UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE DERECHO Y HUMANIDADES

ESCUELA PROFESIONAL DE DERECHO

Propuesta modificatoria de artículos 8 y 9 de Ley 30096 ante incremento de Delitos Informáticos.

TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE:
Abogado

AUTOR:

Huayca Jimenez, Hamer Guillermo (orcid.org/0000-0002-2401-340X)

ASESOR:

Dr. Espinoza Azula, Cesar Napoleon (orcid.org/0000-0002-9928-0422)

LÍNEA DE INVESTIGACIÓN:

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

LÍNEA DE RESPONSABILIDAD SOCIAL UNIVERSITARIA:

Fortalecimiento de la democracia, liderazgo y ciudadanía

LIMA - PERÚ

2022

Dedicatoria

A Raisa que es mi inspiración para avanzar a pesar de la adversidad. A mi amada Madre por sus enseñanzas, su sacrificio y esfuerzo ya que sin ello no sería la persona que soy en la actualidad. A los señores Godofredo y Nercida que me han instruido y dado su apoyo en un momento difícil de mi vida.

Agradecimiento

Agradezco a Dios por brindarme una familia maravillosa, quienes siempre han creído en mí, y me han dado el ejemplo de superación, humildad y sacrificio. A mi asesor el Dr. Espinoza Azula, César Napoleón por su apoyo y conocimientos que hicieron posible esta investigación.

Índice de contenidos

Índice de tablas

Resumen

La presente investigación tiene como objetivo general, determinar las deficiencias en de la ley 30096 en base a los delitos de fraude informático y suplantación de identidad ante el incremento de delitos informáticos. Como objetivos específicos se buscó analizar como la deficiencia artículos 8 y 9 de la ley 30096 y proponer una modificatoria ante incremento de Delitos Informáticos.

Ello, desde un acercamiento doctrinal y legal al fenómeno detectado y observado, teniendo en la categoría principal, las deficiencias en los delitos de fraude informático y suplantación de identidad; con sub - categorías, i) la falta de conocimiento informático y ii) falta de conocimiento y dominio en delitos de fraude informático y suplantación de identidad.

Se empleó un método no experimental, desde un enfoque cualitativo, tipo básico y diseño de investigación fenomenológico. Para la muestra se llevó a cabo la entrevista a los diferentes expertos en la materia, como Maestros en Derecho Penal y Abogado, como resultado se pudo determinar que las principales modificatorias que deben llevarse a cabo son la actualización sistemática y anual de la ley 30096 en general e implementar los nuevos delitos informáticos derivados de los arriba mencionados.

Palabras clave: deficiencias, delitos informáticos, delitos de fraude informático y suplantación de identidad.

Abstract

The present investigation has as a general objective, to determine the deficiencies in the law 30096 based on the crimes of computer fraud and identity theft due to the increase in computer crimes. As specific objectives, it was sought to analyze how deficiency 8 and 9 of Law 30096 and propose a modification in the face of an increase in Computer Crimes.

This, from a doctrinal and legal approach to the phenomenon detected and observed, having in the main category, the deficiencies in the crimes of computer fraud and identity theft; with sub-categories, i) lack of computer knowledge and ii) lack of knowledge and domain in crimes of computer fraud and identity theft.

See used a non-experimental method, from a qualitative approach, basic type and phenomenological research design. For the sample, the interview was carried out with the different experts in the field, such as Masters in Criminal Law and Lawyer, as a result it was possible to determine that the main modifications that must be carried out are the systematic and annual updating of Law 30096 in general and implement the new computer crimes derived from those mentioned above.

Keywords: deficiencies, computer crimes, computer fraud crimes and identity thefttrial

I. INTRODUCCIÓN

En el presente la informática ejerce una influencia constante y secuencial en la vida diaria de las personas y organizaciones comerciales, y la importancia que tiene su constante cambio y desarrollo dentro de un país al momento de la realización de transacciones comerciales, la comunicación en tiempo real, seguridad, sanidad, etc.

Estos son todos aspectos de la vida diaria que se desenvuelven a través del uso informático, creando una dependencia social alta, por lo cual era inevitable pensar que de estos mismo surgirían comportamientos ilícitos que con el tiempo y el avance acelerado de los medios informáticos acabarían derivando en un crecimiento exponencial.

Desde octubre de 2013 a julio de 2020, las fiscalías penales comunes y mixtas de todo el país recibieron un total de 21,687 denuncias por delitos informáticos, y la ciberdelincuencia sufrió un incremento sustancial al mismo ritmo de los diferentes usuarios que acceden a las redes virtuales comparable a las plataformas utilizadas en la actualidad.

Según los resultados de un estudio de tecnología realizado por el Departamento de Salud Pública en 2020, las denuncias incluyen el fraude informático, el fraude virtual y el robo de identidad, todos los cuales forman parte de lo que llamamos "ciberdelincuencia".

Igualmente, Renzo Vinelli Vereau (2021) nos expone que, según el Banco Central de Reserva, los instrumentos de pago distintos al efectivo ascendieron a 958 mil millones de soles, y de enero de 2020 a mayo de 2020, el negocio a través de bancos virtuales creció un 18% (las transferencias electrónicas se incrementaron en un 13% hacia mayo, y el uso de las tarjetas de crédito disminuyó en 25% para el 2020).

Es claro que estamos ante una nueva forma de convivencia económica dominada por los sistemas informáticos. Sin embargo, esta “evolución” también ha ido acompañada de la proliferación de un nuevo tipo de delito económico, lo que demuestra que los operadores legítimos son perfectamente capaces de combatirlo.

Pues bien, los medios de comunicación permiten a la sociedad conocer de primera mano la proliferación de esta nueva organización criminal dedicada a cometer delitos informáticos. Para entender la gravedad de estos delitos, vale la pena destacar algunos datos: Durante la primera semana de enero a agosto de 2020, Perú registró 1.481.963 ataques de phishing, un promedio de 7.000 ataques por día. Por otro lado, de enero de 2020 a julio de 2020 se recibieron un total de 1.117 denuncias de fraude informático. De estos, 974 fueron transacciones o transferencias electrónicas no autorizadas y 142 fueron compras fraudulentas en Internet.

Es comprobado que en nuestra sociedad, hay un nuevo sistema de intercambio y de relaciones comerciales, por lo tanto, también una nueva manera de criminalidad, para la cual el Perú no está preparado para responder de forma eficaz e inmediata, la poca capacitación técnica de parte del ministerio público, así como la vaga base legal pone a la sociedad en una coyuntura de indefensión.

Al observar este crecimiento emergente y consistente del tráfico y venta de información a través de los diversos mercados donde se comercializan estos tipos de datos de un alto valor económico, en forma más concisa el mercado negro de información hurtada sirve como primordial motor de impulso a la ola de ataques informáticos, principalmente destinados a la obtención de bases de datos con información personal en su defecto a la estafa por medio de las compras y ventas virtuales que es una acción recurrente y común en el nuevo mundo informático que vivimos el cual nos obliga a vincular la informática de forma inherente a nuestra vida diaria ya que recurrimos a la tecnología para realizar acciones diarias y cotidianas de necesidad básica.

