, pueden captar información confidencial de terceros, como contraseñas de redes sociales, correos electrónicos y financieros, con el fin de suplantar la identidad de los usuarios y sacar provecho de ello; por otra parte, los proveedores de las TIC, dentro de sus ordenadores, tienen acceso a la información confidencial de las personas, por ende, tienen la responsabilidad de garantizar que sus productos y servicios sean seguros y estén protegidos contra los ataques de suplantación de identidad, mediante la implementación de sistemas biométricos y medidas de seguridad adecuadas, la actualización constante de los softwares y la

capacitación constante del personal para detectar y responder a amenazas de seguridad.

Por ende, se concluye finalmente que la deducción resultante de las entrevistas a los participantes, comparada con las manifestaciones teóricas de los autores citados, relacionados al objetivo específico 2 de la presente tesis, se ha hallado concordancias en muchos puntos, lo que fortalece la conclusión procedente de la entrevista; además, dicha conclusión comprueba afirmativamente el supuesto especifico Nro 2 (dos) “Las TIC contribuyen en el delito informático de la suplantación de identidad en las telecomunicaciones, Jaén 2022”.

Con relación el Objetivo Especifico 3: Analizar las medidas de protección normativa que tienen los usuarios de la telefonía móvil, frente al delito informático de la suplantación de identidad en las telecomunicaciones, Jaén 2022, se analizaron las siguientes fuentes documentales:

El Perú ha suscrito un relevante convenio internacional en materia para combatir los ciberdelitos, que es el convenio de Budapest (2004), por lo que se promulgó la Ley Nro. 30096, la cual fue modificada mediante la Ley Nro. 30171 “Ley de Delitos Informáticos” (en adelante Ley Nro. 30171), normas legislativas incorporadas al sistema penal peruano con el propósito de que exista un ordenamiento jurídico y se adecue a los estándares internacionales estipulados en el “convenio de Budapest”; por ello en la Ley Nro. 30171 se tipificaron los delitos informáticos como ejemplo: la interceptación de datos informáticos, los atentados a la integridad de datos informáticos, la suplantación de la identidad, etc. (Leyva, 2021).

La Agencia Europea para la Seguridad de las Redes y de la Información (ENISA), manifiesta que existen 15 (quince) amenazas más relevantes utilizadas por los delincuentes cibernéticos, dentro de las cuales están el Malware, el uso inapropiado de las aplicaciones web, el robo de la identidad, etc.; además, el reto esta que las naciones deben determinar estos nuevos delitos y sus penas, y que la legislación relacionada a estos delitos deben estar atentos a sus permanentes cambios tecnológicos que tienen día a día, porque de no hacerlo los delincuentes cibernéticos sacarían gran provecho de ello (Pons, 2017).

La impunidad en relación a los delitos informáticos, se da por los vacíos legales en materia de estos delitos, pues las leyes actuales carecen de relevancia y no son suficientes para atribuirles responsabilidad judicial a los infractores que comenten estos delitos cibernéticos (Acosta, et al., 2020).

Las leyes en relación a los delitos informáticos es generalizada, por lo que, necesita una reforma legislativa, mediante leyes específicas acorde a cada tipo de ciberdelito, las cuales deben estar en constante actualización por los cambios veloces que se producen en la tecnología y en la sociedad, con el propósito de generar seguridad a los usuarios tecnológicos que consumen redes móviles (Saltos, 2021).

El delito de suplantación de identidad se ubica regulado dentro de los delitos informáticos, reconociéndose así, porque hace uso de la tecnología informática y de las telecomunicaciones para cometer el delito de la suplantación de identidad de una persona natural o jurídica, cometiendo perjuicios económicos y morales; el delito de suplantación de identidad en los últimos años no ha tenido regularización y modificación alguna, siendo en estos últimos años uno de delitos más ejecutados, por lo que en el Perú existe una incertidumbre legal sobre la regularización de la participación de los medios informáticos en el delito de la suplantación de identidad (Aldecoa, 2020).

La comisión de una delito mediante la utilización de los medios tecnológicos (hardware o software) no configura en su totalidad un delito informático, pues para que sea catalogado un delito informático tiene que establecerse ciertas características, de lo contrario, se estaría adjudicando un delito de forma inadecuada: además, para tener una lucha más eficiente contra los delitos informáticos, es necesario convocar a diversos Estados, con el propósito de suscribir un nuevo convenio internacional, que proponga nuevas herramientas y que estén acordes a las nuevas modalidades delictivas informáticas, pues las organizaciones criminarles están en constante evolución y perfeccionamiento (Vinelli, 2021).

De las entrevistas a los participantes expertos, se dedujo que, se debe revisar y actualizar el marco legislativo relacionados a los delitos informáticos; actualmente se cuenta con el D.L. Nro 1412, Ley del Gobierno Digital y la Ley Nro 30096, Ley de Delitos Informáticos, que fue actualizada y modificada con la Ley N° 30171; normas

legislativas que contemplan la prevención y sanción de los delitos informativos, pero que no abarcan específicamente a los delitos por medios tecnológicos, sobre todo si se trata de temas relacionados a las TIC que cambian constantemente y son usadas en el delito digital de suplantación de identidad en sus modalidad de SIM swapping, phishing y fraudes en línea, etc; por lo que, se observa que existen vacíos legales en el tratamiento de las nuevas modalidades de delito de suplantación de identidad; otra medida a modificar en el marco legislativo seria, la ampliación del ámbito de aplicación de la ley, pues debe abarcar no solo la suplantación de identidad, sino también, cualquier acción que pueda contribuir al delito, como la elaboración, venta o distribución de software malicioso o herramientas de suplantación de identidad; otros cambios, pero no relacionados al marco legislativo, es que se debe invertir más presupuesto y constituir a nivel regional fiscalías especializadas en delitos informáticos, incluyendo formación en tecnología con la colaboración de expertos en ciberseguridad, puesto que las diligencias tienen un carácter especializado y de poco dominio común por parte de las fiscalías corporativas, puesto que, los medios con los que cuentan las autoridades fiscalizadoras e investigadoras son deficientes, por ello, en algunos casos de delitos de suplencia, es difícil identificar al delincuente o recopilar pruebas suficientes para condenarlos y al final no hay solución alguna.

Por ende, se concluye finalmente que la deducción resultante de las entrevistas a los participantes, comparada con las manifestaciones teóricas de los autores citados, relacionados al objetivo específico 3 de la presente tesis, se ha hallado concordancias en muchos puntos, lo que fortalece la conclusión procedente de la entrevista; además, dicha conclusión comprueba afirmativamente el supuesto especifico Nro 3 (dos) “Las medidas de protección normativa de los usuarios de la telefonía móvil son deficientes, frente al delito informático de la suplantación de identidad en las telecomunicaciones, Jaén 2022”.

V. CONCLUSIONES

1. Los medios tecnológicos, a través del mal uso de los medios o sistemas informáticos y las TICs, contribuyen y facilitan a los delincuentes a suplantar el derecho de identidad de otras personas, pues en Jaén y en zonas aledañas, los delitos más frecuentes son el pishing y el swanpping, que son modalidades de delitos de suplantación que se ejecutan con el propósito de cometer fraudes financieros, suplantación en redes sociales, desfalco de tarjetas financieras, etc; así también, se tienen otros delitos frecuentes, pero en menor escala, que son el grooming (delito por el cual se adopta la identidad de otra persona, para cometer acoso sexual y abuso sexual a terceros) y el ciberbullying; delitos realizados a través del mal uso del internet, mediante el envió de emails malintencionados, ingreso a páginas web peligrosas, envió de link maliciosos, encriptación de información personal, facilidad al acceso digital de la información personal en la redes sociales, creación de correos cuentas falsas; así también, a través de la clonación de tarjetas SIM móviles, llamadas telefónicas falsas, etc.
2. El mal uso de los medios o sistemas informáticos, contribuyen y facilitan a los delincuentes a suplantar el derecho de la identidad de un tercero, mediante la modalidad del phishing; los delincuentes que cometen estos tipos de delitos, son personas capacitadas en informática y medios tecnológicos, asimilando habilidades que mediante el uso de escáners, lectoras POS, clonación de tarjetas SIM, computadoras, hackeos de softwares, páginas y ordenadores, etc, acceden a información confidencial personal de usuarios en sus redes sociales y su banca personal, con el propósito de sacar beneficios ilícitos a favor del suplantador; los delitos relacionados a la suplantación de identidad en la ciudad de Jaén y zonas aledañas, por lo general son archivadas, porque dichos delitos son difíciles de demostrar, porque no cuentan con los profesionales expertos, y tampoco cuentan con los medios tecnológicos e informáticos en relación probatoria al delito; por lo tanto, una forma para remediar estos tipos de delitos, es que las empresas de telecomunicaciones y las que desarrollan software,

deben estar reguladas y contar y garantizar adecuados mecanismos de seguridad.

3. El mal uso de las TIC, contribuyen a realizar el delito de la suplantación del derecho de la identidad, puesto que proporcionan a los delincuentes informáticos, herramientas como las redes sociales y el internet sin restricciones y controles, para que a través de métodos de ingeniería social y el malware, insertados por correos electrónicos, páginas webs falsas y links peligroso, pueden captar información confidencial de terceros, como contraseñas de redes sociales, correos electrónicos y financieros, con el fin de suplantar la identidad de los usuarios y sacar provecho de ello; por otra parte, los proveedores de las TIC, dentro de sus ordenadores, tienen acceso a la información confidencial de las personas, por ende, tienen la responsabilidad de garantizar que sus productos y servicios sean seguros y estén protegidos contra los ataques de suplantación de identidad, mediante la implementación de sistemas biométricos y medidas de seguridad adecuadas, la actualización constante de los softwares y la capacitación constante del personal para detectar y responder a amenazas de seguridad.
4. Se debe revisar y actualizar el marco legislativo relacionados a los delitos informáticos; actualmente se cuenta con el D.L. Nro 1412, Ley del Gobierno Digital y la Ley Nro 30096, Ley de Delitos Informáticos, que fue actualizada y modificada con la Ley N° 30171; normas legislativas que contemplan la prevención y sanción de los delitos informativos, pero que no abarcan específicamente a los delitos por medios tecnológicos, sobre todo si se trata de temas relacionados a las TIC que cambian constantemente y son usadas en el delito digital de suplantación de identidad en sus modalidad de SIM swapping, phishing y fraudes en línea,etc; por lo que, se observa que existen vacíos legales en el tratamiento de las nuevas modalidades de delito de suplantación de identidad; otra medida a modificar en el marco legislativo seria, la ampliación del ámbito de aplicación de la ley, pues debe abarcar no solo la suplantación de identidad, sino también, cualquier acción que pueda contribuir al delito, como la elaboración, venta o distribución de software malicioso o herramientas de

suplantación de identidad; otros cambios, pero no relacionados al marco legislativo, es que se debe Invertir más presupuesto y constituir a nivel regional fiscalías especializadas en delitos informáticos, incluyendo formación en tecnología con la colaboración de expertos en ciberseguridad, puesto que las diligencias tienen un carácter especializado y de poco dominio común por parte de las fiscalías corporativas, puesto que, los medios con los que cuentan las autoridades fiscalizadoras e investigadoras son deficientes, por ello, en algunos casos de delitos de suplencia, es difícil identificar al delincuente o recopilar pruebas suficientes para condenarlos y al final no hay solución alguna.

VI. RECOMENDACIONES

1. Las empresas (proveedores de internet) deben contar con controles y herramientas de seguridad, tanto a nivel interno y externo que detecten a tiempo los delitos informáticos de suplantación de identidad; en la mayoría de los casos, el contar con ese tipo de herramientas y con una certificación en Seguridad de la Información (SGSI ISO 27001) permite mitigar los riesgos que conllevan a ataques cibernéticos de suplantación, y sobre todo prevenirlos, que es lo más importante; los diferentes controles aplicados por medio del SGSI ayudan a mantener actualizados y en constante alerta a los sistemas operativos informáticos y a los equipos que usan TIC, contra todo tipo de ataques y vulnerabilidades.
2. A nivel internacional, se debe fomentar la cooperación internacional para perseguir a los delincuentes que comenten delitos de suplantación de identidad a través de Internet, ya que este tipo de delito a menudo tiene implicaciones transfronterizas, y a nivel nacional, se debe invertir más presupuesto, proporcionando más recursos a las autoridades encargadas de investigar y perseguir los delitos de suplantación, constituyendo a nivel regional fiscalías especializadas en delitos informáticos, incluyendo formación en tecnología con la colaboración de expertos en ciberseguridad, puesto que las diligencias tienen un carácter especializado y de poco dominio común por parte de las fiscalías corporativas y así tener acceso a medios probatorios más acordes a la realidad actual de las TIC y los medios o sistemas informáticos que cambian día a día.
3. Se debe realizar mejoras en la regulación y la implementación de medidas de seguridad de las líneas tecno-informáticas digitales, para proteger a los usuarios de los delitos informáticos; porque las falencias en la regulación es son difíciles de procesar legalmente y no castigan a los delincuentes que cometen suplantación de identidad, porque en algunos casos, puede ser difícil identificar al delincuente o delincuentes o de recopilar pruebas suficientes para condenarlos; las leyes y los procesos penales deben ser mejorados para facilitar la investigación y el enjuiciamiento de los delitos de suplantación de identidad.

4. Ampliar el ámbito de aplicación de la ley, pues debe abarcar no solo el delito en sí de la suplantación de identidad, sino también cualquier acción o acto que pueda contribuir a dicho delito, como la elaboración, desarrollo, venta y distribución de softwares maliciosos o herramientas que colaboren al ciberdelito de suplantación de identidad, así también se debe regular la responsabilidad de los proveedores de servicios tecnológicos informáticos, pues deben ser responsables de proporcionar medidas de seguridad efectivas para prevenir la suplantación de identidad, además, deben tener la obligación de notificar a los usuarios si se produce una vulneración de seguridad que pueda afectar su información personal.

REFERENCIAS

Acosta, M., Benavides, M., & García , N. (2020). Delitos Informáticos: Impunidad Organizacional y su Complejidad en el Mundo de los Negocios. *Redalyc.org - Revista Venezolana de Gerencia, 25*(89), 351-368. Obtenido de https://www.redalyc.org/journal/290/29062641023/html/

Aldecoa, M. (2020). *El Delito de Suplantación de Identidad y los Medios Informáticos, en el Sector Financiero de Lima, 2019.* Lima: Peru - Universidad César Vallejo. Obtenido de https://repositorio.ucv.edu.pe/discover

Arab, E., & Díaz, A. (2015). Impacto de las Redes Sociales e Internet en la Adolescencia: Aspectos Positivos y Negativos. *Revista Médica Clínica Las Condes, 26*(1), 07-13. Obtenido de https://www.elsevier.es/es-revista-revista-medica-clinica-las-condes-202-pdf-S0716864015000048

Arias, M., & Giraldo, C. (2011). Scientific Rigor In Qualitative Research. *Scielo Analyties, 29*(3), 500-514. Obtenido de http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0120-53072011000300020

Cabezas, E., Andrade, D., & Johana, T. (2018). *Introducción a la Metodología de la Investigación Científica.* Ecuador: Universidad de las Fuerzas Armadas ESPE. Obtenido de http://repositorio.espe.edu.ec/xmlui/handle/21000/15424

Colectivo ARCIÓN. (2015). La Suplantación de Identidad de Tipo Físico, Informático y de Telecomunicaciones Como Nueva Manifestación de las Conductas Antisociales. *Visión Criminológica - Criminalística, 1*(1), 6-22. Obtenido de http://revista.cleu.edu.mx/24-1301/23-01-la-suplantacion-de-identidad-de-tipo-fisico-informatico-y-de-telecomunicaciones-como-nueva-manifestacion-de-consductas-antisociales

Congreso de la República del Perú. (1991, 8 de abril). *Código Penal Decreto Legislativo Nro 635.* Diario Oficial el Peruano. Obtenido de https://apps.contraloria.gob.pe/unetealcontrol/pdf/07_635.pdf

Congreso de la República del Perú. (2013, 22 de octubre). *Ley Nro 30096, Ley de Delitos Informáticos.* Diario Oficial El Peruano. Obtenido de

https://busquedas.elperuano.pe/normaslegales/ley-de-delitos-informaticos-ley-n-30096-1003117-1/

Dextre, C. (30 de octubre de 2022). Perú es el País con Mas Ataques de Phishing en Latinoamérica: ¿Cómo Evitar Caer en Esta Ciberestafa? *La República*. Recuperado el 12 de diciembre de 2022, de https://larepublica.pe/tecnologia/2022/10/30/peru-es-el-pais-con-mas-ataques-de-phishing-en-latinoamerica-como-evitar-caer-en-esta-ciberestafa-evat/

Domínguez, R., & Vera, R. (2022). Spatial Analysis of Cybercrime to E-Commerce: Considerations for Political Agenda in Tamaulipas. *Scielo - Universidad Espíritu Santo - UEES, 41*(1), 21-40. Obtenido de http://scielo.senescyt.gob.ec/scielo.php?script=sci_arttext&pid=S2588-09692022000100021

Durand, J. (2010). Determinación del Derecho del Consumidor como Disciplina Jurídica Autónoma. *Asociación Civil Derecho & Sociedad, PUCP*(34), 69-81. Obtenido de https://revistas.pucp.edu.pe/index.php/derechoysociedad/article/view/13329