II. MARCO TEÓRICO

Más recientemente, los delitos informáticos son delitos que eluden los sistemas electrónicos o códigos de acceso, ya que en su mayoría son causados por la tecnología, ello conlleva a la afectación de diversos bienes jurídicos, no protegen la confiabilidad de los datos, por lo que el Estado interviene a través del sector público junto al apoyo del gobierno en conjunto con el departamento de investigación de delitos de alta tecnología para evitar fugas electrónicas de mensajes, correos electrónicos o información personal.

En relación a lo mencionado anteriormente se toma en consideración a nivel internacional lo siguiente:

Larios y Sánchez (2014), en su investigación “Ciberdelito”, concluye lo siguiente:

Las tecnologías de la información son las herramientas y métodos creados para facilitar la vida de las personas mediante los cuales se recopila, retiene, procesa o distribuye información, un ejemplo de esto es el envío de correo electrónico. La carta debe escribirse y depositarse en un buzón para que otra persona pueda llevarla a la oficina de correos y enviársela al destinatario, lo que puede demorar hasta semanas si el destino está lejos. Con la nueva tecnología, basta con escribir una carta y enviarla a una dirección de correo electrónico para que llegue a cualquier parte del mundo en segundos.

De esto se puede concluir que la tecnología de la información y todas las herramientas que de ella resultan están diseñadas para la conveniencia y comodidad del usuario, sin embargo, como lo demuestra este trabajo, esta tecnología ha sido herramientas de terceros, o para ocasionar desastres económicos y en algunos casos hasta sociales.

El desarrollo de la tecnología de la información ha hecho que sea muy fácil acceder ilegalmente a muchos sistemas informáticos, extraer información de ellos o simplemente destruir sitios web como medida de rebelión, protesta o simple malicia, y ni siquiera existe actualmente una herramienta para hacer que la información sea completamente segura. .

Se habla de cortafuegos, software antivirus, contraseñas encriptadas con métodos digitales muy avanzados e innumerables técnicas creadas para mantener los sistemas seguros; sin embargo, a medida que avanza la tecnología, también lo hacen los métodos para hackear estos sistemas, convirtiéndose en herramientas de defensa La efectividad nunca será del 100 %

Aquí es donde entra el término ciberdelito, que debe incluir todos los delitos cometidos utilizando tecnologías de la información, especialmente aquellos que involucran sistemas informáticos.

Una de las consecuencias más graves del uso de estas tecnologías es lo que en este documento se denomina ciberterrorismo, que en adelante no se limita al terror físico a través de bombas o guerra, sino a diversos tipos de terror que ahora se pueden crear utilizando medios cibernéticos como las herramientas Flame y Stuxnet, estas poderosas herramientas informáticas no pudieron lidiar con ellos antes de que la catástrofe golpeara e inhabilitara la planta de energía nuclear de Irán.

Los usuarios ordinarios tampoco pueden ser excluidos. Una utilidad tan simple como una red social puede tener un efecto profundamente negativo en cualquier persona si estas redes se utilizan para difamar, ridiculizar o como fuente de información para posibles ataques o secuestros; se puede argumentar que estos propósitos se deben a la falta de los facilitados por filtros de seguridad; sin embargo, en la sociedad en la que vivimos, No se puede subir a las redes sociales lo que los delincuentes consideran un “lujo” porque eso haría que la gente sea presa fácil para que estas personas cometan actos ilegales.

Un claro ejemplo de usuarios habituales que son víctimas de delitos cibernéticos sin culpa propia es el robo de identidad, el fraude bancario y el phishing. En última instancia, los usuarios bancarios podrán realizar fácilmente sus operaciones bancarias en línea simplemente ingresando sus números de tarjeta y PIN; los ciberdelincuentes están utilizando este método para clonar sitios web bancarios para que los usuarios desprevenidos puedan ingresar de manera segura, y esos números de tarjeta y PIN quedan atrás. manos de los delincuentes, pueden hacer lo que quieran.

Como estos ejemplos, son muchas más las personas que son víctimas de los ciberdelincuentes, O de desarrolladores que buscan su propio interés solo para ellos o para las empresas para las que trabajan (el adware es un ejemplo obvio de estas prácticas); si no tienes un conocimiento tan profundo en informática, eres víctima de piratas informáticos cuyo único propósito es Destruir o robar información, o en el peor de los casos, equipos de cómputo completos; muchas veces, las personas no tienen una forma efectiva de defensa contra estos actos.

Es por estas acciones que se han tenido que transformar los temas informáticos, no solo en cuanto a programas o dispositivos defensivos como antivirus y firewalls, sino también en aspectos políticos y de seguridad. capaz de manejar estas acciones.

En muchos países existen leyes y acuerdos de cooperación internacional para enjuiciar a los delincuentes que realizan ataques desde fuera del país de residencia de la víctima, pero estas medidas aún no son suficientes, Para paliar este problema.

Una de las razones de esta imposibilidad es la falta de acuerdo y cooperación interna en muchos países para promulgar leyes efectivas para controlar estos delitos, siendo México un claro ejemplo.

Como pudimos comprobar en este documento, la ley que existe aquí no sanciona explícitamente el uso de las tecnologías de la información para delinquir, sino que se sanciona el delito en sí, eso es todo. Debido a esta enorme brecha en la ley, los piratas informáticos pueden hacer lo que quieran con las computadoras de otras personas con poco o ningún castigo; este no es el caso de las personas que usan la tecnología de la información para formar parte de las redes de pedofilia; las personas, pero no porque usen la web para ese fin, sino porque son pedófilos.

Uno de los principales problemas con la creación de leyes es puramente político, debido a la mala reputación que tienen los políticos en México. Han hecho un esfuerzo por controlar Internet, alegando que solo aquellos que sean sospechosos de haber cometido un delito enfrentarán acciones legales. A partir de este punto, las personas pueden o no ser sospechosas de haber cometido un delito, según lo que vean en línea. Esto solo podría determinarse investigando lo que cada sospechoso consulta en línea, lo que enfurece a los ciberactivistas que afirman que

esto viola el derecho a la privacidad de las personas porque equivale a husmear en ellas, lo que contribuye al problema permanente de los activistas contra los políticos.

El problema con las leyes de tecnología de la información no se limita a eso; se utiliza la frase "sobrerregulación". Los activistas que se oponen a cualquier ley que rija Internet hacen referencia a que estos documentos contienen numerosas normas sin ofrecer una defensa convincente. Mencionan que se restringirá el uso de Internet.

El sitio que quieren no va a ser accesible para ellos, se están violando sus derechos, etc. El tema es que como no hay leyes ni reglamentos en el área de la informática, están todos los delitos informáticos que ya se han mencionado y hay impunidad por no poder sancionar a quienes hacen mal uso de Internet. Los ejemplos incluyen piratería: al descargar cualquier archivo ilegalmente que esté protegido por derechos de autor; fraude bancario, por no b.

En otras palabras, la solución a este problema pasa por una adecuada regulación de internet, como leyes que sancionen a los infractores sin vulnerar los derechos humanos ni la libertad de las personas para navegar por la web, pero sin olvidar la necesidad de perseguir a los ciberdelincuentes que utilizan la red. Internet para llevar a cabo sus crímenes.

Esto se logrará cuando los políticos de esta nación lleguen a un entendimiento, dejando de lado sus diferentes ideologías partidistas y velando por los intereses de la población, que en última instancia son las principales víctimas de estos crímenes. Cuando se alcancen estos acuerdos, se puede avanzar con la aprobación de leyes que atiendan las necesidades de los ciudadanos de la nación y no solo las de un pequeño número de políticos y empresarios, como es el caso en este momento.

Los ingenieros que eligieron los campos de telecomunicaciones, informática y sistemas informáticos tienen la responsabilidad de velar por la seguridad de los servicios ofrecidos, que en este caso utilizan tecnologías de la información. También tienen la responsabilidad de crear y adelantar ideas para que se hagan leyes en esta materia, aunque no es una rama que le corresponda a un ingeniero, y en esto deben trabajar muy de cerca. Con esto, podría ser posible tomar las

acciones legales necesarias para vigilar Internet, enjuiciar a los infractores y disminuir el impacto que tiene el delito cibernético en la vida cotidiana.

Primero se debe educar al usuario final para lograr el objetivo de garantizar la seguridad de los servicios informáticos prestados y evitar ser víctima de ciberdelincuencia. Para evitar que los usuarios de caer en las trampas de los ciberdelincuentes con tanta facilidad, inicialmente serían útiles las campañas de educación informática, las advertencias sobre posibles programas falsificados y la clonación de páginas bancarias. Incluso si su computadora está protegida por los mejores antivirus o firewalls disponibles en el mercado, el usuario final sin educación siempre será un blanco muy fácil en la ejecución de estos delitos.

El siguiente paso es proteger eficazmente el equipo con el que está trabajando después de educar al usuario final. Al cambiar de encriptación WEP a encriptación WPA o WPA2, la encriptación instalada de fábrica en los módems modernos se puede cambiar, lo que hace mucho más difícil o incluso imposible que los piratas informáticos accedan a las redes inalámbricas caseras que tiene la mayoría de las personas.

El proceso debe ser más complicado cuando se trata de redes empresariales, lo que siempre exige una inversión mayor que en ocasiones los gerentes de las empresas no quieren hacer. También se debe implementar un sistema de seguridad perimetral basado en firewalls con configuraciones estratégicas que funcionen como filtros para diversos ataques. Y en caso de que ocurra un ataque, esté preparado para tales contingencias, con servidores de respaldo a los que solo tenga acceso personal de confianza, para evitar que usuarios maliciosos dañen físicamente las ubicaciones donde se encuentran sus equipos.

Una vez completado lo mencionado anteriormente, se requiere la cooperación con los profesionales del derecho. Para localizar la actividad de la red que está compuesta única y exclusivamente por aquellas personas que se ha comprobado que han llevado a cabo un acto ilícito en el que utilizaron las tecnologías de la información como herramienta para delinquir, los proveedores de servicios de Internet deben estar obligados a cooperar con los organismos encargados de impartir justicia, tales como las Procuradurías Generales de Justicia, tanto de los

estados como de la República. Las leyes también deben estar escritas. que solo aborden el derecho informático y la ciberdelincuencia, limitando el uso de Internet para las actividades cotidianas. Esto no implica que prohíban realizar cualquier actividad diaria, sino que prestan especial atención a los sitios web y otras herramientas utilizadas para cometer cualquier tipo de ciberdelito.

Igualmente, Quevedo (2017) en su tesis titulada “Investigación y prueba del ciberdelito”, señala que:

Una vez vistas las características técnicas básicas de Internet, es hora de discutir en qué medida estas características son especialmente relevantes para facilitar la comisión de delitos, y luego analizar los problemas y desafíos que plantea la incursión de nuevos tipos penales en la sociedad de la información.

Como se mencionó anteriormente, Internet es una red global con conexiones instantáneas y una estructura descentralizada, basada en la representación digital de información, que permite conexiones en tiempo real entre personas, sin importar dónde se encuentren. Esto presenta una oportunidad especial para el crimen, ya que el tiempo, la distancia y las fronteras nacionales son mucho menos importantes que el crimen tradicional. Estas características interrelacionadas representan especificidades que facilitan la comisión de determinados delitos, al mismo tiempo que dificultan su investigación y persecución judicial.

1. Con la aparición de nuevos tipos de delincuencia, así como la aparición de nuevas formas de delincuencia tradicional, el desarrollo de Internet se ha reflejado en la delincuencia y la delincuencia. En la actualidad, las tecnologías de la información no son sólo un medio, sino incluso un objeto potencial para la implementación de ilegalidades estrictamente telemáticas o cibernéticas.

2. Internet es una red global con alcance global y acceso instantáneo desde casi cualquier parte del mundo. Esto permite a los posibles delincuentes operar en cualquier parte del mundo, buscar a las víctimas más vulnerables en cualquier lugar y atacar en cualquier lugar o desde cualquier lugar, evitando la persecución por la migración que proporciona dicha actividad cibernética. Internet y su crecimiento global no sólo han incrementado su trascendencia criminológica, sino que también

han hecho más difícil la justificación de conductas punibles de personas o equipos responsables de la acción ilícita.

3. Esta influencia global conduce a la desterritorialización, lo que significa que el fenómeno del ciberdelito casi se puede definir como internacionalizado. Esto genera dificultades en la persecución de los delitos y, con ello, los desafíos jurídicos para la cooperación internacional en la persecución de hechos ilícitos de estas características. Por ejemplo, supongamos que un sujeto puede cometer un delito contra otro sujeto a miles de kilómetros de distancia inicialmente, y la información se encuentra en otro lugar diferente a estos. El carácter transnacional o transfronterizo de estos delitos se ha incrementado, y con ello surge la cuestión de la competencia entre distintas jurisdicciones nacionales, las diferencias en sus estatutos penales para sancionar una misma conducta, e incluso si se considera delito o no.

Asimismo, Celli (2019) en su investigación sobre “Las nuevas tecnologías y los Delitos Informáticos. Análisis de la ley 26.388, modificación del Código Penal argentino”, su objetivo fue realizar una indagación con respecto al ordenamiento jurídico de Argentina, si brinda las herramientas para el control de los delitos a través de las nuevas tecnologías. Con respecto a la metodología, el tipo fue descriptiva. En conclusión, los delitos informáticos se pueden realizar desde cualquier lugar, mantiene su identidad en secreto y es una herramienta que si se usa indebidamente puede ocasionar graves daños.

Los antecedentes nacionales son los siguientes:

Alarcon & Barrera (2017) en su investigación titulado “Uso de internet y delitos informáticos en los alumnos del primer ciclo de la Universidad Pedagógica y Tecnológica de Colombia, 2016”. En la investigación a partir del incremento de posibilidades para usar las tecnologías de la información y comunicación, asimismo con la relación global entre satélite, personas, organizaciones públicas y privadas, quedaron inseguras la información por lo que son vulnerables mediante el sistema de intercomunicación y manejo de información, mientras que ha sido un gran beneficio en forma general en los países, la débil o poca instrucción para utilizarlos, ha sido un progresivo peligro con el impacto del ciberdelito. Desde los años 80, a

nivel internacional, la revolución de la tecnología, ha generado un gran avance con respecto a las computadoras, siendo estas cada vez más sofisticadas y ahora más con el internet.