Espinoza, M. (2018). El Derecho Penal Informático Humano Como Cautela Frente al Poder Punitivo en la Sociedad de Control. *Revista Derecho, Universidad Nacional del Altiplano, 2*(3), 233-245. Obtenido de http://revistas.unap.edu.pe/rd/index.php/rd/article/view/26

Fernández, F. (2002). El Análisi de Contenido Como Ayuda Metodológica. *Revista de Ciencias Sociales, 2*(96), 35-53. Obtenido de https://www.redalyc.org/pdf/153/15309604.pdf

Fernández, P. (2018). La importancia de la Técnica de la Entrevista en la Investigación en Comunicación y las Ciencias Sociales. Investigación Documental. Ventajas y Limitaciones. *Sintaxis, Revista del Centro de Investigación Para la Comunicación Aplicada, 07*(1), 78-93. doi:https://doi.org/10.36105/stx.2018n1.07

Flores, P. (2020). *Relación Entre los Recursos Tecnológicos y el Logro de Aprendizajes Significativos de los Estudiantes de Posgrado, del Instituto para la Calidad de la Educación de la Universidad de San Martin de Porres, 2017.* Lima:

Peru. Obtenido de https://repositorio.usmp.edu.pe/handle/20.500.12727/6831?show=full

Gabaldón, L., & Pereira, W. (2008). Usurpación de Identidad y Certificacion Digital: Propuesta Para el Control del Fraude Electronico. *Scielo 5 Brasil - Sociologias, 10*(20), 164-190. Obtenido de https://www.scielo.br/j/soc/a/TSw5QX8TVH3s7BQyppCBQrb/?lang=es

Goris, S. (2015). Usefulness and Types of Literature Review. *Scielo Analytics, 9*(2). Obtenido de https://scielo.isciii.es/scielo.php?script=sci_arttext&pid=S1988-348X2015000200002&lng=es&nrm=iso&tlng=es

Leyva, C. (2021). Estudio de los Delitos Informáticos y la Problemática de su Tipificación en el Marco de los Convenios Internaciones. *Lucerna Luris Et Investigatio - Revista Investigacion UNMSM, 1*(1), 29-47. Obtenido de https://revistasinvestigacion.unmsm.edu.pe/index.php/Lucerna/article/view/18373

Loayza, E. (2020). La Investigación Cualitativa en Ciencias Humanas y Educación. Criterios Para Elaborar Artículos Científicos. *Educare Et Comunicare, 8*(2), 56-66. doi:https://doi.org/10.35383/educare.v8i2.536

Manterola, C., Grande, L., Otzen, T., Garcia, N., Salazar, P., & Quiroz, G. (2018). Confiabilidad, Precisión o Reproducibilidad de las Mediciones. Métodos de Valoración, Utilidad y Aplicaciones en la Práctica Clínica. *Revista Chilena de Infectologia, Scielo Analytics, 35*(6), 680-688. Obtenido de https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0716-10182018000600680

Morales, M. (2022). Suplantación de Identidad en Línea: Incrementan Denuncias, Pero no hay Responsables. *LR Data, 1*(1), 1-9. Obtenido de https://data.larepublica.pe/suplantacion-de-identidad-en-linea-incrementan-denuncias-pero-no-hay-responsables/

Muntané, J. (2010). Introducción a la Investigación Básica. *Revista Temáticas, RAPD Online, 33*(3), 221-227. Obtenido de https://www.sapd.es/revista/2010/33/3/03/resumen

Núñez, F., & Carhuancho, B. (2020). Ciberdelincuencia en Tiempos de Covid-19 ¿La Vulneración a Derechos Constitucionales? *Revista - Universidad Femenina del Sagrado Corazon, 16*(1), 93-100. Obtenido de https://revistas.unife.edu.pe/index.php/lumen/article/view/2287

Okuda, M., & Gómez, C. (2005). Método en Investigación Cualitativa: Triangulación. *Scielo Analytics, 34*(1), 118-124. Obtenido de http://www.scielo.org.co/pdf/rcp/v34n1/v34n1a08.pdf

Ortiz, N. (2019). Normativa Legal Sobre Delitos Informáticos en Ecuador. *Dialnet - Revista Hallazgos21, 4*(1), 100-111. Obtenido de https://revistas.pucese.edu.ec/hallazgos21/article/view/336

Páramo, D. (2015). La Teoría Fundamentada (Grounded Theory), Metodología Cualitativa de Investigación Científica. *Redalyc, Pensamiento & Gestión*(39), vii-xiii. Obtenido de https://www.redalyc.org/pdf/646/64644480001.pdf

Pinargote, K., & Cevallos, A. (2020). El Uso y Abuso de las Nuevas Tecnologías en el Área Educativa. *Dominio de las Ciencias, Dialnet, 6*(3), 517-532. Obtenido de https://dialnet.unirioja.es/servlet/articulo?codigo=7539716

Plaza, J., Uriguen, P., & Bejarano, H. (2017). Validez y Confiabilidad en la Investigación Cualitativa. *ARJÉ, Revista de Postgrado FaCE-UC, 11*(21), 352-357. Obtenido de http://arje.bc.uc.edu.ve/arj21/art24.pdf

Pons, V. (2017). Internet, la Nueva Era del Delito: Ciberdelito, Ciberterrorismo, Legislación y Ciberseguridad. *Urvio - Revista Latinoamericana de Estudios de Seguridad*(20), 80-93. doi:DOI: http://dx.doi.org/10.17141/urvio.20.2017.2563

Ramírez, E., Norabuena, R., Toledo, R., & Henostroza, P. (2022). Validación de una Escala de Conciencia Sobre Ciberdelito en Estudiantes Universitarios de Perú. *Scielo Analytics, Revista Científica General José María Córdova, 20*(37), 209-224. Obtenido de http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S1900-65862022000100208

Redacción Gestión. (12 de diciembre de 2022). Los Ciberdelitos Más Comunes Durante Navidad y Año Nuevo: Sepa Cómo Evitarlos. *Gestión*. Recuperado el 14 de diciembre de 2022, de https://gestion.pe/tecnologia/los-ciberdelitos-mas-

comunes-durante-navidad-y-ano-nuevo-sepa-como-evitarlos-ministerio-publico-sim-swapping-phishing-rmmn-noticia/

Riega, Y., Huamani, H., & Machuca, J. (2021). Contratación Electrónica y los Delitos Informáticos. En Protección al Consumidor en el Perú. *Dialnet, Lex, Revista UAP, 19*(28), 197-236. Obtenido de http://revistas.uap.edu.pe/ojs/index.php/LEX/article/view/2318

Rodríguez, C., Lorenzo, O., & Herrera, L. (2005). Teoría y Practica del Análisis de Datos Cualitativos. Proceso General y Criterios de Calidad. *International Journal Of Social Sciencies a Humanities, 15*(2), 133-154. Obtenido de https://www.redalyc.org/articulo.oa?id=65415209

Saltos, M. (2021). Análisis Conceptual del Delito Informático en Ecuador. *Scielo - Revista Conrado, 17*(78), 343-351. Obtenido de http://scielo.sld.cu/pdf/rc/v17n78/1990-8644-rc-17-78-343.pdf

Sepúlveda, J., Lago, C., Rosete, A., Sepúlveda, R., & Sepúlveda, J. (2008). Sistema Informático Para Análisis y Procesamiento de Datos de los Computadores de a Bordo de la Serie AGM-200X. *Revista Cubana de Ciencias Informáticas, 2*(1-2), 11-19. Obtenido de https://rcci.uci.cu/?journal=rcci&page=article&op=view&path%5B%5D=36

Spradley, J. (1980). Participant Onservation. *The Geoarge Washington University Institute For Ethnographic Research, 53*(4), 260-261. Obtenido de https://www.researchgate.net/publication/274761027_Participant_Observation

Valdés, Á., Carlos, E., & Torres, G. (2018). Propiedades Psicométricas de una Escala para Medir Cibervictimizacion en Universitarios. *Scielo Analytics - Revista Electronica de Investigación Educativa, 20*(4), 36-48. Obtenido de https://www-scielo-org-mx.translate.goog/scielo.php?script=sci_arttext&pid=S1607-40412018000400036&lng=es&nrm=iso&tlng=es&_x_tr_sl=es&_x_tr_tl=en&_x_tr_hl=es

Vargas, A. (2021). La Banca Digital: Innovación Tecnológica en la Inclusión financiera en el Perú. *Scielo Analytics - Revista Industrial Data, 24*(2), 99-120. Obtenido de http://www.scielo.org.pe/scielo.php?script=sci_arttext&pid=S1810-99932021000200099

Villavicencio, F. (2014). Delitos Informáticos. *IUS Et Veritas*(49), 2014. Obtenido de https://alicia.concytec.gob.pe/vufind/Record/RPUC_a8086424f1a713aab49c520da8424f84

Vinelli, R. (2021). Los Delitos Informáticos y su Relación con la Criminalidad Económica. *Lus Et Praxis - Universidad de Lima*(53), 95-110. doi:https://doi.org/10.26439/iusetpraxis2021.n053.4995

ANEXOS

ANEXO 1: Matriz de Consistencia

Título: Contribución de los Medios Tecnológicos en el Delito Informático de la Suplantación de Identidad en las Telecomunicaciones, Jaén 2022

<table>
<tr><th>FORMULACIÓN DEL PROBLEMA</th><th>OBJETIVOS DE LA INVESTIGACIÓN</th><th>SUPUESTOS</th><th>CATEGORIAS</th><th>PARTICIPANTES</th><th>METODOLOGIA</th><th>TÉCNICA / INSTRUMENTO</th></tr>
<tr><td>Problema Principal:

¿Cómo contribuyen los medios tecnológicos en el delito informático de la suplantación de identidad en las telecomunicaciones, Jaén 2022?</td><td>Objetivo Principal:

Determinar cómo contribuyen los medios tecnológicos en el delito informático de la suplantación de identidad en las telecomunicaciones, Jaén 2022.</td><td>Supuesto General

Los medios tecnológicos si contribuyen en el delito informático de la suplantación de identidad en las telecomunicaciones, Jaén 2022.</td><td rowspan="2">C.1: Delito de Suplantación de Identidad</td><td rowspan="3">4 (Participantes)
- Abogados especialistas
- Ingenieros de sistemas</td><td rowspan="3">Investigación:
Cualitativa

Tipo de Investigación:
Básica

Diseño de Investigación:
Teoría Fundamentada</td><td rowspan="3">Técnicas:
➢ Entrevistas
➢ Revisión Bibliográfica

Instrumentos:
➢ Guía o cedula de entrevistas.
➢ Revistas indexadas
➢ Tesis de Investigación
➢ Normas o Leyes
➢ Periódicos</td></tr>
<tr><td>Problemas específicos:

1. ¿Cómo ayudan los medios informáticos en el delito de suplantación de identidad en las telecomunicaciones, Jaén 2022?

2. ¿De qué forma contribuyen las TIC en el delito informático de la suplantación de identidad en las telecomunicaciones, Jaén 2022?

3. ¿Qué medidas de protección normativa tienen los usuarios de la telefonía móvil, frente al delito informático de la suplantación de identidad en las telecomunicaciones, Jaén 2022?</td><td>Objetivos Específicos:

1. Determinar cómo ayudan los medios informáticos en el delito de suplantación de identidad en las telecomunicaciones, Jaén 2022.

2. Diagnosticar de qué forma contribuyen las Tic en el delito informático de la suplantación de identidad en las telecomunicaciones, Jaén 2022.

3. Analizar las medidas de protección normativa que tienen los usuarios de la telefonía móvil, frente al delito informático de la suplantación de identidad en las telecomunicaciones.</td><td>Supuestos Específicos

1. Los medios informáticos ayudan en el delito de suplantación de identidad en las telecomunicaciones, Jaén 2022.

2. Las Tic contribuyen en el delito informático de la suplantación de identidad en las telecomunicaciones, Jaén 2022.

3. Las medidas de protección normativa de los usuarios de la telefonía móvil son deficientes, frente al delito informático de la suplantación de identidad en las telecomunicaciones, Jaén 2022.</td><td>C.2: Medios Tecnológicos</td></tr>
</table>

ANEXO 2: Matriz de Categorización

CATEGORÍAS	DEFINCIÓN CONCEPTUAL	DEFINICIÓN OPERACIONAL	DIMENSIONES
Delito de Suplantación de Identidad	Modalidad por la cual un individuo suplanta a otra persona o usuario, con el propósito de beneficiarse ilegalmente de la titularidad de un derecho u obtener beneficios por la obtención de un bien o una prestación de un servicio; el delito de suplantación de identidad se ha visto incrementado por el uso fraudulento de los medios tecnologías de información, pues las redes móviles se han convertido en una de las fuentes de alto riesgo para esta modalidad de fraude tecnológico (Gabaldón & Pereira, 2008).	Cuando mediante el uso de los medios tecnológicos, un usuario se hace pasar o usurpar la identidad de otra persona o institución, acto ilícito que puede ocasionar problemas a una víctima, como perjudicarla económicamente, moralmente y socialmente, Congreso de la República del Perú, Ley Nro 30096, (2013).	Phishing
			Normas de protección al usuario
Medios Tecnológicos	Son recursos o fuentes que hacen uso de la tecnología o la informática, para poder cumplir un propósito o tarea estipulada por un usuario (Flores, 2020).	Son medios digitales e informáticos, de tendencias innovadoras y relacionadas a la tecnología, el uso de ellas genera formas virtuales y digitales de comunicación con demás usuarios. La categoría será evaluada mediante un cuestionario de modalidad abierta.	Medios Informáticos
			TIC

ANEXO 3: VALIDACIÓN DE INSTRUMENTOS

UNIVERSIDAD CÉSAR VALLEJO

CARTA DE PRESENTACIÓN

Jaén, 19 de enero del 2023

Señor (a): Luis Alberto Tienado Solis
Especialidad: Maestro en derecho penal y ciencias criminológicas de la UNT
Presente

Asunto: **VALIDACIÓN DE INSTRUMENTO A TRAVÉS DE JUICIO DE EXPERTO**
De nuestra consideración.

Es muy grato dirigirme a usted para expresarle nuestro saludo cordial, asimismo, hacerle de su conocimiento que, en calidad de estudiante de la Escuela Profesional de Derecho de la Universidad "César Vallejo", en la sede Trujillo, promoción 2022-2, requerimos validar los instrumentos con el cual recogeremos la información necesaria para poder desarrollar nuestra investigación y optar el título profesional de ABOGADO (A).

El título de nuestro proyecto de investigación es: **"Contribución de los medios tecnológicos en el delito informático de la suplantación de identidad en las telecomunicaciones, Jaén 2022"** y es imprescindible contar con la aprobación de los instrumentos por parte de expertos del tema; por ello, se ha considerado conveniente recurrir a usted, ante su connotada experiencia en temas relacionados a la línea de investigación, de Derecho Penal, Procesal Penal, Sistemas de Penas, Causas y Formas del Fenómeno Criminal.

El expediente de validación contiene:

- Carta de presentación.
- Definiciones conceptuales de las Categorías.
- Matriz de consistencia
- Matriz de Categorización.
- Instrumento de investigación (Guía de Entrevista)
- Certificado de validez de contenido del instrumento.

Quedamos agradecidos por la atención a la presente.

Atentamente,

Flores Machuca Moisés
DNI: 40102384

Uriarte Pérez Greyci Sheraldine
DNI: 70358906

UNIVERSIDAD CÉSAR VALLEJO

CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO

INFORME DE OPINIÓN DE EXPERTOS DEL INSTRUMENTO DE INVESTIGACIÓN

I. DATOS GENERALES:

1.1. Apellidos y Nombres del Informante	:	Luis Alberto Tienado Solis
1.2. Especialidad del Valuador	:	Maestro en derecho penal y ciencias criminológicas de la UNT
1.3. Cargo e Institución donde labora	:	Docente de la UCV
1.4. Nombre del Instrumento motivo de la evaluación	:	Entrevista
1.5. Autor del Instrumento:	:	Flores Machuca Moisés Alcides Uriarte Pérez Greyci Sheraldine

II. ASPECTOS DE VALIDACIÓN E INFORME:

INDICADORES	CRITERIOS	Deficiente 0-20%	Regular 21-40%	Bueno 41-60%	Muy Bueno 61-80%	Excelente 81-100%
Claridad	Esta formulado con lenguaje apropiado					
Objetividad	Esta expresado de manera coherente y lógica					
Pertinencia	Responde a las necesidades de los Objetivos de la Investigación					
Actualidad	Esta adecuado para valorar aspectos y análisis de la Categorias					
Organización	Comprende los aspectos de calidad y claridad.					
Suficiencia	Tiene coherencia entre las categorias y los dimensiones.					
Intencionalidad	Estima las estrategias que responda al propósito de la investigación.					
Consistencia	Considera que los items utilizados en este instrumento son propios del campo que se está investigando.					
Coherencia	Consiste la estructura del presente instrumento es adecuado al tipo de usuario a quienes se dirige el instrumento					
Metodología	Considera que el item recoge información a lo que pretende la investigación.					
	PROMEDIO DE VALORIZACIÓN					

III. OPINIÓN DE LA APLICACIÓN

¿Qué aspecto tendría que modificar, incrementar o suprimir en el instrumento de investigación?

.....

.....