Rodríguez Rodríguez, & Nadia Katherine (2019), en su Artículo titulado "Protegiendo a nuestros hijos del cibercrimen", nos expresa que la realidad actual en el mundo digital, es lamentable, ya que el cibercrimen se está haciendo universal y esto se puede explicar como un delito que se comente mediante un medio tecnológico informático (videojuego, computadora y/o Smartphone) que está conectado al internet

DQ Institute sostiene que, a nivel mundial, el 56% de niños, entre 8 y 12 años de edad, están expuestos a ciberacosos, a la adicción al juego, a engaños de pederastas o riesgos relacionados a la violencia sexual; asimismo, en el Perú el promedio es mayor, siendo de 58%.

Desde el año 2013, en el Perú existe una ley con respecto a delitos informáticos, en la que hay un artículo en particular, que castiga el cibercrimen, en relación a propuestas de tipo sexuales a través de la tecnología hacia niños y adolescentes; no hay campañas de las autoridades sobre concientización a la ciudadanía con educación o información de los grandes riesgos cibernéticos a los que se exponen los niños y especialmente a saber cómo mitigarlos.

Este crimen es demasiado serio y se va incrementando con el avance de la tecnología, por ello es necesario conocer las formas de protección a los menores, ya que utilizan los dispositivos tecnológicos por muchas horas, ya sea en redes sociales, YouTube y juegos en línea.

Posteriormente Adarmes Álvarez & Ortiz Cahuana (2020), en su tesis "Intervención de los operadores de justicia ante el aumento de amenazas de delitos informáticos durante el estado de emergencia por covid-19", en sus conclusiones señala:

1 Que los bienes jurídicos protegidos afecten en relación al daño causado por el sujeto activo, esto por desconocimiento total o parcial de las normas vigentes. Cabe señalar que, si bien es cierto que afectan en relación al daño causado, el común en este tipo de escenarios es la información privilegiada que la víctima

posee en su dispositivo cibernético, ya sea en laptops, teléfonos móviles, PCs. y tabletas, pudiendo así causar daños graves a su propio sistema operativo, secuestrando información personal o a nivel nacional, según el interesado. En cuanto a hacer frente a un posible ataque masivo a nivel informático, dentro del propio entorno, se argumenta que lo que tenemos no es suficiente, el gobierno debería invertir más en seguridad informática, por la misma razón que maneja fondos públicos, como documentos de gran importancia para el estado, aquí incluso deberíamos adjuntar secretos del mismo, como datos de cada ciudadano asegurado, a partir de esto cabe mencionar a las entidades bancarias que son las que tienen mayor índice de siniestros por cobros fraudulentos o compras fraudulentas realizadas, sin contar los seguros incluidos en tu tarjeta. Entiende lo anterior como una modalidad de delito informático propiamente dicha denominada Phishing, donde ingresas a una plataforma aleatoria que te ofrece servicios o productos similares a los que podrías necesitar en ese momento. Cabe agregar que es necesario emprender acciones preventivas y no reactivas, a las que está acostumbrado el gobierno.

2. En un principio se podría argumentar que todo esto está sucediendo por nuestra propia negligencia, esto ya mencionado a la falta de interés de nuestros políticos, quienes, con la intención, tal vez de controlarlo, también podría ser brindar herramientas dentro del ciberespacio. misma, con el fin de reportar o advertir de posibles páginas fraudulentas con una nomenclatura similar a la de recolección de datos, con el fin de realizar diversas operaciones en perjuicio del titular de una tarjeta de crédito, suplantando su identidad, ya que al momento del pago la imagen del titular no parece dar validez a lo que en sí mismo es el titular, como si no bastara con pedir también el documento de identidad.

3. Otro punto es que no existe jurisprudencia y/o condenas del delito informático en sí, esto se debe a que se basan en el resultado obtenido, como la extorsión, por el secuestro de información ocasionado por el Ransonware, que es un software que ingresa al dispositivo a través de las descargas realizadas en

cualquier anuncio que lo redirecciona a la página principal y al hacer clic por error, secuestra información importante, exigiendo una cantidad pecuniaria de dicha cuenta bancaria o en BITCOINS, que viene a hacer la moneda digital. Por otra parte, se confirma la insistencia en la creación de oficinas tributarias, así como de juzgados especializados en delitos informáticos, para un mayor estudio e interacción de estos delitos y su correcta persecución para que luego sean sancionados, conforme a la exigencia del delito comprometido. Finalmente, es necesario acotar que es necesaria una mayor capacitación del personal policial de la división de investigaciones de alta tecnología (DIVINDAD), así como el fortalecimiento de las fiscalías y procuradurías judiciales para restablecer la seguridad de las víctimas de estos delitos. los cuales se han visto perjudicados económicamente y tienen que lidiar con el estrés de pagar lo perdido, aunque no fueran ellos o lo fueran inconscientemente.

Por un lado, el CONAPOC (2020) en su artículo denominado “Diagnóstico situacional Multisectorial sobre la Ciberdelincuencia en el Perú”. Señala que, si bien contamos con normativa específica relacionada con el ciberdelito, como la Ley N° 30096 de Delitos Informáticos o la Ley N° 30999 de Ciberdefensa, además de estar en el Convenio de Budapest como país miembro; Todavía tenemos un largo camino por recorrer para mejorar dicha normativa, teniendo en cuenta la incorporación de diferentes componentes relacionados con el análisis de conductas enmarcadas en delitos informáticos.

La incidencia del ciberdelito mantiene un crecimiento innegable que se puede apreciar en la evolución de los datos correspondientes a los expedientes de denuncias y casos que tramitan las entidades policiales y fiscales, principalmente. En la misma línea, la notable presencia de los ciberdelitos relacionados con la defraudación y el fraude informático resuena lo suficiente como para reflexionar sobre la adecuación de las capacidades estatales frente a los delitos contra la propiedad, con el objetivo de incluir perspectivas y enfoques que favorezcan el análisis de los medios y espacios informáticos utilizados, con el fin de obtener mejores resultados, particularmente en el campo preventivo.

Junto a los delitos contra la propiedad, promovidos o perpetrados con el apoyo de las tecnologías de la información y la comunicación, también vemos que la

pornografía infantil, el ciberacoso o la ciberextorsión también han ganado mayor notoriedad; involucrando y afectando a poblaciones que tienen más dificultades para defenderse y protegerse de estas formas delictivas.

Si bien existe un mayor avance en la aplicación de medidas y protocolos de protección y prevención del ciberdelito, por parte de las grandes corporaciones y entidades bancarias del sector privado; Es importante no descuidar ni abordar a los actores menores dentro de este grupo, como los micro y pequeños empresarios, quienes no solo se ven afectados por las brechas en el acceso a la tecnología y la información, sino que también suelen tener menos capacidad financiera y conocimiento para protegerse contra ciberataques, amenazas, poniendo en riesgo sus negocios, más aun considerando el contexto actual de lenta recuperación económica y la fragilidad de las iniciativas de las pequeñas empresas.

Diferentes actores estatales como la Policía Nacional del Perú, el Ministerio Público, el Poder Judicial, entre otros, están realizando esfuerzos para prevenir, perseguir y controlar los delitos cibernéticos en el Perú. En este sentido, es importante que su labor vaya acompañada de los recursos necesarios para combatir este tipo de delitos, ya que nos encontramos ante tipos de delincuentes que utilizan tecnología especializada y muy avanzada para cometer hechos punibles.

Diversos organismos internacionales, como la Organización de las Naciones Unidas o el Banco Interamericano de Desarrollo, han realizado diagnósticos situacionales del ciberdelito en el mundo, incluyendo al Perú en sus estudios y exteriorizando los problemas y brechas que aún deben corregirse, especialmente en todos los países, áreas de atención a los recursos y cooperación entre los diferentes actores involucrados.

El cibercrimen está en lo más alto de la agenda global, no solo por su riesgo asociado y su potencial impacto negativo en el PIB de los países, sino también porque reconfigura actos delictivos que traspasan fronteras territoriales con gran facilidad y rapidez. Perú forma parte de los acuerdos globales de ciberdelincuencia y ha logrado un progreso considerable en la legislación relacionada, pero aún carece de las herramientas de gestión para coordinar de manera efectiva los esfuerzos del sector público y privado.

Así mismo nos señala Aredo Luján, (2021) en su tesis “El phishing y su vulneración a la protección de datos personales en los delitos informáticos”. El phishing vulnera la protección de datos personales en los delitos informáticos, Debido al uso generalizado de la ingeniería social, muchas veces es difícil identificar a los participantes en delitos informáticos debido a que los ciberdelincuentes explotan conocimientos técnicos, causan daños a la propiedad y afectan la privacidad, por lo que la normativa existente debe actualizarse ya que la sociedad lo refleja después de un estado de crisis. emergencia. El alcance e impacto del phishing como la sustracción de datos personales se fundamenta en la jurisprudencia, la doctrina y la poca pedagogía informática en la obtención de información confidencial de las víctimas mediante el uso de engaños o ardid. Además, indican qué mecanismos de autenticación usar, como huella digital y reconocimiento facial, tokens digitales SMS y más. De esta forma, se busca generar una cultura de prevención por parte del cliente, así como una adecuada capacitación del personal bancario. De acuerdo con las enseñanzas, la importancia de proteger los datos personales como garantía para proteger la privacidad radica en que las entidades bancarias necesitan establecer un cierto nivel de control para mantener los datos personales en un lugar seguro, también conocido como privacidad informática, para salvaguardar la privacidad cuando se utilizan medios electrónicos. dispositivos. Los presupuestos de los delitos informáticos en el código penal peruano se sancionan con el Art. 154-A.- Tráfico ilegal de datos personales, y también en el Art. 196-A.- Estafa agravada inciso 5; los cuales generan ambigüedad. Así también con la Ley N.º 30096, “Ley de Delitos Informáticos”, el cual en su inciso 9º menciona La sustitución de la identidad de una persona física o jurídica por tecnología informática, cuyo resultado sea material o moralmente perjudicial. Estos valores predeterminados son definiciones muy generales y son insuficientes para definir qué es el phishing. Además, expertos señalan que son claros delitos dolosos

III. METODOLOGÍA

En el próximo capítulo se presentará la investigación a través de un enfoque cualitativo, se describirá el tipo así como el diseño, introduciremos una matriz apriorística y detallaremos las categorías así como subcategorías en base a los conceptos relacionados con la investigación, explicaremos el instrumento que se aplicó y consecuentemente las técnicas y se darán algunos conceptos concernientes a la investigación.

3.1. Tipo y diseño de Investigación

El tipo de investigación es básica, que, según Hernández, Collado & Baptista (2014) es una investigación que busca producir conocimientos y teorías, como en este caso, que se busca expandir los conocimientos que se tienen en la actualidad acerca de los delitos informáticos fundamentado en teorías de diversos autores los cuales son de gran influencia en el impacto jurisprudencial de aquellos países en los que el delito informático se encuentra en una etapa más avanzada y constante, de esta forma, los operadores de justicia podrán dar una respuesta ante los delitos informáticos de fraude y suplantación de identidad.

Diseño de investigación

En cuanto al diseño de investigación, fue fenomenológico porque se basa en una investigación experimental de los hechos de la vida a nivel observacional, tomando en cuenta los hechos pasados desde la mirada de un sujeto, y fundamentalmente analizando los descubrimientos tecnológicos a través de la teoría para poder identificar las deficiencias en los delitos de estafa informática y usurpación de identidad. (Furster, 2019).

Fenómeno lógico.

Hernández (2014), señala que, el investigador busca dar una explicación general de un fenómeno observable ya existente y presenta, una descripción respecto al problema planteado, si se sigue el procedimiento adecuado, cualquier individuo

puede elaborar una investigación en base la observación fenomenológica la cual deberá ser validada.

Enfoque (Cualitativo)

Así mismo se continuo con un enfoque cualitativo, ya que se establece como una actividad estructurada y orientada a profundizar el estudio de los fenómenos observables, mediante la recopilación de información actividades destinadas al descubrimiento y desarrollo de un nuevo conocimiento. (Sandín, 2003, p. 88, Citado en: Bisquerra, 2016, p. 72)

3.2. Categorías, sub categorías y matriz de categorización

Esta matriz se encuentra ubicada en el Anexo 01.

3.3 Escenario de estudio

El principal escenario de estudio para el desarrollo de la presente investigación ha sido la utilización de los diferentes medios tecnológicos como (laptop, celular, etc.), siendo una forma de obtención de información inmediata, dado que inicia el dialogo con el participante en tiempo real, todo consignado con los respectivos correos personales, para aportar los conocimientos a la problemática que se identifica en la investigación.

3.4 Participantes

Los participantes son los operadores de justicia tales como el ministerio público y abogados que tienen trayectoria en casos de delitos informáticos y la búsqueda de los ciberdelincuentes y, asimismo, se fundamentará teóricamente en fuentes de investigación de repositorios institucional y científico.

Tabla N°1

Tabla de entrevistados

Participantes	Grado	Ocupación
Miguel Hernán Sáenz Cabrera	Abogado	Abogado
Zegarra Castañeda, Giany	Magister	Abogado
Zegarra Castañeda, Reimy	Magister	Abogado
	Abogado	Abogado
	Total: 04	

3.5 Técnicas e instrumentos, de recolección de datos

3.5.1 Técnicas (La entrevista)

La técnica utilizada en esta encuesta es la entrevista, ya que es una técnica de recolección de datos que permite extraer la opinión de los participantes a través de una serie de preguntas elaboradas en un escenario específico. (Hernández, 2018)

3.5.1. Instrumentos (Guía de entrevistas)

Por ello, una herramienta que permite una correcta recopilación de información es la guía de entrevista, que proporciona a los encuestados una amplia gama de respuestas. (Hernández, 2018)

Tabla N°2

Propósito de la técnica e instrumento.

Técnica	Instrumento	Propósito
Entrevista	Guía de Entrevista	Recoger información de forma directa de los expertos en la materia.

3.6 Procedimientos

La encuesta se realizó de manera ordenada, utilizando un método inductivo, aplicando herramientas a los participantes antes mencionados, quienes mediante preguntas describieron y respondieron casos específicos de la encuesta en base a su propia experiencia, cotejando y comparando las respuestas para ver si hubo coincidencias, similares o inconsistentes para llegar a una conclusión lógica sobre lo que se investiga, a partir de un conjunto de experiencias vividas por la persona entrevistada.

Triangulación

Se sugiere una gama de fuentes y métodos de recopilación de datos, y en las encuestas cualitativas, la triangulación es una forma de intersectar la información de los datos recopilados durante la encuesta si los datos se recopilan de diferentes sujetos, diferentes fuentes y más formas del proceso (Hernández et al., 2014, p.417).