IV. PROMEDIO DE VALORACIÓN: _____

Jaén, 19 de enero del 2023

Firma del experto informante

UNIVERSIDAD CÉSAR VALLEJO

V. PERTINENCIA DEL ÍTEM O PREGUNTA DEL INSTRUMENTO:

Categoría 1: Delito Informático de Suplantación de Identidad

INSTRUMENTO	INSUFICIENTE	MEDIANAMENTE SUFICIENTE	SUFICIENTE
Ítem 1			
Ítem 2			
Ítem 3			
Ítem 4			
Ítem 5			

Categoría 2: Actividades en la Oficina de Tesorería del Gobierno Regional Amazonas

INSTRUMENTO	INSUFICIENTE	MEDIANAMENTE SUFICIENTE	SUFICIENTE
Ítem 6			
Ítem 7			
Ítem 8			
Ítem 9			
Ítem 10			

Jaén, 06 de enero del 2023

Firma del experto informante
DNI: 40836541

UNIVERSIDAD CÉSAR VALLEJO

CARTA DE PRESENTACIÓN

Jaén, 19 de enero del 2023

Señor (a): Wilfredo Rios Sánchez
Especialidad: Maestro en derecho penal
Presente

Asunto: **VALIDACIÒN DE INSTRUMENTO A TRAVÉS DE JUICIO DE EXPERTO**

De nuestra consideración.

Es muy grato dirigirme a usted para expresarle nuestro saludo cordial; asimismo, hacerle de su conocimiento que, en calidad de estudiante de la Escuela Profesional de Derecho de la Universidad "César Vallejo", en la sede Trujillo, promoción 2022-2, requerimos validar los instrumentos con el cual recogeremos la información necesaria para poder desarrollar nuestra investigación y optar el título profesional de ABOGADO (A).

El título de nuestro proyecto de investigación es: **"Contribución de los medios tecnológicos en el delito informático de la suplantación de identidad en las telecomunicaciones, Jaén 2022"** y es imprescindible contar con la aprobación de los instrumentos por parte de expertos del tema; por ello, se ha considerado conveniente recurrir a usted, ante su connotada experiencia en temas relacionados a la línea de investigación, de Derecho Penal, Procesal Penal, Sistemas de Penas, Causas y Formas del Fenómeno Criminal.

El expediente de validación contiene:

- Carta de presentación.
- Definiciones conceptuales de las Categorías.
- Matriz de consistencia
- Matriz de Categorización.
- Instrumento de investigación (Guía de Entrevista)
- Certificado de validez de contenido del instrumento.

Quedamos agradecidos por la atención a la presente.

Atentamente,

Flores Machuca Moisés
DNI: 40102384

Uriarte Pérez Greyci Sheraldine
DNI: 70358906

UNIVERSIDAD CÉSAR VALLEJO

CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO

INFORME DE OPINIÓN DE EXPERTOS DEL INSTRUMENTO DE INVESTIGACIÓN

I. DATOS GENERALES:

1.1. Apellidos y Nombres del Informante	:	Wilfredo Ríos Sánchez
1.2. Especialidad del Valuador	:	Maestro en derecho penal
1.3. Cargo e Institución donde labora	:	Docente de la UCV
1.4. Nombre del Instrumento motivo de la evaluación	:	Entrevista
1.5. Autor del Instrumento:	:	Flores Machuca Moisés Alcides Uriarte Pérez Greyci Sheraldine

II. ASPECTOS DE VALIDACIÓN E INFORME:

INDICADORES	CRITERIOS	Deficiente 0-20%	Regular 21-40%	Bueno 41-60%	Muy Bueno 61-80%	Excelente 81-100%
Claridad	Esta formulado con lenguaje apropiado					
Objetividad	Esta expresado de manera coherente y lógica					
Pertinencia	Responde a las necesidades de los Objetivos de la Investigación					
Actualidad	Esta adecuado para valorar aspectos y análisis de la Categorías					
Organización	Comprende los aspectos de calidad y claridad.					
Suficiencia	Tiene coherencia entre las categorías y los dimensiones.					
Intencionalidad	Estima las estrategias que responda al propósito de la investigación.					
Consistencia	Considera que los ítems utilizados en este instrumento son propios del campo que se está investigando.					
Coherencia	Consiste la estructura del presente instrumento es adecuado al tipo de usuario a quienes se dirige el instrumento					
Metodología	Considera que el ítem recoge información a lo que pretende la investigación.					
	PROMEDIO DE VALORIZACIÓN					

III. OPINIÓN DE LA APLICACIÓN

¿Qué aspecto tendría que modificar, incrementar o suprimir en el instrumento de investigación?

.....

.....

IV. PROMEDIO DE VALORACIÓN: _____

Jaén, 19 de enero del 2023

Firma del experto informante
DNI: 76161730

UNIVERSIDAD CÉSAR VALLEJO

V. PERTINENCIA DEL ÍTEM O PREGUNTA DEL INSTRUMENTO:

Categoría 1: Delito Informático de Suplantación de Identidad

INSTRUMENTO	INSUFICIENTE	MEDIANAMENTE SUFICIENTE	SUFICIENTE
Ítem 1			
Ítem 2			
Ítem 3			
Ítem 4			
Ítem 5			

Categoría 2: Actividades en la Oficina de Tesorería del Gobierno Regional Amazonas

INSTRUMENTO	INSUFICIENTE	MEDIANAMENTE SUFICIENTE	SUFICIENTE
Ítem 6			
Ítem 7			
Ítem 8			
Ítem 9			
Ítem 10			

Jaén, 06 de enero del 2023

Firma del experto informante
DNI: 18161730

UNIVERSIDAD CÉSAR VALLEJO

CARTA DE PRESENTACIÓN

Jaén, 26 de enero del 2023

Señor (a): Shikara Vásquez Shimajuko

Presente

Asunto: **VALIDACIÓN DE INSTRUMENTO A TRAVÉS DE JUICIO DE EXPERTO**
De nuestra consideración.
Es muy grato dirigirme a usted para expresarle nuestro saludo cordial; asimismo, hacerle de su conocimiento que, en calidad de estudiante de la Escuela Profesional de Derecho de la Universidad "César Vallejo", en la sede Trujillo, promoción 2022-2, requerimos validar los instrumentos con el cual recogeremos la información necesaria para poder desarrollar nuestra investigación y optar el título profesional de ABOGADO (A).

El título de nuestro proyecto de investigación es: **"Contribución de los medios tecnológicos en el delito informático de la suplantación de identidad en las telecomunicaciones, Jaén 2022"** y es imprescindible contar con la aprobación de los instrumentos por parte de expertos del tema; por ello, se ha considerado conveniente recurrir a usted, ante su connotada experiencia en temas relacionados a la línea de investigación, de Derecho Penal, Procesal Penal, Sistemas de Penas, Causas y Formas del Fenómeno Criminal.

El expediente de validación contiene:

- Carta de presentación.
- Definiciones conceptuales de las Categorías.
- Matriz de consistencia
- Matriz de Categorización.
- Instrumento de investigación (Guía de Entrevista)
- Certificado de validez de contenido del instrumento.

Quedamos agradecidos por la atención a la presente.

Atentamente,

Flores Machuca Moisés Alcides
DNI: 40102384

Urtarte Pérez Greyci Sheraldine
DNI: 70358906

UNIVERSIDAD CÉSAR VALLEJO

CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO

INFORME DE OPINIÓN DE EXPERTOS DEL INSTRUMENTO DE INVESTIGACIÓN

I. DATOS GENERALES:

1.1. **Apellidos y Nombres del Informante** : **Shikara Vásquez Shimajuko**
1.2. **Especialidad del Valuador** : Maestro en derecho penal

1.3. **Cargo e Institución donde labora** : ---
1.4. **Nombre del Instrumento motivo de la evaluación** : Entrevista
1.5. **Autor del Instrumento:** : Flores Machuca Moisés Alcides
Uriarte Pérez Greycl Sheraldine

II. ASPECTOS DE VALIDACIÓN E INFORME:

INDICADORES	CRITERIOS	Deficiente 0-20%	Regular 21-40%	Bueno 41-60%	Muy Bueno 61-80%	Excelente 81-100%
Claridad	Esta formulado con lenguaje apropiado					
Objetividad	Esta expresado de manera coherente y lógica					
Pertinencia	Responde a las necesidades de los Objetivos de la Investigación					
Actualidad	Esta adecuado para valorar aspectos y análisis de la Categorías					
Organización	Comprende los aspectos de calidad y claridad.					
Suficiencia	Tiene coherencia entre las categorías y los dimensiones.					
Intencionalidad	Estima las estrategias que responda al propósito de la investigación.					
Consistencia	Considera que los ítems utilizados en este instrumento son propios del campo que se está investigando.					
Coherencia	Consiste la estructura del presente instrumento es adecuado al tipo de usuario a quienes se dirige el instrumento					
Metodología	Considera que el ítem recoge información a lo que pretende la investigación.					
PROMEDIO DE VALORIZACIÓN						

III. OPINIÓN DE LA APLICACIÓN

¿Qué aspecto tendría que modificar, incrementar o suprimir en el instrumento de investigación?

.....
.....

IV. PROMEDIO DE VALORACIÓN: _____

Jaén, 26 de enero del 2023

_____
Firma del experto informante

UNIVERSIDAD CÉSAR VALLEJO

V. PERTINENCIA DEL ÍTEM O PREGUNTA DEL INSTRUMENTO:

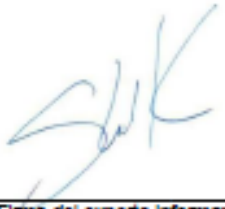
Categoria 1: Delito Informático de Suplantación de Identidad

INSTRUMENTO	INSUFICIENTE	MEDIANAMENTE SUFICIENTE	SUFICIENTE
Item 1			
Item 2			
Item 3			
Item 4			
Item 5			

Categoria 2: Actividades en la Oficina de Tesoreria del Gobierno Regional Amazonas

INSTRUMENTO	INSUFICIENTE	MEDIANAMENTE SUFICIENTE	SUFICIENTE
Item 6			
Item 7			
Item 8			
Item 9			
Item 10			

Jaén, 26 de enero del 2023



Firma del experto informante
DNI: 18212895

ANEXO 4: MATRIZ DE CONVERGENCIAS Y DIVERGENCIAS

<table>
<tr><th colspan="4">Pregunta Nro 1</th></tr>
<tr><td colspan="4">¿Conoce usted que es el delito de suplantación de identidad?</td></tr>
<tr><th>Entrevistado 1</th><th>Entrevistado 2</th><th>Entrevistado 3</th><th>Entrevistado 4</th></tr>
<tr><td>Sí, es el delito que se comete utilizando las tecnologías de la información mediante el cual el sujeto activo se apropia de la identidad de una persona natural o jurídica.</td><td>Sí, es un delito regulado en el Código Penal peruano, donde un individuo suplanta el derecho de identidad de otra, causándole perjuicio económico y moral.</td><td>Sí, es cuando una persona usa las tecnologías para hacerse pasar por otra persona.</td><td>Sí, es el delito por el cual se suplanta la identidad de una persona natural o jurídica, siempre que dicha conducta resulte en algún perjuicio.</td></tr>
<tr><th>Entrevistado 5</th><th>Entrevistado 6</th><th>Entrevistado 7</th><th>Entrevistado 8</th></tr>
<tr><td>Sí, es un delito que muchas veces utiliza los sistemas informáticos, que consiste en usurpar la identidad de una persona, ocasionándole daños.</td><td>Sí, El delito de suplantación de identidad radica en hacerse pasar por otra persona este tipo de delitos están normados en el Código Penal Peruano, existen delito de suplantación de identidad tanto en materia electoral como en materia informática Artículo 9 de la Ley Nº 30096.</td><td>Sí, la suplantación de identidad, son acciones de una persona que tiene el fin de apropiarse de la identidad de otro individuo, para obtener beneficios ilícitos de dicho acto; por lo general estos tipos de actos se realizan digitalmente, mediante el uso de la tecnología.</td><td>Sí, es un delito que consiste en utilizar la identidad de otra persona sin su autorización y con fines ilícitos.</td></tr>
<tr><th colspan="2">Convergencias</th><th>Divergencias</th><th>Interpretación</th></tr>
<tr><td colspan="2">• Delito mediante el cual el sujeto activo se apropia de la identidad de una persona natural o jurídica, se comete utilizando las tecnologías (Entrevistado 1).
• Delito donde un individuo suplanta el derecho de identidad de otra, causándole perjuicio económico y moral, está regulado en el Código Penal (Entrevistado 2).
• Delito donde una persona usa las tecnologías para hacerse pasar por otra persona (Entrevistado 3).
• Delito por el cual se suplanta la identidad de una persona natural o jurídica, siempre que dicha conducta resulte en algún perjuicio (Entrevistado 4).
• Delito que consiste en usurpar la identidad de una persona, ocasionándole daños, utiliza los sistemas informativos (Entrevistado 5).
• Delito que radica en hacerse pasar por otra persona, este tipo de delitos están normados en el Código Penal Peruano, existen delito de suplantación de identidad tanto en materia electoral como en materia informática Artículo 9 de la Ley Nº 30096.
• Delito donde las acciones de una persona tiene el fin de apropiarse de la identidad de otro individuo, para obtener beneficios ilícitos de dicho acto;</td><td></td><td>Teniendo en cuenta las respuestas convergentes de los entrevistados, se considera que, la suplantación de identidad es el delito donde un usuario activo realiza o ejecuta acciones para apropiarse del derecho de la identidad de otra persona natural o jurídica (usuario pasivo) sin su autorización, con el fin de obtener beneficios ilícitos por dicho acto, así también generando al suplantado, perjuicios económicos y/o morales, por lo general estos tipos de delitos se realizan digitalmente, mediante el uso de la tecnología informática.</td></tr>
</table>

por lo general estos tipos de actos se realizan digitalmente, mediante el uso de la tecnología (Entrevistado 7). • Delito que consiste en utilizar la identidad de otra persona sin su autorización y con fines ilícitos (Entrevistado 8).		

<table>
<tr><th colspan="4">Pregunta Nro 2</th></tr>
<tr><td colspan="4">¿En el ámbito de su experiencia profesional, conoce que modalidades más comunes ejecutan los delincuentes para cometer el delito de suplantación de identidad?</td></tr>
<tr><th>Entrevistado 1</th><th>Entrevistado 2</th><th>Entrevistado 3</th><th>Entrevistado 4</th></tr>
<tr><td>• Fraude en el sistema financiero, como compras online, transferencias bancarias, etc.
• Ciberbullying.
• Grooming o ganar la confianza de un menor y cometer abuso sexual y acoso sexual contra este.</td><td>• Suplantación en el uso de las redes sociales
• Suplantación en el teléfono celular.</td><td>• Suplantación del usuario en las telecomunicaciones.</td><td>• Fraude financiero (compras en línea, transferencias bancarias, etc).
• Acoso sexual.
• Estafa.</td></tr>
<tr><th>Entrevistado 5</th><th>Entrevistado 6</th><th>Entrevistado 7</th><th>Entrevistado 8</th></tr>
<tr><td>• Suplantación de tarjetas bancarias (débito o crédito),
• Envió de link, para extraer información del sujeto agraviado, para posteriormente sacar dinero de las cuentas bancarias.</td><td>• Creación de cuentas falsas en redes sociales</td><td>• El Pishing, a través emails recepcionados, ingresos a páginas peligrosas y/o llamadas telefónicas, donde roban información personal y financiera para suplantar.</td><td>• SIM Swapping, o la suplantación de la tarjeta SIM del móvil, para fraudes telefónicos
• El Phishing, fraude en línea, robo de identidad en redes sociales, entre otros.</td></tr>
<tr><th colspan="2">Convergencias</th><th>Divergencias</th><th>Interpretación</th></tr>
<tr><td colspan="2">• El Pishing, delito de suplantación de identidad, haciendo uso del internet, a través del envió de emails malintencionados, ingreso a paginas peligrosas, envió de link maliciosos y llamadas telefónicas, con el propósito de extraer datos de sujeto agraviado, para suplantación de tarjetas de débito y crédito, compras online, transferencias financieras, robo de identidad en las redes sociales, etc (Entrevistado 1, 4, 5, 7 y 8).
• El Swanpping, suplantación y duplicación de la tarjeta SIM del celular móvil, con la finalidad de realizar fraudes telefónicos, suplantación en la redes sociales, acceso a la información de la banca móvil de los celulares, para fraudes financieros (Entrevistado 2, 3, 6 y 8)
• El Grooming, delito por el cual se adopta la identidad de otra persona, para cometer acoso sexual y abuso sexual a terceros, mayormente a menores de edad. (Entrevistado 1 y 4)</td><td>• El Ciberbullying (Entrevistado 1).</td><td>Teniendo en cuenta las respuestas convergentes y divergentes resaltantes de los entrevistados, se considera que, los ciberdelitos de suplantación de identidad más comunes en la provincia de Jaén y zonas aledañas, son el Pishing y el Swanpping, delitos que hacen uso frecuente de sistemas informáticos y las TICs, con el propósito de cometer fraudes financieros, suplantación en redes sociales, desfalco de tarjetas financieras, etc; otros delitos comunes, pero en menor escala, son el Grooming y el Ciberbullying, delitos realizados a través del mal uso del internet, mediante el envió de emails malintencionados, ingreso a páginas web peligrosas, envió de link maliciosos, así también, a través de</td></tr>
</table>