Desde un punto de vista metodológico, la confiabilidad y validez se realizará con la participación activa de los actores sociales estudiados a través del consenso sobre el diálogo y la intersubjetividad, aplicando estrategias como la triangulación y comparación de diversas fuentes. (Palomino, 2019, pág. 76)

3.7 Rigor científico

Los estándares de rigor científico describen paradigmas relevantes para la investigación, dada la aceptación de axiomas que son consistentes con lo enunciado y siguen los fundamentos establecidos por la indagación natural, anteriores a estos paradigmas, planteados por Arias y Girardo Content (2011)

3.8. Método de análisis de datos

Después de recopilar los datos, en este estudio se utilizó el método de análisis del triángulo de datos, que tiene como objetivo comparar los datos utilizando varias estrategias y fuentes de investigación para llegar a información consolidada. (Hernández, 2018)

3.9. Aspectos Éticos

En lo que respecta a la investigación científica y tecnológica, teniendo en cuenta que en materia de ética, los principios y valores son considerados como referentes congruentes con la investigación presentada, utilizando el campo de la ciencia para observar el comportamiento y especialmente el carácter humano.

El presente trabajo tiene los siguientes aspectos éticos: 1) la autorización de la institucion y validación de los instrumentos que aplica; 2) la veracidad de la información analizada, 3) la credibilidad de las opiniones vertidas en las entrevistas, con su consentimiento y autorización, y 4) respeto a la autoría según lo establecido en el Decreto N° 822 y sus reformas a la Ley N° 30276, mediante citas y referencias tipo APA.

IV. RESULTADOS Y DISCUSIÓN

En el siguiente capítulo de la investigación se desarrolla lo resultados presentando las coincidencias, las discrepancias la interpretación y los resultados.

Tabla N°3

Pregunta: ¿Cuáles considera usted que son las modificatorias que se deberían realizar a los delitos de fraude informático y suplantación de identidad en función a la Ley 30096?			
MHSC1	GZC2	4ZC3	HCB4
Considero que es necesaria una modificatoria ya que a mi parecer el incremento de los delitos informáticos se debe a las deficiencias en cuanto a las investigaciones fiscales, iniciando porla falta de capacitación hacia los órganos jurisdiccionales y una incorrecta aplicación de la normativa vigente, así como la falta de dominio de investigación en lo que respecta a criminalidad tecnológica.	Creo que como enfoque principal se debe dar una actualización de los delitos informáticos ya que están en constante cambio y la legislación actual no regula todas las nuevas modalidades que están surgiendo con los nuevos avances tecnológicos.	Principalmente las modificatorias que se deberían aplicar son en cuanto a la pena y a la actualización de los ilícitos informáticos, ya que la actual Ley 30096 no contempla las nuevas y diversas formas tecnológicas derivados de los delitos de fraude informático y suplantación de identidad	Lo primero seria implementar penas mas severas para este tipo de ilícitos penales, así como el realizar una actualización periódica de las diversas conductas derivadas las cuales no están correctamente reguladas por la normativa peruana.

Coincidencias

De acuerdo al objetivo general el cual busca determinar Cuáles considera usted que son las modificatorias que se deberían realizar a los delitos de fraude informático y suplantación de identidad en función a la Ley 30096, encontramos que las respuestas planteadas por los especialistas entre ellos nos dan a entender que la mayoría councluye que es necesaria una actualización de la normativa vigente debido a que se han ido generando nuevas modalidades derivadas de los delitos de fraude informatico y suplantación de identidad al ser los mas recurrentes, señalando que en su momento la ley se creo como una formalidad ya que en esos momento no era lo habitual la ciberdelincuencia y que al no encontrarse tipificadas estas nuevas modalidades genera dificultad al momento de identificar e individualizar el tipo penal para llevar a cabo una correcta investigación preliminar.

Otro punto es que por mayoría se tiene concordancia en que es necesaria el aumento de las penas para este tipo de delitos informáticos que afectan el patrimonio mediante el robo de datos empleando diversos medios tecnológicos.

Discrepancias

Se tiene como discrepancias el que no es necesaria una modificatoria y que solo se requiere la correcta capacitación y la introducción de herramientas que ayuden a mejorar la eficiencia al momeno de realizar las investigaciones preliminares correspondiente para poder identificar e individualizar al sujeto responsable del ilícito.

Interpretación

A interpretación personal considero que esto es una clara muestra que los delitos informáticos se han convertido en un tema cotidiano para lo sociedad donde nos desarrollamos y que conforme vaya avanzando los medios tecnológicos empleados para cometer este tipo de ilícitos informáticos que afectan principalmente al patrimonio mas desfazada quedara la normativa vigente, por lo cual modificatorias que amplíen la norma como en su sanción es clave para poder identificar e individualizar el tipo penal.

Tabla N°4

Pregunta: 2. En referencia a la pregunta anterior, ¿Considera usted que estas modificatorias son necesarias debido a la mala aplicación de la norma o a la falta de capacitación por parte del Estado a los órganos judiciales?			
MHSC1	GZC2	4ZC3	HCB4
Considero que no es necesaria una modificatoria y si una correcta capacitación de los órganos judiciales.	Considero que ambas tienen incidencia debido que la normativa al no estar actualizada a la realidad social y tecnológica nacional, esto dificulta la labor de los órganos jurisdiccionales al momento de realizar las investigaciones, así como la falta de capacitación crea una falta de eficacia, ya que no se cuentan con los equipos necesarios para combatir este tipo de delitos	En opinión creo que es el conjunto de ambas ya que por una parte al existir ciertos vacíos legales generados de que la norma, no se regula correctamente las nuevas modalidades de ciberdelitos que van surgiendo y no se toma en cuenta el avance tecnológico constante esto en correlación con la poca capacitación que tiene el personal de los órganos judiciales llevan a que no puedan llevar a cabo una correcta investigación.	En mi opinión se debe a la falta de capacitación por parte del estado peruano ya que los órganos judiciales no cuentan con la instrucción necesaria para poder afrontar esta clase de delitos ya que esto genera que no haya una adecuada coordinación.

Coincidencias

Se coincide por unanimidad es que es necesaria una capacitación extensa tanto a la PNP como al Ministerio Publico, debido a que no cuentan con el conocimiento necesario en los nuevos medios tecnológicos que emplean para concretar este tipo de delitos que requiren especial atención ya que para nuestra sociedad se ha convertido en algo cotidiano realizar diversas transacciones sean monetarias o de datos que son el principal objetivo de los ciberdelincuentes.

Asi mismo se considera que existe un vacio legal ya que la normativa no abarca las diversas variaciones en los delitos de fraude informatico y suplantación de identidad

Discrepancias

Se encuentran discrepancias entre los intrevistadoas ya que uno considera que no existen vacíos legales y es mas necesaria solo una capacitación extensa que asegure un mejor funcionamiento de los organismos judiciales.

Interpretación

Como interpretación tenemos que por una amplia mayoría se llega a la conclusión que existen vacíos legales y falta de capacitación tanto de la PNP como el ministerio publico, ya que no se encuentran instruidos adecuadamente para afrontar este tipo de ilícitos penales.