		la clonación de tarjetas SIM móviles, llamadas telefónicas falsas, etc

Pregunta Nro 3			
¿En el ámbito de su experiencia profesional, usted cree que se debe modificar el marco legislativo relacionado al delito de suplantación de identidad, y que modificaciones plantearía?			
Entrevistado 1	**Entrevistado 2**	**Entrevistado 3**	**Entrevistado 4**
No estoy de acuerdo, porque los tipos penales de suplantación poseen aspectos básicos que permiten que el operador jurídico a través de una interpretación teológica, sancione la mayor cantidad de conductas posibles. Más aún, si los delitos informáticos presentan a lo largo de los años nuevas modalidades de comisión. En lo que sí, estaría de acuerdo, es que se invierta más en presupuesto y se constituya a nivel regional fiscalías especializadas en delitos informáticos, puesto que las diligencias tienen un carácter especializado y de poco dominio común por parte de las fiscalías corporativas.	Si debiera modificarse el marco legislativo respecto al delito de suplantación de identidad; las modificaciones que plantearía son las siguientes: aumentar la pena privativa de libertad y las multas no debieran darse en este delito.	Sí, plantearía aumentar las penas, porque son penas muy cortas.	Sí, y las modificaciones que plantearía es que dote de equipos tecnológicos para la investigación del delito de suplantación, porque de lo contrario no se podría hallar los medios probatorios de los responsables.
Entrevistado 5	**Entrevistado 6**	**Entrevistado 7**	**Entrevistado 8**
Sí, primero, sería bueno que los delitos informáticos sean incorporados específicamente dentro del Código Penal, pues al encontrarse en una legislación separada, muy pocas personas conoces sobre este delito; segundo, en cuanto al delito de suplantación de identidad la norma debe especificar que la acción típica del delito consiste en adoptar, crear, apropiarse o utilizar la identidad de una persona, en cualquier sistema informático, medio de comunicación o por cualquier otro medio.	Sí, debería tener penas más altas y que se deben implementar métodos de seguridad y confiabilidad que no permitan crear cuentas falsas.	Desconoce el marco legislativo, pero creo que se debería tener en cuenta el tipo de delito y el daño causado, ya que el término suplantación de identidad engloba un campo muy extenso.	Sí, considero que se debe revisar y actualizar el marco legislativo (Ley Nº 30096 o Ley de delitos informáticos) para abordar adecuadamente estas amenazas emergentes, sobre todo si se trata de temas relacionados a las TIC que cambian constantemente, una posible modificación que plantearía sería: • Definir claramente los delitos relacionados con la suplantación de identidad en el ámbito digital en sus diferentes modalidades, incluyendo SIM swapping, la creación de perfiles falsos en redes sociales, el phishing y el fraude en línea, aunque este

			último fue actualizado en la Ley N° 30171 (Ley que modifica la Ley 30096, Ley de Delitos Informáticos). • Sin embargo, no sólo se debe quedar en un marco, también debe haber un seguimiento continuo para ser efectivo el cumplimiento de las definiciones establecidas, y para lograrlo es importante fomentar la cooperación internacional para perseguir a los delincuentes que comenten delitos de suplantación de identidad a través de Internet, ya que este tipo de delito a menudo tiene implicaciones transfronterizas, proporcionar más recursos a las autoridades encargadas de investigar y perseguir los delitos relacionados con la suplantación de identidad, incluyendo la formación en tecnología y la colaboración con expertos en ciberseguridad así como también educar a la población sobre cómo proteger su información personal y financiera y cómo reconocer y evitar los intentos de suplantación de identidad.
Convergencias		**Divergencias**	**Interpretación**
• Sí, debe tener penas más altas, además se deben implementar métodos de seguridad y confiabilidad que no permitan adoptar, crear, apropiar o utilizar la identidad de una persona (Entrevistado 2, 3, 5 y 6). • Se debe Invertir más presupuesto y constituir a nivel regional fiscalías especializadas en delitos informáticos, incluyendo formación en tecnología con la colaboración de expertos en ciberseguridad, puesto que las diligencias tienen un carácter especializado y de poco dominio común por parte de las fiscalías corporativas, y así tener acceso a medios probatorios más acordes a la realidad actual de las TIC (Entrevistado 1, 4 y 8).		• Sí, se debe revisar y actualizar el marco legislativo de la Ley Nº 30096, Ley de Delitos Informáticos, para abordar adecuadamente estas amenazas emergentes, sobre todo si se trata de temas relacionados a las TIC que cambian constantemente, pues se debe definir claramente los delitos de suplantación de identidad en el	Teniendo en cuenta las respuestas convergentes y divergentes resaltantes de los entrevistados, se considera que, sí se debe revisar y actualizar el marco legislativo de la Ley Nº 30096, Ley de Delitos Informáticos, para abordar adecuadamente las nuevas amenazas emergentes, sobre todo si se trata de temas relacionados a las TIC que cambian constantemente,

	ámbito digital en sus diferentes modalidades, como el SIM Swapping, el Phishing y el fraude en línea, aunque este último fue actualizado en la Ley N° 30171, Ley que modifica la Ley 30096 (Entrevistado 8). • Educar a la población sobre cómo proteger su información personal y financiera y cómo reconocer y evitar los intentos de suplantación de identidad (Entrevistado 8).	para ser usadas en el delito digital de suplantación de identidad en sus modalidad de SIM Swapping, Phishing y fraudes en línea, aunque este último ya fue actualizado en la Ley N° 30171, Ley que modifica la Ley 30096, también se debe aumentar las penas relacionadas al delito de suplantación digital; otros cambios, pero no relacionados al marco legislativo, se debe Invertir más presupuesto y constituir a nivel regional fiscalías especializadas en delitos informáticos, incluyendo formación en tecnología con la colaboración de expertos en ciberseguridad, puesto que las diligencias tienen un carácter especializado y de poco dominio común por parte de las fiscalías corporativas.

Pregunta Nro 4			
¿En el ámbito de su experiencia profesional, ha tenido casos relacionados al delito informático del Phishing, y cuál fue su tratamiento?			
Entrevistado 1	**Entrevistado 2**	**Entrevistado 3**	**Entrevistado 4**
Si, en esos casos se solicita que la entidad bancaria en la cual se ha sufrido la afectación proporcione la investigación interna y a partir de la misma se logre determinar si realmente se sufrió de una vulneración los datos privados financieros.	No he tenido ningún caso relacionado al delito informático, más si tengo conocimiento de ello, ya que el delito informático del Phishing es la suplantación de identidad de las personas ya sea por medio de los sistemas informáticos, por medio de los correos electrónicos y los sitios web y así mismo lo realizan con las empresas.	Por lo general son archivados, porque es difícil de demostrar, y no se tiene profesionales expertos en la región.	Si, en realidad nada o poco se puede hacer, porque en la ciudad de Jaén, no se cuenta con los medios tecnológicos que permitan llegar a la verdad y son archivados.
Entrevistado 5	**Entrevistado 6**	**Entrevistado 7**	**Entrevistado 8**
Sí, en la mayoría de casos debido a que no se lograba encontrar a las personas responsables, se terminaban archivando.	No, he tenido casos.	No, hemos tenido casos este tipo de delito.	Si, de hecho el Phishing es uno de los más comunes, y los que llegan a través de correo electrónico, sin embargo, en la empresa se cuentan con herramientas de seguridad, tanto a nivel interno y externo (proveedores de Internet) que detectan a tiempo este tipo de ataques, en la mayoría de los casos, el contar con este tipo de herramientas y con una certificación en Seguridad de la Información (SGSI ISO 27001) nos ha permitido mitigar los riesgos que conllevan este tipo de ataques, y sobre todo prevenirlos, que es lo más importante. Los diferentes controles aplicados por medio del SGSI ayudan a mantenernos actualizados y alertas contra todo tipo de ataques y vulnerabilidades, además de mantener siempre informados y capacitados a los usuarios de la empresa
Convergencias		**Divergencias**	**Interpretación**

• En la ciudad de Jaén, por lo general son archivados, porque son difíciles de demostrar, porque no se cuenta con los profesionales expertos en relación del delito, no se cuenta con los medios tecnológicos e informáticos en relación al delito (Entrevistado 3,4 y 5). • No han tenido casos (Entrevistado 2, 6 y 7). • Phishing, se comente por medio de los sistemas informáticos, por medio de los correos electrónicos y los sitios web (Entrevistado 2 y 8)	• En casos de Phishing, solicita que la entidad bancaria en la cual se ha sufrido la afectación proporcione la investigación interna y a partir de la misma se logre determinar si realmente se sufrió de una vulneración los datos privados financieros (Entrevistado 1). • Las empresas deben contar con controles y herramientas de seguridad, tanto a nivel interno y externo (proveedores de Internet) que detecten a tiempo este tipo de ataques, en la mayoría de los casos, el contar con ese tipo de herramientas y con una certificación en Seguridad de la Información (SGSI ISO 27001) permiten mitigar los riesgos que conllevan a ese tipo de ataques, y sobre todo prevenirlos (Entrevistado 8).	Resaltando las respuestas convergentes de los expertos entrevistados, se considera que, el Phishing, normalmente es cometido mediante el uso de sistemas o medios informáticos, teniendo acceso a correos electrónicos falsos y sitios web peligrosos (TICs) en la ciudad de Jaén y zonas aledañas, el de delito de Phishing, por lo general son archivados, porque son delitos difícil de demostrar, porque no se cuenta los profesionales expertos en relación del delito, y tampoco se cuenta con los medios tecnológicos e informáticos en relación al delito; por ello, las empresas deberían de contar con controles y herramientas tanto a nivel interno como externo, para detectar y prevenir este tipos de delito, y así apoyar a la criminalización del delito.

Pregunta Nro 5			
¿En el ámbito de su experiencia profesional, usted, cree que existen falencias en las normas de protección al usuario en relación al delito de suplantación de identidad?			
Entrevistado 1	**Entrevistado 2**	**Entrevistado 3**	**Entrevistado 4**
No, puesto que las normas de protección al usuario tienen cláusulas de no divulgación de información, que si son puesta al servicio de particulares contiene una sanción para la empresa, en donde, si puede haber una vulneración es a través de los sistemas informáticos.	Si existen falacias en las normas de protección al usuario en relación al delito de suplantación de identidad, las cuales debieran modificarse a favor del usuario, ya que lamentablemente esta protección al usuario solo es un saludo a la bandera.	Sí, tiene falencias, porque para que se haga efectivo, normalmente se tiene que comprar paquetes prepago o postpago de un seguro digital.	Sí, lamentablemente lo teórico no coincide con la realidad, pues si bien la norma establece que existe pena aplicable al autor (es), sin embargo los medios con los que se cuenta la autoridad que investiga son deficientes y por ello el caso sale impune.
Entrevistado 5	**Entrevistado 6**	**Entrevistado 7**	**Entrevistado 8**
Sí, pero más que todo el usuario no conoce todos sus derechos.	Las diligencias de la policía cibernética deben ser más céleres.	Sí, porque existen a diario casos de víctimas de robos cibernéticos, estafas, entre otras y usuarios que denuncian pero que no obtienen solución alguna.	Sí, una de las principales falencias en la regulación es que la suplantación de identidad puede ser difícil de detectar y prevenir, especialmente en línea y en las plataformas digitales, para hacerse pasar por otra persona y obtener información personal o cometer fraudes; por ende, es necesario mejorar la regulación y la implementación de medidas de seguridad de las líneas digitales, para proteger a los usuarios de estos delitos; además, otra falencia en la regulación es que puede ser difícil procesar y castigar a los delincuentes que cometen suplantación de identidad, porque en algunos casos, puede ser difícil identificar al delincuente o recopilar pruebas suficientes para condenarlos; las leyes y los procesos penales deben ser mejorados para facilitar la investigación y el enjuiciamiento de los delitos de suplantación de identidad, en resumen, es necesario mejorar la regulación y la

			implementación de medidas de seguridad en línea y fortalecer los procesos penales para investigar y enjuiciar a los delincuentes que cometen este tipo de delitos.
Convergencias		**Divergencias**	**Interpretación**
• Sí, existe falencias en las normas de protección al usuario en relación al delito de suplantación de identidad (Entrevistado 2, 3, 4, 5 y 8). • Los medios con los que cuentan las autoridades fiscalizadoras e investigadoras son deficientes, por ello, en algunos casos de delitos de suplencia, pueden ser difícil identificar al delincuente o recopilar pruebas suficientes para condenarlos y no hay solución alguna (Entrevistado 4, 7 y 8).		• No, puesto que las normas de protección al usuario tienen cláusulas de no divulgación de información, que si son puesta al servicio de particulares contiene una sanción para la empresa (Entrevistado 1). • Para que se haga efectivo o eficiente las normas de protección al usuario, las empresas proveedoras de tecnológicas, ofrecen paquetes prepago o postpago de seguros digitales (Entrevistado 3). • Sí, una de las principales falencias en la regulación, es que la suplantación de identidad es difícil de detectar y prevenir, especialmente en líneas y plataformas digitales (Entrevistado 8). • Es necesario mejorar la regulación y la implementación de medidas de seguridad de las líneas digitales, para proteger a los usuarios de estos delitos. (Entrevistado 8).	Teniendo en cuenta las respuestas convergentes y divergentes resaltantes de los entrevistados, se considera que, sí, existe falencias en las normas de protección al usuario en relación al delito de suplantación de identidad, pues es necesario mejorarlas y además implementar medidas de seguridad de las líneas y plataformas digitales, porque el delito de suplantación de identidad es difícil de detectar y prevenir, puesto que, los medios con los que cuentan las autoridades fiscalizadoras e investigadoras son deficientes, por ello, en algunos casos de delitos de suplencia, es difícil identificar al delincuente o recopilar pruebas suficientes para condenarlos y al final no hay solución alguna.

Pregunta Nro 6			
¿Mencione usted a su criterio profesional, si los medios tecnológicos contribuyen a cometer el delito informático de suplantación de identidad?			
Entrevistado 1	**Entrevistado 2**	**Entrevistado 3**	**Entrevistado 4**
Sí, porque muchas los medios tecnológicos permiten la encriptación de información personal y no se puede identificar el dominio o IP responsable de los hechos delictivos.	Los medios tecnológicos no, sino que es la mala voluntad del ser humano al querer enriquecerse y aprovechar de los medios tecnológicos para su beneficio.	Sí, porque utilizan generalmente el escáner para los documentos (medios o sistemas informáticos).	Sí, porque permiten a los delincuentes tener acceso con facilidad a la información personal, así también, se ha convertido en una ayuda importante para la celeridad de los usuarios.
Entrevistado 5	**Entrevistado 6**	**Entrevistado 7**	**Entrevistado 8**
Sí, debido a que nuestra sociedad actualmente funciona por los medios tecnológicos, estos se han convertido en las actuales herramientas para cometer actos delictivos.	Si, en el ámbito tecnológico (TICs) existen muchas facilidades de que se creen cuentas falsas atribuyendo hechos o efectuando adquisiciones a nombre de terceros. .	Si, por lo general se hace por medio de computadoras, celulares, vía telefónica, skimmer para tarjetas de banco, dispositivo tipo POS para leer chip de tarjetas por acercamiento, entre otros (medios o sistemas informativos).	Sí, los medios tecnológicos pueden contribuir significativamente, en particular, los avances en la tecnología de la información y la comunicación han hecho que sea más fácil para los delincuentes suplantar la identidad de otra persona y cometer fraudes. Por ejemplo, los correos electrónicos falsos y las páginas web falsas pueden ser creadas para hacer que el destinatario crea que está interactuando con una persona o entidad legítima, cuando en realidad es un delincuente que está intentando obtener información personal o financiera. Además, los delincuentes pueden utilizar técnicas de phishing para engañar a las personas para que revelen información confidencial, como contraseñas o números de tarjetas de crédito. También existen aplicaciones y herramientas en línea que pueden ser utilizadas para suplantar la identidad de una persona. Por ejemplo, las aplicaciones de falsificación de llamadas pueden hacer que una llamada parezca que proviene de un número de teléfono diferente, lo que

			puede permitir que los delincuentes realicen fraudes telefónicos.
Convergencias		**Divergencias**	**Interpretación**
• Si, a través de la encriptación de información personal (Entrevistado 1). • Sí, porque utilizan generalmente el escáner (Entrevistado 3) • Sí, porque permiten a los delincuentes tener acceso con facilidad a la información personal (Entrevistado 4). • Sí, debido a que nuestra sociedad actualmente funciona por los medios tecnológicos (Entrevistado 5). • Si, a través de las TICs, existen muchas facilidades de que se creen cuentas falsas (Entrevistado 6). • Si, a través de los medios o sistemas informativos (Entrevistado 7). • Sí, los medios tecnológicos pueden contribuir significativamente, en particular, los avances en la tecnología de la información y la comunicación han hecho que sea más fácil para los delincuentes suplantar la identidad de otra persona y cometer fraudes (Entrevistado 8).		• Los medios tecnológicos no, sino que es la mala voluntad del delincuente (Entrevistado 2).	Resaltando las respuestas convergentes de los expertos entrevistados, se considera que, los medios tecnológicos, a través del mal uso de los medios o sistemas informáticos y las TICs, contribuyen y facilitan a los delincuentes a suplantar el derecho de identidad de otra persona, ejecutándose a través de la encriptación de información personal, llamadas telefónicas falsas, uso de escaners, lectoras POS, facilidad al acceso digital de la información personal en la redes sociales, creación de correos cuentas falsas.

Pregunta Nro 7			
¿Mencione usted a su criterio profesional, si cree que se debe modificar el marco legislativo relacionado a los medios tecnológicos, con el propósito de evitar el delito de suplantación de identidad, y que modificaciones plantearía?			
Entrevistado 1	**Entrevistado 2**	**Entrevistado 3**	**Entrevistado 4**
No sería necesario una modificación normativa.	Sí deben modificar el marco legislativo ya que la pena privativa de libertad es muy leve en esta clase de delitos, sabiendo que muchas veces el robo a través de estos medios tecnológicos son de sumas demasiadas altas las cuales ya no se pueden devolver.	Sí, porque toda persona para realizar un acto lo debe hacer a través de la huella digital, eso quiere decir que al momento de poner su huella en biométrico, le deben salir todos sus datos, para el cual todos los biométricos deben estar vinculados a RENIEC.	No, lo que se debe agregar es datos de los medios tecnológicos, para investigar los delitos tecnológicos.
Entrevistado 5	**Entrevistado 6**	**Entrevistado 7**	**Entrevistado 8**
No, considero que la palabra medios tecnológicos es un concepto amplio que abarca muchas modalidades de suplantación de identidad a través del uso de la tecnología.	Sí, las medidas de seguridad y las penas de cárcel deberían incrementarse. .	Sí, fortaleciendo de la cooperación internacional, los delitos de suplantación de identidad digital a menudo cruzan las fronteras nacionales, por lo que es necesario fortalecer la cooperación internacional entre las autoridades encargadas de hacer cumplir la ley para investigar y enjuiciar a los delincuentes.	Actualmente contamos con el Decreto Legislativo N.° 1412, que aprueba la Ley del Gobierno Digital, sin embargo esta ley no cuenta con lineamientos relacionado a los medios tecnológicos con el propósito de evitar el delito de suplantación de identidad, y la Ley Nº 30096, Ley de Delitos Informáticos contempla la prevención y sanción de este tipo de delitos, pero no abarca medios tecnológicos, por lo que se observa que existe una brecha respecto a este tema que sería importante incluirlos en ambos marcos legislativos. Algunas modificaciones que podrían ser consideradas en el marco legislativo para evitar el delito de suplantación de identidad podrían ser: • Ampliación del ámbito de aplicación de la ley, pues debe abarcar no solo la suplantación de identidad, sino también cualquier las acciones que pueda contribuir al delito, como la elaboración, venta o distribución de software malicioso o

			herramientas de suplantación de identidad. • Fortalecimiento de la responsabilidad de los proveedores de servicios en línea, pues deben ser responsables de proporcionar medidas de seguridad efectivas para prevenir la suplantación de identidad, además, deben tener la obligación de notificar a los usuarios si se produce una brecha de seguridad que pueda afectar su información personal. • Aumento de las sanciones y penas, las sanciones y penas para los delitos de suplantación de identidad deben ser lo suficientemente severas para disuadir a los delincuentes de cometerlos.
Divergencias		**Convergencias**	**Interpretación**
• Sí, se debe implementar actividades con lectoras de huella, a través de biométricos, para tener los datos de las personas que realizan dichas actividades (Entrevistado 3). • Sí, los delitos de suplantación de identidad digital a menudo cruzan las fronteras nacionales, por lo que es necesario fortalecer la cooperación internacional entre las autoridades encargadas de hacer cumplir la ley, y así investigar y enjuiciar a los delincuentes (Entrevistado 7). • Si, actualmente contamos con el Decreto Legislativo N.° 1412, que aprueba la Ley del Gobierno Digital, sin embargo esta ley no cuenta con lineamientos relacionado a los medios tecnológicos con el propósito de evitar el delito de suplantación de identidad, y la Ley Nº 30096, Ley de Delitos Informáticos contempla la prevención y sanción de este tipo de delitos, pero no abarca específicamente a los medios tecnológicos, por lo que se observa que existe una brecha respecto a este tema que sería importante incluirlos en ambos marcos legislativos (Entrevistado 8). • Sí, mediante la ampliación del ámbito de aplicación de la ley, pues debe abarcar no solo la suplantación de identidad, sino también, cualquier acción que pueda contribuir al delito, como la elaboración, venta o distribución de software malicioso o herramientas de suplantación de identidad (Entrevistado 8).		• No se debe modificar el marco legislativo de suplantación de identidad, relacionado a los medios tecnológicos (Entrevistado 1, 4 y 5). • Sí, se debe aumentar las sanciones y penas de cárcel, relacionadas al delito de suplantación de identidad, pues deben ser lo suficientemente severas para disuadir a los delincuentes de cometerlos (Entrevistado 2, 6 y 8).	Resaltando las respuestas convergentes de los expertos entrevistados, se considera que, actualmente se cuenta con el D.L. Nro 1412, Ley del Gobierno Digital, sin embargo esta ley no cuenta con lineamientos relacionados a los medios tecnológicos, para evitar el delitos de suplantación de identidad, también está la Ley Nro 30096, Ley de Delitos Informáticos, que contempla la prevención y sanción de este tipo de delitos, pero no abarca específicamente a los delitos por medios tecnológicos, por lo que, se observa que existe un vacío legal en el tratamiento de las nuevas modalidades de delito de suplantación de identidad; otra medida a modificar en el marco legislativo seria, la ampliación del

		ámbito de aplicación de la ley, pues debe abarcar no solo la suplantación de identidad, sino también, cualquier acción que pueda contribuir al delito, como la elaboración, venta o distribución de software malicioso o herramientas de suplantación de identidad.

<table>
<tr><th colspan="4">Pregunta Nro 8</th></tr>
<tr><td colspan="4">¿Mencione usted a su criterio profesional, si cree que los sistemas informáticos, ayudan a los delincuentes a cometer el delito del Phishing?</td></tr>
<tr><th>Entrevistado 1</th><th>Entrevistado 2</th><th>Entrevistado 3</th><th>Entrevistado 4</th></tr>
<tr><td>En mi criterio personal, sí creo que los sistemas informáticos ayudan a facilitar el delito de Phishing.</td><td>En este sentido si ayudan los medios informáticos a los delincuentes a delinquir de esta manera, sabiendo aún que los delincuentes son personas que estudian y se capacitan detalladamente todo el proceso en sí y como se generan estos dentro de los medios tecnológicos.</td><td>Los delincuentes jaquean siempre información, a través de las computadoras (medios informáticos).</td><td>Sí, a través de los medios informáticos, se puede acceder con facilidad a la información personal de los usuarios.</td></tr>
<tr><th>Entrevistado 5</th><th>Entrevistado 6</th><th>Entrevistado 7</th><th>Entrevistado 8</th></tr>
<tr><td>Sí, ya que estos medios sirven como un conducto para que los delincuentes puedan apropiarse de datos personales de terceros de manera más fácil, pues se aprovechan de la ingenuidad de personas que aún están aprendiendo a manejar los medios tecnológicos o se aprovechan un descuido para lograr obtener su cometido.</td><td>Sí, porque a través de las redes informáticas se puede acceder a datos almacenados de los clientes y al no contar con la seguridad informática estos pueden ser vulnerados.</td><td>Depende del tipo de seguridad que manejen los sistemas y ordenadores, ya que por lo general el phishing, cosiste en engañar al usuario para que éste brinde la información que ellos necesitan para cometer el delito.</td><td>Sí, los sistemas informáticos pueden ayudar a los delincuentes a cometer el delito de phishing de varias maneras, al igual que las TIC, por eso es importante que las empresas que desarrollan software se encuentren reguladas o cuenten con adecuados mecanismos de seguridad.</td></tr>
<tr><th colspan="2">Convergencias</th><th>Divergencias</th><th>Interpretación</th></tr>
<tr><td colspan="2">Los sistemas o medios informáticos, si ayudan y facilitan a los delincuentes a cometer el delito del Phishing (Entrevistado 1, 2, 4, 5 y 8).
Mediante los medios o sistemas informáticos, se puede acceder a información confidencial personal de terceros, para delinquir (Entrevistado 4, 5 y 6)
Los delincuentes, se aprovechan de la ignorancia, descuido e ingenuidad de los usuarios, que desconocen y que no manejan los medios informáticos y tecnológicos, para cometer los delitos de suplantación de identidad (Entrevistado 5 y 7)</td><td>Los delincuentes que cometen Phishing, son personas estudiosas y capacitadas en informática y medios tecnológicos para cometer dichos delitos (Entrevistado 2)
Los delincuentes hackean información a través de las computadoras (Entrevistado 3).
Las empresas que desarrollan software, deben estar reguladas y contar y garantizar adecuados mecanismos de seguridad (Entrevistado 8).</td><td>Resaltando las respuestas convergentes y divergentes de los expertos participantes, se considera que, los sistemas o medios informáticos, si ayudan y facilitan a cometer el delito de Phishing, pues los delincuentes que cometen esta modalidad de suplantación de identidad, son personas estudiosas y capacitadas en informática y medios tecnológicos, para poder ingresar mediante computadoras a distintos ordenadores y softwares y así poder hackear información, accediendo con</td></tr>
</table>

		facilidad a información personal de terceros, a veces aprovechándose de la ingenuidad, descuido e ignorancia de los usuarios que no manejan los medios informáticos y tecnológicos.

Pregunta Nro 9			
¿Mencione usted a su criterio profesional, si cree que las TIC, ayudan a los delincuentes a cometer el delito del Phishing?			
Entrevistado 1	**Entrevistado 2**	**Entrevistado 3**	**Entrevistado 4**
Sí, las Tecnología de la Información contribuyen a la realización del Phishing, puesto que remiten datos de identificación de información básicos que permiten identificar información sensible de los agraviados a través de sus redes sociales, como principal medio de escape o difusión.	Si ayudan a cometer el delito del Phishing, ya que las TIC se pueden usar para cosas buenas o malas.	Claro que sí.	Sí, los delincuentes utilizan las TICs para engañar a la población, asumiendo sus identidades.
Entrevistado 5	**Entrevistado 6**	**Entrevistado 7**	**Entrevistado 8**
Sí, las TICs son herramientas que aprovechan los delincuentes para poder engañar a los ciudadanos y lograr que entreguen su información personal.	Sí, porque a través del internet y la redes sociales, los delincuentes captan información para suplantar a terceros.	Sí, porque hoy en día todo se maneja mediante dispositivos tecnológicos, para la administración y distribución de la información de forma digitalizada. Las así llamadas TIC nos brindan un sinfín de beneficios. Esto también es utilizado por los delincuentes para cometer el phishing, así como otro tipo de delitos informáticos.	En efecto sí, y se debe en gran medida también al acceso a Internet sin restricción o sin los adecuados controles de seguridad, por lo tanto cualquier persona que quiera hacer daño y cuente con los conocimientos pueden utilizar la tecnología para cometer el delito del phishing de varias maneras, como por ejemplo: Los delincuentes pueden enviar correos electrónicos fraudulentos y crear sitios web falsos que parecen auténticos. Los delincuentes pueden utilizar técnicas de ingeniería social para engañar a los usuarios para que revelen información confidencial, como contraseñas y números de tarjetas de crédito. Estos correos electrónicos y sitios web falsos pueden ser muy convincentes, utilizando logos y diseños similares a los sitios web legítimos. Los delincuentes pueden enviar correos electrónicos de phishing a gran escala utilizando sistemas informáticos comprometidos como

			"bots" o "zombies". Los delincuentes pueden acceder a información personal y financiera de los usuarios a través de software malicioso o malware. Este software malicioso puede ser enviado a través de correos electrónicos o descargado desde sitios web infectados. Una vez que se instala en el sistema de un usuario, el malware puede recopilar información confidencial y enviarla a los delincuentes. En resumen, las TIC pueden ser utilizadas por los delincuentes para cometer el delito del phishing de varias maneras, por lo tanto, es importante que los usuarios estén conscientes de estas amenazas y tomen medidas para proteger su información en línea. Además, es importante que los sistemas informáticos estén protegidos por software de seguridad actualizado para evitar la infección por malware.
Convergencias		**Divergencias**	**Interpretación**
• Las TICs contribuyen a realizar el delito del Phishing, puesto que proporcionan herramientas como el internet y las redes sociales a los delincuentes cibernéticos, para captar información personal de terceros (Entrevistado 1, 2, 3, 6, 7 y 8). • Los delincuentes a través de las TICs, engañan a la población, para que entreguen información confidencial de ellos y así poder suplantarlos (Entrevistado 4 y 5).		• Los delincuentes a través de correos electrónicos y páginas web falsas, así también, utilizando métodos de ingeniería social, pueden captar información confidencial de terceros, como contraseñas de sus redes sociales, de sus correos electrónicos y de sus finanzas, para sacar beneficio de ello (Entrevistado 8). • Los delincuentes también pueden acceder a información personal y financiera de terceros a través de softwares maliciosos o malware, enviados a traes de correos electrónicos o links (Entrevistado 8).	Resaltando las respuestas convergentes y divergentes de los expertos participantes, se considera que, el mal uso de las TICs, contribuyen a realizar el delito del Phishing, puesto que proporcionan herramientas como las redes sociales y el internet sin restricciones y controles, es decir, los delincuentes informáticos, a través del malware y métodos de ingeniería social, utilizando correos electrónicos y páginas webs falsas y links peligroso, pueden captar información confidencial de terceros, como contraseñas de redes sociales, correos electrónicos y financieros,

		para suplantar la identidad de los usuarios y sacar provecho de ello.

Pregunta Nro 10			
¿Mencione usted a su criterio profesional, cree que los proveedores de sistemas informáticos y TIC, deben tener responsabilidad directa en el delito informático de suplantación de identidad, frente al usuario consumidor?			
Entrevistado 1	**Entrevistado 2**	**Entrevistado 3**	**Entrevistado 4**
Siempre y cuando haya de por medio un beneficio económico con la transmisión de información que identifique al usuario.	Sí, porque los proveedores de los medios tecnológicos son conocedores de toda la información personal de los usuarios.	Sí, pero si se aplica el sistema biométrico no podrán suplantar no podrán hacer nada.	Directamente no, porque la responsabilidad es indirecta, la responsabilidad debe caer en los terceros civiles, dado que deben tener el cuidado debido.
Entrevistado 5	**Entrevistado 6**	**Entrevistado 7**	**Entrevistado 8**
Sí, pero en algunos casos, como por ejemplo, cuando el proveedor sea una entidad bancaria, en esos casos el banco también debe tener responsabilidad frente al agraviado, pues ellos deberían haber tenido un procedimiento riguroso para hacer operaciones bancarias de retiro de dinero o compras con tarjeta de débito.	Los proveedores de los sistemas informáticos si deberían ser responsables solidarios a efectos de que en proceso eventual puedan resarcir el daño ocasionado.	Creo que el usuario consumidor es el encargado de proteger su información personal; asimismo los proveedores de sistemas y TIC, tienen responsabilidad si se ha vulnerado o robado la información de sus sistemas informáticos o bases de datos.	En general, los proveedores de sistemas informáticos y TIC no tienen una responsabilidad directa en el delito informático de suplantación de identidad, ya que este delito es cometido por terceros que utilizan las tecnologías de manera ilegal. Sin embargo, los proveedores de sistemas informáticos y TIC sí tienen la responsabilidad de garantizar que sus productos y servicios sean seguros y estén protegidos contra los ataques de suplantación de identidad y otros delitos informáticos. Esto incluye la implementación de medidas de seguridad adecuadas, la actualización constante del software y la capacitación del personal para detectar y responder a amenazas de seguridad. Además, en algunos casos, los proveedores de sistemas informáticos y TIC pueden ser responsables si se demuestra que han actuado negligentemente y han contribuido a la comisión del delito de suplantación de identidad. Por

			ejemplo, si un proveedor de servicios de correo electrónico no implementa medidas de seguridad adecuadas para proteger las cuentas de sus usuarios, y como resultado se produce una violación de seguridad que permite a los delincuentes robar información personal de los usuarios, el proveedor de servicios de correo electrónico podría ser considerado responsable de la violación.
Convergencias		**Divergencias**	**Interpretación**
• En general, los proveedores de sistemas informáticos y TIC no tienen una responsabilidad directa en el delito informático de suplantación de identidad, ya que este delito es cometido por terceros que utilizan las tecnologías de manera ilegal (Entrevistado 4 y 8). • Los proveedores de sistemas informáticos y TIC, tienen acceso a la información confidencial de las personas, por ende, tienen la responsabilidad de garantizar que sus productos y servicios sean seguros y estén protegidos contra los ataques de suplantación de identidad y otros delitos informáticos; esto incluye la implementación de sistemas biométricos y medidas de seguridad adecuadas, la actualización constante del software y la capacitación del personal para detectar y responder a amenazas de seguridad (Entrevistado 2, 3, 6 y 8). • Los proveedores de sistemas informáticos y TIC pueden ser responsables si se demuestra que han actuado negligentemente y han contribuido a la comisión del delito de suplantación de identidad (7 y 8).		• El usuario consumidor es el encargado de proteger su información personal (Entrevistado 7).	Resaltando las respuestas convergentes y divergentes de los expertos participantes, se considera que, los proveedores de las TIC no tienen una responsabilidad directa en el delito informático de suplantación de identidad, ya que este delito es cometido por terceros que utilizan las tecnologías de manera ilegal, por otra parte, dichos proveedores, si tienen acceso a la información confidencial de las personas, por ende, tienen la responsabilidad de garantizar que sus productos y servicios sean seguros y estén protegidos contra los ataques de suplantación de identidad; esto incluye implementación de sistemas biométricos y medidas de seguridad adecuadas, la actualización constante del software y la capacitación del personal para detectar y responder a amenazas de seguridad; los proveedores de las TIC, pueden ser responsables si se demuestra que han actuado negligentemente y han contribuido a la comisión del delito de suplantación de identidad.