Tabla N°5

Pregunta: 3. A su parecer, ¿A qué se debe la existencia de una deficiente investigación por parte del ministerio público con relación a los delitos de fraude informático y suplantación de identidad?			
MHSC1	GZC2	4ZC3	HCB4
A la falta de reacción e inmediatez debido al desconocimiento sobre el manejo de la criminalidad tecnológica ya que no cuentan con una correcta estructura.	En gran parte es a la complejidad que contienen los delitos informáticos los cuales requieren necesariamente que estos sean ventilados ante una unidad especializada, en este caso la División de Investigación de Delitos de Alta Tecnología (DIVINDAT), ya que fuera de esta no se cuenta con los medios y la capacitación necesaria.	A mi parecer esto se debe a que no se puede llevar a cabo una correcta investigación por parte de los órganos judiciales ya que la norma no tiene en cuenta los nuevos alcances de los delitos de suplantación y fraude informático.	Se debe a la carencia de herramientas para llevar a cabo una correcta investigación ya que solo existe una unidad especializada y ello no da abasto para combatir la ciberdelincuencia eficazmente y llevar una correcta investigación.

Coincidencias

De acuerdo al primer objetivo especiico el cual busca determinar A qué se debe la existencia de una deficiente investigación por parte del ministerio público con relación a los delitos de fraude informático y suplantación de identidad, encontramos que las respuestas planteadas por los especialistas entre ellos nos dan a entender que la mayoría councluye que como principal cincidencia entre los entrevistados tenemos que se considera que no hay las herramientas necesarias para combatir estos delitos, ya que solo la unidad especializada, en este caso la División de Investigación de Delitos de Alta Tecnología (DIVINDAT) es la que esta completamente capacitada para hacer frente a este tipo de delitos, lo que genera que no se de abasto suficiente.

Otro punto importante es que la complejidad de este tipo de delitos genera que no se pueda llevar a cabo una correcta investigación preliminar sin el equipamiento necesario para recolectar los indicios necesarios.

Discrepancias

Encontramos discrepancia ya que si bien es un hecho que no se cuentan en todos los despachos con las herramientas necesarias para llevar a cabo las investigaciones de este tipo de delitos, también se considera que es debido a la falta de normativa que permita encuadrar el tipo penal correspondiente.

Interpretacion

Como interpretación se tiene que es necesario la implementación de herramientas tecnológicas que faciliten las investigaciones, ya que el identificar el tipo penal y darle seguimiento resulta complejo sin los mecanismos necesarios, para lo cual tanto la PNP como el Ministerio Publico deben estar correctamente instruidos en su uso.

Tabla N°6

Pregunta: 4. A su criterio, ¿La deficiente investigación del ministerio público en relación a los delitos de fraude informático y suplantación de identidad se debe a los diferentes vacíos legales y escasez normativa de la criminalidad informática?			
MHSC1	GZC2	4ZC3	HCB4
Creo que es una parte del problema, pero lo principal es capacitar a los órganos jurisdiccionales para que sean efectivos ante este tipo de delitos.	Si, ya que hay nuevos medios de fraude tecnológico que aún no se encuentran regulados en la normativa actual, y por lo tanto no tiene una pena establecida que ayude a poder contrarrestar estos nuevos delitos en función a la criminalidad informática que observamos en la realidad nacional.	Considero que si ya que no esta contemplada en la actual normativa los nuevos medios utilizados en la actualidad para los delitos de suplantación y fraude informático	Si, ya que lo que se refiere a fraude y suplantación de identidad informática considero que la ley no da el alcance necesario y no se lleva a cabo un correcto desarrollo de sus verbos rectores.

Coincidencias

La amplia mayoría de los entrevistados considera que si existen vacíos legales y escasez de normativa que realmente pueda regular correctamente este tipo de delitos ya que existen nuevos medios para los cuales no existe un correcto desarrollo en sus verbos rectores.

Discrepancias

Se tiene como discrepancia el hecho de que mas que escasez normativa es el hecho de que los órganos jurisdiccionales no son efectivos al combatir este tipo de delitos ya que no cuentan con la capacitación necesaria principalmente.

Interpretacion

Como interpretación se tiene que la normativa actual no abarca todas las nuevas modalidades derivadas de la suplantación y el fraude informatico, lo que genera vacíos legales aunado al pobre desarrollo de los verbos rectores en la norma.

Tabla N°7

Pregunta: 5. A su criterio, ¿Qué medidas debe implementar el Estado peruano para poder resolver mejor los casos de fraude informático y suplantación de identidad?			
MHSC1	GZC2	4ZC3	HCB4
Se debe llevar una capacitación extensa a servidores y funcionarios públicos para avanzar combatiendo el ciberdelito e implementar nuevos recursos tecnológicos a favor del ministerio público..	Primeramente, se debe actualizar la normativa a la actualidad tecnológica se la sociedad en que nos desarrollamos, incorporando las diversas modalidades habidas y por haber; segundo, debería implementarse capacitaciones a los servidores y funcionarios públicos del Ministerio Publicoy la Policía Nacional del Perú, a fin de aplicarla ciberseguridad de forma correcta y de este modo poder combatir los delitos informáticos.	Indudablemente llevar a cabo una capacitación de los funcionarios y servidores públicos con el fin de que estos puedan tener un mejor entendimiento y panorama sobre los ciber delitos, igualmente por parte del estado peruano es necesario orientar a la población mediante programas paraque tomen el resguardo necesario al momento de utilizar los diversos medios tecnológicos que se han vuelto algo indispensable para nuestro día a día.	Debe poner a disposición equipos tecnológicos de vanguardia para poder seguir una correcta investigación teniendo en cuenta la naturaleza de este tipo de delitos.

Coincidencias

Como principal coincidencia se tiene que, es necesaria la implementación de herramientas tecnológicas y capacitación por parte del Estado peruano en este tipo de delitos, los cuales requieren una adecuada instrucción en el uso de medios tecnológicos vanguardistas que aseguren la eficacia al momento de realizar las investigaciones y la identiicacion del culpable.

Discrepancias

Se tiene como principales discrepancias el hecho de la importancia de realizar primero la actualización de la normativa y de esta forma resolver con mayor eficacia los casos de raude y suplantación de identidad inormatica en correlación con la capacitación de los nuevos medios delictivos como de las herramientas tecnológicas para combatirlos.

Interpretacion

Se interpreta que las principales medidas a tomar es instruir tanto en los nuevos medios tecnológicos ustilizado para la comisión de estos delitos, como la implmentacion y capacitación sobre nuevas herramientas vanguardistas que permitan agilizar la investigación y asegurar los datos de las victimas e este tipo de delitos.

Tabla N°8

Pregunta: 6. En su opinión,¿La falta de conocimiento y dominio en las investigaciones por delitos de fraude informático y suplantación de identidad se debe a que la normativa no está acorde a la realidad nacional?			
MHSC1	GZC2	4ZC3	HCB4
Es más, una cuestión de capacitación ya que la normativa engloba correctamente la realidad nacional.	Si, y para ello se deben capacitar en las nuevas tecnológicas y en los derechos fundamentales, incrementando un mejor comercio electrónico, a través de las nuevas incorporaciones normativas que necesitan ser implementadas y capacitando a los operadores judiciales de acuerdo a la actual realidad informática de nuestro país.	Opino que si ya que para abordar las nuevas modalidades y los actuales delitos informáticos se deben contar con nuevas herramientas y la realidad nacional nos muestra quelos organismos jurídicos están desfasados en ese aspecto, ya que no hay una adecuación al constante cambio tecnológico que se genera.	En mi opinión si, ya que al momento de la creación de la ley de delitos informáticos estos no eran algo habitual en el día a día, sin embargo, con los diversos avances tecnológicos estos han tomado una relevancia y cotidianeidad que ha dejado desfazada la normativa actual en gran medida.