ANEXO 5: ENTREVISTAS

Proyecto de Investigación

"Contribución de los Medios Tecnológicos en el Delito Informático de la Suplantación de Identidad en las Telecomunicaciones, Jaén 2022"

Estimado funcionario (a) o servidor (a) público:

INSTRUCCIONES: Agradecemos de antemano su buena disposición por colaborar con la presente investigación al atender a las preguntas planteadas y por brindarnos su valiosa opinión sobre el tema materia de investigación. Asimismo, cabe recalcar que la información brindada por su persona es de carácter confidencial y solo servirá para los fines de estudios de investigación científica. En este sentido, se le solicita responder, de acuerdo a su convicción y experiencia, así como de manera veraz, cada una de las siguientes interrogantes.

Datos Generales

- Nombre de la Persona Entrevistada: Martha Rosales Echevarría
- Profesión: Fiscal Provincial Penal
- Área/Oficina: Tercera Fiscalía Provincial Penal Corporativa de Trujillo
- Tiempo de Experiencia: más de 10 años de experiencia

CUESTIONARIO SOBRE EL DELITO INFORMÁTICO DE SUPLANTACIÓN DE IDENTIDAD

Desarrollo de la Entrevista:

1. ¿Conoce usted que es el delito de suplantación de identidad?

   Sí, es el delito que se comete utilizando las tecnologías de la información mediante el cual el sujeto activo se apropia de la identidad de una persona natural o jurídica.

2. ¿En el ámbito de su experiencia profesional, conoce que modalidades más comunes ejecutan los delincuentes para cometer el delito de suplantación de identidad?

   Entre modalidades más comunes de suplantación se encuentra las utilizadas para cometer: 1. fraude financiero como compras en línea, transferencias bancarias, etc; 2. Ciberbullying o acoso sexual y 3. Grooming o ganar la confianza de un menor y cometer abuso sexual contra este.

3. ¿En el ámbito de su experiencia profesional, usted cree que se debe modificar el marco legislativo relacionado al delito de suplantación de identidad, y que modificaciones plantearía?

   No estaría de acuerdo porque los tipos penales de suplantación poseen aspectos básicos que permiten que el operador jurídico, a través de una interpretación teleológica, sanciona la mayor cantidad de conductas posibles. Más aún, si los delitos informáticos presentan a lo largo de los años nuevas modalidades de comisión. En lo que si estaría de acuerdo, es que se invierta más en presupuesto y se constituya a nivel regional fiscalías especializadas en delitos informáticos, puesto que las diligencias tienen un carácter especializado y de poco dominio común por parte de las fiscalías corporativas.

4. ¿En el ámbito de su experiencia profesional, ha tenido casos relacionados al delito informático del Phishing, y cuál fue su tratamiento?

   Si, en esos casos se solicita que la entidad bancaria en la cual se ha sufrido la afectación proporcione la investigación interna y a partir de la misma se logre determinar si realmente se sufrió de una vulneración los datos privados financieros.

5. ¿En el ámbito de su experiencia profesional, usted, cree que existe falencias en las normas de protección al usuario en relación al delito de suplantación de identidad?

No, puesto que las normas de protección al usuario tienen cláusulas de no divulgación de información, que si son puesta al servicio de particulares contiene una sanción para la empresa. En donde, si puede haber una vulneración es a través de los sistemas informáticos.

UNIVERSIDAD CÉSAR VALLEJO

Proyecto de Investigación

"Contribución de los Medios Tecnológicos en el Delito Informático de la Suplantación de Identidad en las Telecomunicaciones, Jaén 2022"

Estimado funcionario (a) o servidor (a) público:

INSTRUCCIONES: Agradecemos de antemano su buena disposición por colaborar con la presente investigación al atender a las preguntas planteadas y por brindarnos su valiosa opinión sobre el tema materia de investigación. Asimismo, cabe recalcar que la información brindada por su persona es de carácter confidencial y solo servirá para los fines de estudios de investigación científica. En este sentido, se le solicita responder, de acuerdo a su convicción y experiencia, así como de manera veraz, cada una de las siguientes interrogantes.

Datos Generales

- Nombre de la Persona Entrevistada: Martha Rosales Echevarría
- Profesión: Fiscal Provincial Penal
- Área/Oficina: Tercera Fiscalía Provincial Penal Corporativa de Trujillo
- Tiempo de Experiencia: más de 10 años de experiencia

CUESTIONARIO SOBRE MEDIOS TECNOLÓGICOS

Desarrollo de la Entrevista:

6. ¿Mencione usted a su criterio profesional, si los medios tecnológicos contribuyen a cometer el delito informático de suplantación de identidad?

   Si, porque muchas los medios tecnológicos permiten la encriptación de información personal y no se puede identificar el dominio o IP responsable de los hechos delictivos.

7. ¿Mencione usted a su criterio profesional, si cree que se debe modificar el marco legislativo relacionado a los medios tecnológicos, con el propósito de evitar el delito de suplantación de identidad, y que modificaciones plantearía?

   Me ratifico que no sería necesario una modificación normativa.

8. ¿Mencione usted a su criterio profesional, si cree que los sistemas informáticos, ayudan a los delincuentes a cometer el delito del Phishing?

   En mi criterio personal, si creo que los sistemas informáticos ayudan a facilitar el delito de Phising, como expuse anteriormente.

9. ¿Mencione usted a su criterio profesional, si cree que las TIC, ayudan a los delincuentes a cometer el delito del Phishing?

   Las Tecnología de la Información si contribuyen a la realización del Phishing, puesto que remiten datos de identificación de información básicos que permiten identificar información sensible de los agraviados a través de sus redes sociales, como principal medio de escape o difusión.

10. ¿Mencione usted a su criterio profesional, cree que los proveedores de sistemas informáticos y TIC, deben tener responsabilidad directa en el delito informático de suplantación de identidad, frente al usuario consumidor?

    Siempre y cuando brinde haya de por medio un beneficio económico con la transmisión de información que identifique al usuario.

Proyecto de Investigación

“Contribución de los Medios Tecnológicos en el Delito Informático de la Suplantación de Identidad en las Telecomunicaciones, Jaén 2022”

Estimado funcionario (a) o servidor (a) público:

INSTRUCCIONES: Agradecemos de antemano su buena disposición por colaborar con la presente investigación al atender a las preguntas planteadas y por brindarnos su valiosa opinión sobre el tema materia de investigación. Asimismo, cabe recalcar que la información brindada por su persona es de carácter confidencial y solo servirá para los fines de estudios de investigación científica. En este sentido, se le solicita responder, de acuerdo a su convicción y experiencia, así como de manera veraz, cada una de las siguientes interrogantes.

Datos Generales

- Nombre de la Persona Entrevistada: JORGE CÉSAR RODRÍGUEZ GONZÁLEZ
- Profesión: ABOGADO
- Área/Oficina: ESTUDIO JURÍDICO RODRÍGUEZ & FLORES
- Tiempo de Experiencia: 25 AÑOS

CUESTIONARIO SOBRE EL DELITO INFORMÁTICO DE SUPLANTACIÓN DE IDENTIDAD

Desarrollo de la Entrevista:

1. ¿Conoce usted que es el delito de suplantación de identidad? Sí, es un delito regulado en el Código Penal peruano, donde un individuo suplanta el derecho de identidad de otra, causándole perjuicio económico y moral.

2. ¿En el ámbito de su experiencia profesional, conoce que modalidades más comunes ejecutan los delincuentes para cometer el delito de suplantación de identidad?

   Suplantación en el uso de las redes sociales
   Suplantación el teléfono celular

3. ¿En el ámbito de su experiencia profesional, usted cree que se debe modificar el marco legislativo relacionado al delito de suplantación de identidad, y que modificaciones plantearía?

   Si debiera modificarse el marco legislativo respecto al delito de suplantación de identidad.
   Las modificaciones que plantearía son las siguientes: aumentar la pena la pena privativa de libertad; y los días y multas no debieran darse en este delito.

4. ¿En el ámbito de su experiencia profesional, ha tenido casos relacionados al delito informático del Phishing, y cuál fue su tratamiento?

   No he tenido ningún caso relacionado al delito informático más si tengo conocimiento de ello ya que el delito informático del Phishing es la suplantación de identidad de las personas ya sea por medio de los sistemas informáticos, por medio de los correos electrónicos y los sitios web y así mismo lo realizan con las empresas.

5. ¿En el ámbito de su experiencia profesional, usted, cree que existe falencias en las normas de protección al usuario en relación al delito de suplantación de identidad?

   Si existen falacias en las normas de protección al usuario en relación al delito de suplantación de identidad las cuales debieran modificarse a favor del usuario, ya que lamentablemente esta protección al usuario solo es un saludo a la bandera.

Proyecto de Investigación

“Contribución de los Medios Tecnológicos en el Delito Informático de la Suplantación de Identidad en las Telecomunicaciones, Jaén 2022”

Estimado funcionario (a) o servidor (a) público:

INSTRUCCIONES: Agradecemos de antemano su buena disposición por colaborar con la presente investigación al atender a las preguntas planteadas y por brindarnos su valiosa opinión sobre el tema materia de investigación. Asimismo, cabe recalcar que la información brindada por su persona es de carácter confidencial y solo servirá para los fines de estudios de investigación científica. En este sentido, se le solicita responder, de acuerdo a su convicción y experiencia, así como de manera veraz, cada una de las siguientes interrogantes.

Datos Generales

- Nombre de la Persona Entrevistada: JORGE CÉSAR RODRÍGUEZ GONZÁLEZ
- Profesión: ABOGADO
- Área/Oficina: ESTUDIO JURÍDICO RODRÍGUEZ & FLORES
- Tiempo de Experiencia: 25 AÑOS

CUESTIONARIO SOBRE MEDIOS TECNOLÓGICOS

Desarrollo de la Entrevista:

6. ¿Mencione usted a su criterio profesional, si los medios tecnológicos contribuyen a cometer el delito informático de suplantación de identidad?

   Los medios tecnológicos no, sino que es la mala voluntad del ser humano al querer enriquecerse y aprovechar de los medios tecnológicos para su beneficio suplantando identidades.

7. ¿Mencione usted a su criterio profesional, si cree que se debe modificar el marco legislativo relacionado a los medios tecnológicos, con el propósito de evitar el delito de suplantación de identidad, y que modificaciones plantearía?

   Si deben modificar el marco legislativo ya que la pena privativa de libertad es muy leve en esta clase de delitos, sabiendo que muchas veces el robo através de estos medios tecnológicos son sumas demasiadas altas las cuales ya no se pueden devolver.

8. ¿Mencione usted a su criterio profesional, si cree que los sistemas informáticos, ayudan a los delincuentes a cometer el delito del Phishing?

   En este sentido si ayudan los medios informáticos a los delincuentes a delinquir de esta manera, sabiendo aún que los delincuentes son personas que estudian detalladamente todo el proceso en sí y como se generan estos dentro de los medios tecnológicos.

9. ¿Mencione usted a su criterio profesional, si cree que las TIC, ayudan a los delincuentes a cometer el delito del Phishing?

   Si ayudan a cometer el delito del Phishing ya que las TIC se pueden usar para cosas buenas o malas.

10. ¿Mencione usted a su criterio profesional, cree que los proveedores de sistemas informáticos y TIC, deben tener responsabilidad directa en el delito informático de suplantación de identidad, frente al usuario consumidor?

    A manera personal claro que sí, porque los proveedores son conocedores de toda la información personal de los usuarios.

Proyecto de Investigación

"Contribución de los Medios Tecnológicos en el Delito Informático de la Suplantación de Identidad en las Telecomunicaciones, Jaén 2022"

Estimado funcionario (a) o servidor (a) público:

INSTRUCCIONES: Agradecemos de antemano su buena disposición por colaborar con la presente investigación al atender a las preguntas planteadas y por brindarnos su valiosa opinión sobre el tema materia de investigación. Asimismo, cabe recalcar que la información brindada por su persona es de carácter confidencial y solo servirá para los fines de estudios de investigación científica. En este sentido, se le solicita responder, de acuerdo a su convicción y experiencia, así como de manera veraz, cada una de las siguientes interrogantes.

Datos Generales

- Nombre de la Persona Entrevistada: ELITER BARRANTES PRAD
- Profesión Abogado….
- Área/Oficina Pizarro 551 Of.202- Trujillo
- Tiempo de Experiencia: 22 años

CUESTIONARIO SOBRE EL DELITO INFORMÁTICO DE SUPLANTACIÓN DE IDENTIDAD

Desarrollo de la Entrevista:

1. ¿Conoce usted que es el delito de suplantación de identidad?

   Es cuando una persona usa las tecnologías para hacerse pasar por otra persona.

2. ¿En el ámbito de su experiencia profesional, conoce que modalidades más comunes ejecutan los delincuentes para cometer el delito de suplantación de identidad? Como modalidades conozco a la suplantación del usuario en las telecomunicaciones.

3. ¿En el ámbito de su experiencia profesional, usted cree que se debe modificar el marco legislativo relacionado al delito de suplantación de identidad, y que modificaciones plantearía? Si, plantearía aumentar las penas, porque son penas muy cortas.

4. ¿En el ámbito de su experiencia profesional, ha tenido casos relacionados al delito informático del Phishing, y cuál fue su tratamiento?, por lo general son archivados, porque es difícil de demostrar, y no se tiene profesionales expertos en la región.

5. ¿En el ámbito de su experiencia profesional, usted, cree que existe falencias en las normas de protección al usuario en relación al delito de suplantación de identidad? Si, tiene falencias, porque para que se haga efectivo, normalmente se tiene que comprar un seguro digital.

UNIVERSIDAD CÉSAR VALLEJO

Proyecto de Investigación

"Contribución de los Medios Tecnológicos en el Delito Informático de la Suplantación de Identidad en las Telecomunicaciones, Jaén 2022"

Estimado funcionario (a) o servidor (a) público:

INSTRUCCIONES: Agradecemos de antemano su buena disposición por colaborar con la presente investigación al atender a las preguntas planteadas y por brindarnos su valiosa opinión sobre el tema materia de investigación. Asimismo, cabe recalcar que la información brindada por su persona es de carácter confidencial y solo servirá para los fines de estudios de investigación científica. En este sentido, se le solicita responder, de acuerdo a su convicción y experiencia, así como de manera veraz, cada una de las siguientes interrogantes.

Datos Generales

- Nombre de la Persona Entrevistada: ELITER BARRANTES PRAD
- Profesión Abogado….
- Área/Oficina Pizarro 551 Of.202- Trujillo
- Tiempo de Experiencia: 22 años

CUESTIONARIO SOBRE MEDIOS TECNOLÓGICOS

Desarrollo de la Entrevista:

6. ¿Mencione usted a su criterio profesional, si los medios tecnológicos contribuyen a cometer el delito informático de suplantación de identidad?, utilizan generalmente el escáner para los documentos.

7. ¿Mencione usted a su criterio profesional, si cree que se debe modificar el marco legislativo relacionado a los medios tecnológicos, con el propósito de evitar el delito de suplantación de identidad, y que modificaciones plantearía? SI. toda persona para realizar un acto lo debe hacer a través de la huella digital, eso quiere decir que al momento de poner su huella en biométrico, le deben salir todos sus datos. Para el cual todos los biométricos deben estar vinculados a RENIEC.

8. ¿Mencione usted a su criterio profesional, si cree que los sistemas informáticos, ayudan a los delincuentes a cometer el delito del Phishing? los delincuentes jaquean siempre información.

9. ¿Mencione usted a su criterio profesional, si cree que las TIC, ayudan a los delincuentes a cometer el delito del Phishing? Claro que si

10. ¿Mencione usted a su criterio profesional, cree que los proveedores de sistemas informáticos y TIC, deben tener responsabilidad directa en el delito informático de suplantación de identidad, frente al usuario consumidor? Si, pero si se aplica el sistema biométrico no podrán suplantar no podrán hacer nada.

UNIVERSIDAD CÉSAR VALLEJO

Proyecto de Investigación

"Contribución de los Medios Tecnológicos en el Delito Informático de la Suplantación de Identidad en las Telecomunicaciones, Jaén 2022"

Estimado funcionario (a) o servidor (a) público:

INSTRUCCIONES: Agradecemos de antemano su buena disposición por colaborar con la presente investigación al atender a las preguntas planteadas y por brindarnos su valiosa opinión sobre el tema materia de investigación. Asimismo, cabe recalcar que la información brindada por su persona es de carácter confidencial y solo servirá para los fines de estudios de investigación científica. En este sentido, se le solicita responder, de acuerdo a su convicción y experiencia, así como de manera veraz, cada una de las siguientes interrogantes.

Datos Generales

- Nombre de la Persona Entrevistada: Marcelo Mego Fuentes
- Profesión: Abogado
- Área/Oficina: Asesoría y Consultoría Mego & Abogados E.I.R.L
- Tiempo de Experiencia: 18 años

CUESTIONARIO SOBRE EL DELITO INFORMÁTICO DE SUPLANTACIÓN DE IDENTIDAD

Desarrollo de la Entrevista:

1. ¿Conoce usted que es el delito de suplantación de identidad?

   Si. Es el delito por el cual se suplanta la identidad de una persona natural o jurídica, siempre que dicha conducta resulte algún perjuicio.

2. ¿En el ámbito de su experiencia profesional, conoce que modalidades más comunes ejecutan los delincuentes para cometer el delito de suplantación de identidad?

   - Fraude Financiero (compras en línea, transferencias bancarias, etc.)
   - Abuso Sexual
   - Estafa

3. ¿En el ámbito de su experiencia profesional, usted cree que se debe modificar el marco legislativo relacionado al delito de suplantación de identidad, y que modificaciones plantearía? Considero que sí. Incorporando además de la dotación de equipos tecnológicos para la investigación, porque de lo contrario no se podría llegar a saber quien o quienes son los responsables.
4. ¿En el ámbito de su experiencia profesional, ha tenido casos relacionados al delito informático del Phishing, y cuál fue su tratamiento? Sí. En realidad, nada o poco se pudo hacer porque en esta ciudad no contamos con los medios tecnológicos que permitan llegar a la verdad.
5. ¿En el ámbito de su experiencia profesional, usted, cree que existe falencias en las normas de protección al usuario en relación al delito de suplantación de identidad? Sí. Lamentablemente lo teorico se condice con la realidad, pues si bien la norma establece la pena aplicable al autor(es), sin embargo los medios con los que cuenta la autoridad q investiga son deficientes y con ello un caso impune.

UNIVERSIDAD CÉSAR VALLEJO

Proyecto de Investigación

"Contribución de los Medios Tecnológicos en el Delito Informático de la Suplantación de Identidad en las Telecomunicaciones, Jaén 2022"

Estimado funcionario (a) o servidor (a) público:

INSTRUCCIONES: Agradecemos de antemano su buena disposición por colaborar con la presente investigación al atender a las preguntas planteadas y por brindarnos su valiosa opinión sobre el tema materia de investigación. Asimismo, cabe recalcar que la información brindada por su persona es de carácter confidencial y solo servirá para los fines de estudios de investigación científica. En este sentido, se le solicita responder, de acuerdo a su convicción y experiencia, así como de manera veraz, cada una de las siguientes interrogantes.

Datos Generales

- Nombre de la Persona Entrevistada: Marcelo Mego Fuentes
- Profesión: Abogado
- Área/Oficina: Asesoría y Consultoría Mego & Abogados E.I.R.L.
- Tiempo de Experiencia: 18 años

CUESTIONARIO SOBRE MEDIOS TECNOLÓGICOS

Desarrollo de la Entrevista:

6. ¿Mencione usted a su criterio profesional, si los medios tecnológicos contribuyen a cometer el delito informático de suplantación de identidad?
Sí, Si bien ahora se ha convertido en una ayuda importante para la celeridad de los operaciones, tambien permiten a los delincuentes tener acceso con Facilidad a la información.
7. ¿Mencione usted a su criterio profesional, si cree que se debe modificar el marco legislativo relacionado a los medios tecnológicos, con el propósito de evitar el delito de suplantación de identidad, y que modificaciones plantearía?
considero que NO, lo que se debe agregar es dotar de medios tecnologicos para Investigar los delitos tecnologicos.
8. ¿Mencione usted a su criterio profesional, si cree que los sistemas informáticos, ayudan a los delincuentes a cometer el delito del Phishing?
Sí, Pues pueden acceder con Facilidad a la información de las personas.
9. ¿Mencione usted a su criterio profesional, si cree que las TIC, ayudan a los delincuentes a cometer el delito del Phishing?
Sí, Pues aprovechan los medios tecnologicos para engañar a la Población utilizando incluso identidades de otras personas.
10. ¿Mencione usted a su criterio profesional, cree que los proveedores de sistemas informáticos y TIC, deben tener responsabilidad directa en el delito informático de suplantación de identidad, frente al usuario consumidor?
Directa no creo, xq la responsabilidad es directa, sin embargo considero que deben ser terceros civiles responsables, dado a que deben tener el cuidado debido.

Proyecto de Investigación

"Contribución de los Medios Tecnológicos en el Delito Informático de la Suplantación de Identidad en las Telecomunicaciones, Jaén 2022"

Estimado funcionario (a) o servidor (a) público:

INSTRUCCIONES: Agradecemos de antemano su buena disposición por colaborar con la presente investigación al atender a las preguntas planteadas y por brindarnos su valiosa opinión sobre el tema materia de investigación. Asimismo, cabe recalcar que la información brindada por su persona es de carácter confidencial y solo servirá para los fines de estudios de investigación científica. En este sentido, se le solicita responder, de acuerdo a su convicción y experiencia, así como de manera veraz, cada una de las siguientes interrogantes.

Datos Generales

- Nombre de la Persona Entrevistada: Elia Milagros Lujan Avalos
- Profesión…Abogada especializada en área penal……..
- Área/Oficina…Estudio Jurídico Valera & Ortiz…….
- Tiempo de Experiencia: ……10 año…….

CUESTIONARIO SOBRE EL DELITO INFORMÁTICO DE SUPLANTACIÓN DE IDENTIDAD

Desarrollo de la Entrevista:

1. ¿Conoce usted que es el delito de suplantación de identidad? Sí, es un delito que muchas veces utiliza los sistemas informáticos, que consiste en usurpar la identidad de una persona, ocasionándole daños

2. ¿En el ámbito de su experiencia profesional, conoce que modalidades más comunes ejecutan los delincuentes para cometer el delito de suplantación de identidad? modalidad de suplantación a través de las tarjetas bancarias (débito o crédito), cuando envían link y extraen información del sujeto agraviado para posteriormente sacar dinero de las cuentas bancarias o hacer compras en línea.

3. ¿En el ámbito de su experiencia profesional, usted cree que se debe modificar el marco legislativo relacionado al delito de suplantación de identidad, y que modificaciones plantearía? Sí, en primera sería bueno que los delitos informáticos sean incorporados dentro del Código Penal, pues al encontrarse en una legislación separada, muy pocas personas conoces sobre este delito; en segunda, en cuanto al delito de suplantación de identidad la norma debería modificarse en el extremo de la pena y debería especificarse que la acción típica del delito consiste en adoptar, crear, apropiarse o utilizar la identidad de una persona, en cualquier sistema informático, medio de comunicación o por cualquier otro medio.
4. ¿En el ámbito de su experiencia profesional, ha tenido casos relacionados al delito informático del Phishing, y cuál fue su tratamiento? Sí, en la mayoría de casos debido a que no se lograba encontrar a las personas responsables, se terminaban archivando.

5. ¿En el ámbito de su experiencia profesional, usted, cree que existe falencias en las normas de protección al usuario en relación al delito de suplantación de identidad? sí, pero más que todo el usuario no conoce todos sus derechos.

UNIVERSIDAD CÉSAR VALLEJO

Proyecto de Investigación

"Contribución de los Medios Tecnológicos en el Delito Informático de la Suplantación de Identidad en las Telecomunicaciones, Jaén 2022"

Estimado funcionario (a) o servidor (a) público:

INSTRUCCIONES: Agradecemos de antemano su buena disposición por colaborar con la presente investigación al atender a las preguntas planteadas y por brindarnos su valiosa opinión sobre el tema materia de investigación. Asimismo, cabe recalcar que la información brindada por su persona es de carácter confidencial y solo servirá para los fines de estudios de investigación científica. En este sentido, se le solicita responder, de acuerdo a su convicción y experiencia, así como de manera veraz, cada una de las siguientes interrogantes.

Datos Generales

- Nombre de la Persona Entrevistada: Elia Milagros Lujan Avalos
- Profesión…Abogada especializada en área penal……..
- Área/Oficina…Estudio Jurídico Valera & Ortiz…….
- Tiempo de Experiencia: ……10 año…….

CUESTIONARIO SOBRE MEDIOS TECNOLÓGICOS

Desarrollo de la Entrevista:

6. ¿Mencione usted a su criterio profesional, si los medios tecnológicos contribuyen a cometer el delito informático de suplantación de identidad? Sí, debido a que nuestra sociedad actualmente funciona por los medios tecnológicos, estos se han convertido en las actuales herramientas para cometer actos delictivos.

7. ¿Mencione usted a su criterio profesional, si cree que se debe modificar el marco legislativo relacionado a los medios tecnológicos, con el propósito de evitar el delito de suplantación de identidad, y que modificaciones plantearía? No, considero que la palabra medios tecnológicos es un concepto amplio que abarca muchas modalidades de suplantación de identidad a través del uso de la tecnología.

8. ¿Mencione usted a su criterio profesional, si cree que los sistemas informáticos, ayudan a los delincuentes a cometer el delito del Phishing? Efectivamente que sí, ya que estos medios sirven como un conducto para que los delincuentes puedan apropiarse de datos personales de terceros de manera más fácil, pues se aprovecha de la ingenuidad

de personas que aún están aprendiendo a manejar los medios tecnológicos o aprovechan un descuido de las personas para lograr obtener su cometido.

9. ¿Mencione usted a su criterio profesional, si cree que las TIC, ayudan a los delincuentes a cometer el delito del Phishing? Sí, son estos medios de información, las herramientas que aprovechan los delincuentes para poder engañar a los ciudadanos y lograr que entreguen su información personal.

10. ¿Mencione usted a su criterio profesional, cree que los proveedores de sistemas informáticos y TIC, deben tener responsabilidad directa en el delito informático de suplantación de identidad, frente al usuario consumidor? Considero que sí, pero en algunos casos, como por ejemplo cuando el proveedor sea una entidad bancaria, en estos casos el Banco también debe tener responsabilidad frente al agraviado, pues ellos deberían haber tenido un procedimiento riguroso para hacer operaciones bancarias de retiro de dinero o compras con tarjeta de débito.

Proyecto de Investigación

"Contribución de los Medios Tecnológicos en el Delito Informático de la Suplantación de Identidad en las Telecomunicaciones, Jaén 2022"

Estimado funcionario (a) o servidor (a) público:

INSTRUCCIONES: Agradecemos de antemano su buena disposición por colaborar con la presente investigación al atender a las preguntas planteadas y por brindarnos su valiosa opinión sobre el tema materia de investigación. Asimismo, cabe recalcar que la información brindada por su persona es de carácter confidencial y solo servirá para los fines de estudios de investigación científica. En este sentido, se le solicita responder, de acuerdo a su convicción y experiencia, así como de manera veraz, cada una de las siguientes interrogantes.

Datos Generales

- Nombre de la Persona Entrevistada: Alicia Sadit Chavez Vasquez
- Profesión Abogada
- Área/Oficina Asesoría Jurídica
- Tiempo de Experiencia: 6 años.

CUESTIONARIO SOBRE EL DELITO INFORMÁTICO DE SUPLANTACIÓN DE IDENTIDAD

Desarrollo de la Entrevista:

1. ¿Conoce usted que es el delito de suplantación de identidad?, comente.
   El delito de suplantación de identidad radica en hacerse pasar por otra persona este tipo de delitos están normados en el Código Penal Peruano, existen delito de suplantación de identidad tanto en materia electoral como en materia informática **Artículo 9** de la Ley Nº 30096

2. ¿En el ámbito de su experiencia profesional, conoce que modalidades más comunes ejecutan los delincuentes para cometer el delito de suplantación de identidad?, creación de cuentas falsas en redes sociales

3. ¿En el ámbito de su experiencia profesional, usted cree que se debe modificar el marco legislativo relacionado al delito de suplantación de identidad, y que modificaciones plantearía? Considero que debería tener penas más altas y que se deben implementar métodos de seguridad y confiabilidad que no permitan crear cuentas falsas.

4. ¿En el ámbito de su experiencia profesional, ha tenido casos relacionados al delito informático del Phishing, y cuál fue su tratamiento?, NO

5. ¿En el ámbito de su experiencia profesional, usted, cree que existe falencias en las normas de protección al usuario en relación al delito de suplantación de identidad?, Las diligencias de la policía cibernética deben ser más céleres

UNIVERSIDAD CÉSAR VALLEJO

Proyecto de Investigación

"Contribución de los Medios Tecnológicos en el Delito Informático de la Suplantación de Identidad en las Telecomunicaciones, Jaén 2022"

Estimado funcionario (a) o servidor (a) público:

INSTRUCCIONES: Agradecemos de antemano su buena disposición por colaborar con la presente investigación al atender a las preguntas planteadas y por brindarnos su valiosa opinión sobre el tema materia de investigación. Asimismo, cabe recalcar que la información brindada por su persona es de carácter confidencial y solo servirá para los fines de estudios de investigación científica. En este sentido, se le solicita responder, de acuerdo a su convicción y experiencia, así como de manera veraz, cada una de las siguientes interrogantes.

Datos Generales

- Nombre de la Persona Entrevistada: Alicia Sadit Chavez Vasquez

- Profesión Abogada
- Área/Oficina Asesoría Jurídica
- Tiempo de Experiencia: 6 años

CUESTIONARIO SOBRE MEDIOS TECNOLÓGICOS

Desarrollo de la Entrevista:

6. ¿Mencione usted a su criterio profesional, si los medios tecnológicos contribuyen a cometer el delito informático de suplantación de identidad?, comente.
   En el ámbito tecnológico existen muchas facilidades de que se creen cuentas falsas atribuyendo hechos o efectuando adquisiciones a nombre de terceros

7. ¿Mencione usted a su criterio profesional, si cree que se debe modificar el marco legislativo relacionado a los medios tecnológicos, con el propósito de evitar el delito de suplantación de identidad, y que modificaciones plantearía?, si las medidas de seguridad deberían incrementarse

8. ¿Mencione usted a su criterio profesional, si cree que los sistemas informáticos, ayudan a los delincuentes a cometer el delito del Phishing?, si porque a través de la red se puede acceder a datos almacenados de los clientes y al no contar con la seguridad informática estos pueden ser vulnerados

9. ¿Mencione usted a su criterio profesional, si cree que las TIC, ayudan a los delincuentes a cometer el delito del Phishing?, sí, porque a través del internet y la redes sociales, los delincuentes captan información para suplantar a terceros.

10. ¿Mencione usted a su criterio profesional, cree que los proveedores de sistemas informáticos y TIC, deben tener responsabilidad directa en el delito informático de suplantación de identidad, frente al usuario consumidor?, Los proveedor de los sistemas informáticos si deberían ser responsables solidarios a efectos de que en proceso eventual puedan resarcir el daño ocasionado.

Proyecto de Investigación

"Contribución de los Medios Tecnológicos en el Delito Informático de la Suplantación de Identidad en las Telecomunicaciones, Jaén 2022"

Estimado funcionario (a) o servidor (a) público:

INSTRUCCIONES: Agradecemos de antemano su buena disposición por colaborar con la presente investigación al atender a las preguntas planteadas y por brindarnos su valiosa opinión sobre el tema materia de investigación. Asimismo, cabe recalcar que la información brindada por su persona es de carácter confidencial y solo servirá para los fines de estudios de investigación científica. En este sentido, se le solicita responder, de acuerdo a su convicción y experiencia, así como de manera veraz, cada una de las siguientes interrogantes.

Datos Generales

- Nombre de la Persona Entrevistada: Anndy E. Carrasco Rivera
- Profesión: Ingeniería Informática y de Sistemas
- Área/Oficina: Unidad de Sistemas y Soporte Tecnológico
- Tiempo de Experiencia: 14 años

CUESTIONARIO SOBRE EL DELITO INFORMÁTICO DE SUPLANTACIÓN DE IDENTIDAD

Desarrollo de la Entrevista:

1. ¿Conoce usted que es el delito de suplantación de identidad?
   Sí, la suplantación de identidad, son acciones de una persona que tiene el fin de apropiarse de la identidad de otro individuo, para obtener beneficios ilícitos de dicho acto; por lo general estos tipos de actos se realizan digitalmente, mediante el uso de la tecnología.

2. ¿En el ámbito de su experiencia profesional, conoce que modalidades más comunes ejecutan los delincuentes para cometer el delito de suplantación de identidad?
   El Pishing, a través emails recepcionados, ingresos a páginas peligrosas y/o llamadas telefónicas, donde roban información personal y financiera para suplantar

3. ¿En el ámbito de su experiencia profesional, usted cree que se debe modificar el marco legislativo relacionado al delito de suplantación de identidad, y que modificaciones plantearía? Desconozco el marco legislativo, pero creo que se debería tener en cuenta el tipo de delito y el daño causado. Ya que el término suplantación de identidad engloba un campo muy extenso.

4. ¿En el ámbito de su experiencia profesional, ha tenido casos relacionados al delito informático del Phishing, y cuál fue su tratamiento?
   Sí, pero por lo general son difíciles de demostrar.

5. ¿En el ámbito de su experiencia profesional, usted, cree que existe falencias en las normas de protección al usuario en relación al delito de suplantación de identidad?
   Definitivamente, existen a diario casos de víctimas de robos cibernéticos, estafas, entre otras y usuarios que denuncian pero que no obtienen solución alguna.

Proyecto de Investigación

“Contribución de los Medios Tecnológicos en el Delito Informático de la Suplantación de Identidad en las Telecomunicaciones, Jaén 2022”

Estimado funcionario (a) o servidor (a) público:

INSTRUCCIONES: Agradecemos de antemano su buena disposición por colaborar con la presente investigación al atender a las preguntas planteadas y por brindarnos su valiosa opinión sobre el tema materia de investigación. Asimismo, cabe recalcar que la información brindada por su persona es de carácter confidencial y solo servirá para los fines de estudios de investigación científica. En este sentido, se le solicita responder, de acuerdo a su convicción y experiencia, así como de manera veraz, cada una de las siguientes interrogantes.

Datos Generales

- Nombre de la Persona Entrevistada: Anndy E. Carrasco Rivera
- Profesión: Ingeniería Informática y de Sistemas
- Área/Oficina: Unidad de Sistemas y Soporte Tecnológico
- Tiempo de Experiencia: 14 años

CUESTIONARIO SOBRE MEDIOS TECNOLÓGICOS

Desarrollo de la Entrevista:

6. ¿Mencione usted a su criterio profesional, si los medios tecnológicos contribuyen a cometer el delito informático de suplantación de identidad? Por lo general se hace por medio de computadoras, celulares, vía telefónica, skimmer para tarjetas de banco, dispositivo tipo POS para leer chip de tarjetas por acercamiento, entre otros.

7. ¿Mencione usted a su criterio profesional, si cree que se debe modificar el marco legislativo relacionado a los medios tecnológicos, con el propósito de evitar el delito de suplantación de identidad, y que modificaciones plantearía? Si, se debería, mejorar mucho en cuanto a delitos de suplantación, así como delitos cibernéticos en general.

8. ¿Mencione usted a su criterio profesional, si cree que los sistemas informáticos, ayudan a los delincuentes a cometer el delito del Phishing? Depende del tipo de seguridad que manejen los sistemas y ordenadores, ya que por genera el phishing cosiste en engañar al usuario para que éste brinde la información que ellos necesitan para cometer el delito.

9. ¿Mencione usted a su criterio profesional, si cree que las TIC, ayudan a los delincuentes a cometer el delito del Phishing?
   Por su puesto, hoy en día todo se maneja mediante dispositivos tecnológicos, para la administración y distribución de la información de forma digitalizada. Las así llamadas TIC nos brindan un sinfín de beneficios. Esto también es utilizado por los delincuentes para cometer el phishing, así como otro tipo de delitos informáticos.

10. ¿Mencione usted a su criterio profesional, cree que los proveedores de sistemas informáticos y TIC, deben tener responsabilidad directa en el delito informático de suplantación de identidad, frente al usuario consumidor?
    Creo que el usuario consumidor es el encargado de proteger su información personal; asimismo los proveedores de sistemas y TIC, tienen responsabilidad si se ha vulnerado o robado la información de sus sistemas informáticos o bases de datos.

Proyecto de Investigación

"Contribución de los Medios Tecnológicos en el Delito Informático de la Suplantación de Identidad en las Telecomunicaciones, Jaén 2022"

Estimado funcionario (a) o servidor (a) público:

INSTRUCCIONES: Agradecemos de antemano su buena disposición por colaborar con la presente investigación al atender a las preguntas planteadas y por brindarnos su valiosa opinión sobre el tema materia de investigación. Asimismo, cabe recalcar que la información brindada por su persona es de carácter confidencial y solo servirá para los fines de estudios de investigación científica. En este sentido, se le solicita responder, de acuerdo a su convicción y experiencia, así como de manera veraz, cada una de las siguientes interrogantes.

Datos Generales

- Nombre de la Persona Entrevistada: Rodrigo Masías Carmona
- Profesión: Ing. De Sistemas
- Área/Oficina: Oficina de Tecnologías de la Información
- Tiempo de Experiencia: 10 años

CUESTIONARIO SOBRE EL DELITO INFORMÁTICO DE SUPLANTACIÓN DE IDENTIDAD

Desarrollo de la Entrevista:

1. ¿Conoce usted que es el delito de suplantación de identidad?
   Sí, es un delito que consiste en utilizar la identidad de otra persona sin su autorización y con fines ilícitos.

2. ¿En el ámbito de su experiencia profesional, conoce que modalidades más comunes ejecutan los delincuentes para cometer el delito de suplantación de identidad?
   Si, entre las más comunes que conozco está el *SIM swapping*, o la suplantación de la tarjeta SIM del móvil, una modalidad que ha cobrado fuerza en varios países y también aquí en Perú, también está el Phishing, fraude en línea, fraude telefónico, robo de identidad en redes sociales, entre otros.

   Es importante tener en cuenta que estas modalidades pueden ser muy sofisticadas y que los delincuentes pueden utilizar técnicas avanzadas para engañar a las víctimas. Por eso, es fundamental ser cauteloso con la información personal y financiera y tomar medidas para protegerla, como mantener contraseñas seguras y no compartir información personal por correo electrónico o mensaje de texto.

3. ¿En el ámbito de su experiencia profesional, usted cree que se debe modificar el marco legislativo relacionado al delito de suplantación de identidad, y que modificaciones plantearía?
   Sí, considero que se debe revisar y actualizar el marco legislativo (Ley Nº 30096 o Ley de delitos informáticos) para abordar adecuadamente estas amenazas emergentes, sobre todo si se trata de temas relacionados a las TIC que cambian constantemente, una posible modificación que plantearía sería:

   Definir claramente los delitos relacionados con la suplantación de identidad en el ámbito digital en sus diferentes modalidades, incluyendo *SIM swapping,* la creación de perfiles falsos en redes sociales, el phishing y el fraude en línea, aunque este último fue actualizado en la Ley N° 30171 (Ley que modifica la Ley 30096, Ley de Delitos Informáticos).

   Sin embargo, no sólo debe quedar en un marco, debe haber un seguimiento continuo para ser efectivo el cumplimiento de las definiciones establecidas, y para lograrlo es importante fomentar la cooperación internacional para perseguir a los delincuentes que comenten delitos de suplantación de identidad a través de Internet, ya que este tipo de delito a menudo tiene implicaciones transfronterizas, proporcionar más recursos a las autoridades encargadas de investigar y perseguir los delitos relacionados con la suplantación de identidad, incluyendo la formación en tecnología y la colaboración con expertos en ciberseguridad asi como también educar a la población sobre cómo proteger su

información personal y financiera y cómo reconocer y evitar los intentos de suplantación de identidad.

4. ¿En el ámbito de su experiencia profesional, ha tenido casos relacionados al delito informático del Phishing, y cuál fue su tratamiento?
   Si, de hecho el Phishing es uno de los más comunes, y los que llegan a través de correo electrónico, sin embargo, en la empresa se cuentan con herramientas de seguridad, tanto a nivel interno y externo (proveedores de Internet) que detectan a tiempo este tipo de ataques, en la mayoría de los casos, el contar con este tipo de herramientas y con una certificación en Seguridad de la Información (SGSI ISO 27001) nos ha permitido mitigar los riesgos que conllevan este tipo de ataques, y sobre todo prevenirlos, que es lo mas importante. Los diferentes controles aplicados por medio del SGSI ayudan a mantenernos actualizados y alertas contra todo tipo de ataques y vulnerabilidades, además de mantener siempre informados y capacitados a los usuarios de la empresa.

5. ¿En el ámbito de su experiencia profesional, usted, cree que existe falencias en las normas de protección al usuario en relación al delito de suplantación de identidad?
   Una de las principales falencias en la regulación es que la suplantación de identidad puede ser difícil de detectar y prevenir, especialmente en línea. Las plataformas digitales y las redes sociales pueden ser utilizadas por los delincuentes para hacerse pasar por otra persona y obtener información personal o cometer fraudes. Es necesario mejorar la regulación y la implementación de medidas de seguridad en línea para proteger a los usuarios de estos delitos.

   Además, otra falencia en la regulación es que puede ser difícil procesar y castigar a los delincuentes que cometen suplantación de identidad. En algunos casos, puede ser difícil identificar al delincuente o recopilar pruebas suficientes para condenarlos. Las leyes y los procesos penales deben ser mejorados para facilitar la investigación y el enjuiciamiento de los delitos de suplantación de identidad.

   En resumen, es necesario mejorar la regulación y la implementación de medidas de seguridad en línea y fortalecer los procesos penales para investigar y enjuiciar a los delincuentes que cometen este tipo de delitos.

Proyecto de Investigación

"Contribución de los Medios Tecnológicos en el Delito Informático de la Suplantación de Identidad en las Telecomunicaciones, Jaén 2022"

Estimado funcionario (a) o servidor (a) público:

INSTRUCCIONES: Agradecemos de antemano su buena disposición por colaborar con la presente investigación al atender a las preguntas planteadas y por brindarnos su valiosa opinión sobre el tema materia de investigación. Asimismo, cabe recalcar que la información brindada por su persona es de carácter confidencial y solo servirá para los fines de estudios de investigación científica. En este sentido, se le solicita responder, de acuerdo a su convicción y experiencia, así como de manera veraz, cada una de las siguientes interrogantes.

Datos Generales

- Nombre de la Persona Entrevistada: Rodrigo Masías Carmona
- Profesión: Ing. De Sistemas
- Área/Oficina: Oficina de Tecnologías de la Información
- Tiempo de Experiencia: 10 años

CUESTIONARIO SOBRE MEDIOS TECNOLÓGICOS

Desarrollo de la Entrevista:

6. ¿Mencione usted a su criterio profesional, si los medios tecnológicos contribuyen a cometer el delito informático de suplantación de identidad?

   Sí, los medios tecnológicos pueden contribuir significativamente, en particular, los avances en la tecnología de la información y la comunicación han hecho que sea más fácil para los delincuentes suplantar la identidad de otra persona y cometer fraudes.

Por ejemplo, los correos electrónicos falsos y las páginas web falsas pueden ser creadas para hacer que el destinatario crea que está interactuando con una persona o entidad legítima, cuando en realidad es un delincuente que está intentando obtener información personal o financiera. Además, los delincuentes pueden utilizar técnicas de phishing para engañar a las personas para que revelen información confidencial, como contraseñas o números de tarjetas de crédito.

También existen aplicaciones y herramientas en línea que pueden ser utilizadas para suplantar la identidad de una persona. Por ejemplo, las aplicaciones de falsificación de llamadas pueden hacer que una llamada parezca que proviene de un número de teléfono diferente, lo que puede permitir que los delincuentes realicen fraudes telefónicos. Los servicios de correo electrónico anónimos también pueden ser utilizados para ocultar la identidad del remitente de un correo electrónico malintencionado.

7. ¿Mencione usted a su criterio profesional, si cree que se debe modificar el marco legislativo relacionado a los medios tecnológicos, con el propósito de evitar el delito de suplantación de identidad, y que modificaciones plantearía?

   Actualmente contamos con el Decreto Legislativo N.° 1412, que aprueba la Ley de Gobierno Digital, sin embargo esta Ley no cuenta con lineamientos relacionado a los medios tecnológicos con el propósito de evitar el delito de suplantación de identidad, y la Ley Nº 30096 o Ley de delitos informáticos contempla la prevención y sanción de este tipo de delitos, pero no abarca medios tecnológicos, por lo que se observa que existe una brecha respecto a este tema que sería importante incluirlos en ambos marcos legislativos.

   Algunas modificaciones que podrían ser consideradas en el marco legislativo para evitar el delito de suplantación de identidad podrían ser:

   Ampliación del ámbito de aplicación: La ley debe abarcar no solo la suplantación de identidad, sino también cualquier acción que pueda contribuir al delito, como la elaboración, venta o distribución de software malicioso o herramientas de suplantación de identidad.

Fortalecimiento de la responsabilidad de los proveedores de servicios en línea: Los proveedores de servicios en línea deben ser responsables de proporcionar medidas de seguridad efectivas para prevenir la suplantación de identidad. Además, deben tener la obligación de notificar a los usuarios si se produce una brecha de seguridad que pueda afectar su información personal.

Aumento de las sanciones y penas: Las sanciones y penas para los delitos de suplantación de identidad deben ser lo suficientemente severas para disuadir a los delincuentes de cometerlos.

Fortalecimiento de la cooperación internacional: Los delitos de suplantación de identidad en línea a menudo cruzan las fronteras nacionales, por lo que es necesario fortalecer la cooperación internacional entre las autoridades encargadas de hacer cumplir la ley para investigar y enjuiciar a los delincuentes.

Las modificaciones propuestas deben fortalecer la responsabilidad de los proveedores de servicios en línea, aumentar las sanciones y penas, y mejorar la cooperación internacional.

8. ¿Mencione usted a su criterio profesional, si cree que los sistemas informáticos, ayudan a los delincuentes a cometer el delito del Phishing?

   Sí, los sistemas informáticos pueden ayudar a los delincuentes a cometer el delito de phishing de varias maneras, al igual que las TIC, por eso es importante que las empresas que desarrollan software se encuentren reguladas o cuenten con adecuados mecanismos de seguridad.

9. ¿Mencione usted a su criterio profesional, si cree que las TIC, ayudan a los delincuentes a cometer el delito del Phishing?

   En efecto si, y se debe en gran medida también al acceso a Internet sin restricción o sin los adecuados controles de seguridad, por lo tanto cualquier persona que quiera hacer daño y cuente con los conocimientos pueden utilizar la tecnología para cometer el delito del phishing de varias maneras, como por ejemplo:

   Los delincuentes pueden enviar correos electrónicos fraudulentos y crear sitios web falsos que parecen auténticos. Los delincuentes pueden utilizar técnicas de

ingeniería social para engañar a los usuarios para que revelen información confidencial, como contraseñas y números de tarjetas de crédito. Estos correos electrónicos y sitios web falsos pueden ser muy convincentes, utilizando logos y diseños similares a los sitios web legítimos.

Los delincuentes pueden enviar correos electrónicos de phishing a gran escala utilizando sistemas informáticos comprometidos como "bots" o "zombies". Estos sistemas informáticos pueden ser utilizados para enviar correos electrónicos fraudulentos a gran escala, lo que hace que sea más difícil para las autoridades detectar y detener a los delincuentes.

Los delincuentes pueden acceder a información personal y financiera de los usuarios a través de software malicioso o malware. Este software malicioso puede ser enviado a través de correos electrónicos o descargado desde sitios web infectados. Una vez que se instala en el sistema de un usuario, el malware puede recopilar información confidencial y enviarla a los delincuentes.

En resumen, las TIC pueden ser utilizadas por los delincuentes para cometer el delito del phishing de varias maneras, por lo tanto, es importante que los usuarios estén conscientes de estas amenazas y tomen medidas para proteger su información en línea. Además, es importante que los sistemas informáticos estén protegidos por software de seguridad actualizado para evitar la infección por malware.

10. ¿Mencione usted a su criterio profesional, cree que los proveedores de sistemas informáticos y TIC, deben tener responsabilidad directa en el delito informático de suplantación de identidad, frente al usuario consumidor?

    En general, los proveedores de sistemas informáticos y TIC no tienen una responsabilidad directa en el delito informático de suplantación de identidad, ya que este delito es cometido por terceros que utilizan las tecnologías de manera ilegal.

    Sin embargo, los proveedores de sistemas informáticos y TIC sí tienen la responsabilidad de garantizar que sus productos y servicios sean seguros y estén protegidos contra los ataques de suplantación de identidad y otros delitos

informáticos. Esto incluye la implementación de medidas de seguridad adecuadas, la actualización constante del software y la capacitación del personal para detectar y responder a amenazas de seguridad.

Además, en algunos casos, los proveedores de sistemas informáticos y TIC pueden ser responsables si se demuestra que han actuado negligentemente y han contribuido a la comisión del delito de suplantación de identidad. Por ejemplo, si un proveedor de servicios de correo electrónico no implementa medidas de seguridad adecuadas para proteger las cuentas de sus usuarios, y como resultado se produce una violación de seguridad que permite a los delincuentes robar información personal de los usuarios, el proveedor de servicios de correo electrónico podría ser considerado responsable de la violación.

UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE DERECHO Y HUMANIDADES

ESCUELA PROFESIONAL DE DERECHO

Declaratoria de Autenticidad del Asesor

Yo, RIOS SÁNCHEZ WILFREDO, docente de la FACULTAD DE DERECHO Y HUMANIDADES de la escuela profesional de DERECHO de la UNIVERSIDAD CÉSAR VALLEJO SAC - TRUJILLO, asesor de Tesis titulada: "Contribución de los Medios Tecnológicos en el Delito Informático de la Suplantación de Identidad en las Telecomunicaciones , Jaén 2022", cuyos autores son FLORES MACHUCA MOISES ALCIDES, URIARTE PEREZ GREYCI SHERALDINE, constato que la investigación tiene un índice de similitud de 12.00%, verificable en el reporte de originalidad del programa Turnitin, el cual ha sido realizado sin filtros, ni exclusiones.

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

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

TRUJILLO, 08 de Abril del 2023

Apellidos y Nombres del Asesor:	**Firma**
RIOS SÁNCHEZ WILFREDO **DNI:** 18161730 **ORCID:** 0000-0003-4569-3771	Firmado electrónicamente por: RRIOSSA10 el 08-04-2023 18:17:20

Código documento Trilce: TRI - 0540973

INVESTIGA UCV