Coincidencias

De acuerdo al segundo objetivo especifico el cual busca determinar La falta de conocimiento y dominio en las investigaciones por delitos de fraude informático y suplantación de identidad se debe a que la normativa no está acorde a la realidad nacional, encontramos que las respuestas planteadas por los especialistas entre ellos nos dan a entender que la mayoría concluye que como coincidencia principal se llego a que la normativa no esta correctamente ajustada a la realidad nacional del Pais ya que ha sido superada por el constante cambio tecnológico desde la promulgación de la Ley, por lo cual falta implementar nuevas actualizaciones que sancionene con mas severidad.

Discrepancias

Se tiene como una discrepancia que es necesaria solo una correcta capacitación por parte de uno de los entrevistados

Interpretacion

Se puede interpretar que eectivamente la normativa vigente no esta acorde a la realidad nacional ya que en la actualidad las transacciones mediante la banca movil y el almacenamiento de información mediante medios tecnológicos ha ido evolucionando, siendo que estos están siendo vulnerado por métodos como el pishing o el skimming que vulneran la privacidad y el patrimonio de las victimas de estos tipos penales.

Tabla N°9

Pregunta: 7. ¿Qué se debería mejorar en la Ley de delitos informáticos en base a los delitos de fraude y suplantación de identidad informáticos?			
MHSC1	GZC2	4ZC3	HCB4
A mi parecer no es necesaria implementar ninguna mejora en base a la realidad de este tipo de delitos	Se debería implementar nuevos mecanismos de ciberseguridad a fin de tener la certeza de que estos podrán ejercer un correcto control tecnológico, así como establecer nuevas penas de acuerdo a las nuevas modalidades de delitos informáticos.	Como objetivo primordial debería estar el implementar mejores mecanismos de ciberseguridad, así como la promulgación de leyes adecuadas a las nuevas conductas no tipificadas derivada de estos dos delitos que son los mas recurrentes en nuestra sociedad, así mismo implementar sanciones mas severas para.	Se deberían complementar con artículos mediante los cuales se establezca de forma estructurada para poder facilitar la investigación tanto del personal policial como del ministerio público.

Coincidencias

Se coincide por mayoría que en cuanto a los delitos informáticos mencionados se debería aplicar nuevos artículos que involucren una mejor ciberseguridad, en función la ciberseguridad y a las conductas aun no tipificadas, facultando un mejor control tecnológico y fiscalizando el acceso al secreto de las comunicaciones.

Discrepancias

Se tiene como única discrepancia el que uno de los entrevistados no considera indispensable una mejora en base a la normativa vigente.

Interpretacion

Se puede interpretar que es necesario mejorar la ciberseguridad e implementar sanciones mas severas a la vulneración el secreto de las comunicaciones mediante la obtención de datos los cuales son comercializados en el E Commerce.

Tabla N°10

Pregunta: 8. En conclusión, ¿Qué medidas debe tomar el Ministerio Publico y la Policía Nacional para aplicar correctamente la norma penal en relación a los delitos de fraude informático y suplantación de identidad?			
MHSC1	GZC2	4ZC3	HCB4
Se debe efectivizar el desempeño de los efectivos policiales, así como implementar nuevas herramientas tecnológicas que ayuden a reducir los plazos de las investigaciones para este tipo de delitos.	Debe empezar mejorando los medios de identificación de fraude informático y su respuesta hacia ellos, mejorar la seguridad de datos e implementar una capacitación global sobre ciberseguridad.	Principalmente implementar nuevas herramientas de apoyo para agilizar la identificación de aquellos que utilizan los medios tecnológicos para delinquir y de esta manera brindar mayor resguardo a las victimas que resultas perjudicadas de los delitos informáticos de fraude y suplantación.	Se debería realizar un análisis de la realidad nacional para complementar la normativa actual, así como realizar capacitación para mejorar la reacción de la PNP y el ministerio publico y de esta forma encuadrar a los participes con los elementos que el tipo penal requiere.

Coincidencias

Se coincidio por mayoría a que con la actual no se puede relacionar de forma eficaz los delitos, es por eso que entre ambas entidades debe existir una mejor coordinación para brindar medidas adecuadas que ayuden a identificar el uso de las tecnologías y el fraude informático brindando una mejor confiabilidad, integridad y disponibilidad ante los datos de la víctima y de esta forma identificar a los participes con los elementos que el tipo penal requiere.

Otro punto es implementar herramientas que faciliten llevar a cabo las investigaciones por parte de la PNP y el Ministerio Publico aunado a una capacitación global de ciberseguridad.

Discrepancias

No se presentan discrepancias ya que todos comparten globalmente la opinión de que es necesario efectivizar las investigaciones de los mencionados delitos mediante la capacitación e implementación e herramientas tanto la PNP como el Ministerio Publico.

Interpretacion

Se puede interpretar que tanto el Ministerio Publico como la PNP necesitan tomar medidas en cuanto a la implementación tecnológica y capacitarse para pder utilizarlas e forma eficiente a lo largo del proceso penal que engloban los delitos de suplantación y fraude infrmatico, los cuales vulneran los datos mediante los cuales afectan el patrimonio y la privacidad, siendo en muchas ocasiones comerciado estos datos.

V. CONCLUSIONES

Primera:

Se concluye que una de las principales deficiencias identificadas fue la falta de competencia de la policía nacional, del sector público y de los servidores públicos en casos de delitos informáticos, principalmente en la posibilidad de identificar sospechosos y relacionarlos con el tipo de delito como tal; además, otra deficiencia identificada fue la falta de actualizaciones normativas, porque hasta el momento no se han incorporado nuevos modelos y no se han tenido en cuenta los avances tecnológicos que están en constante avance y dejan desfazada la normativa actual.

Segunda:

Tanto el desconocimiento como la falta de dominio en la investigación fueron causados por la aplicación indebida de la norma, así mismo, la determinación de la actual Ley 30096 sobre delitos informáticos debe considerar nuevas disposiciones en materia de mejor ciberseguridad, ya que como se observa el Ministerio Público y La Policía Nacional han ido adoptando ciertas medidas que no tienen una relación válida con el delito en sí, porque no existe una coordinación suficiente entre las dos entidades para brindar mejores medidas que ayuden a identificar el uso de la tecnología y los autores denunciados de fraude informático y la suplantación de identidad.

Tercera:

Los delitos de fraude y suplantación de identidad inormaticos se han encontrado incluso en su regulación desfazados, ya que no se ha modificado en nada desde la publicación de la Ley 30096, siendo que es un delitos que se han ejecutado ampliamente en los últimos años, debido a que en nuestro país existe una amplia inseguridad jurídica en la regulación de la informática tanto en la ejecución del delito, así como en identificar a los participantes del ilícito penal, quienes han ido implmentando diversos métodos no regulados como:

El phishing es una técnica informática que facilita el delito de suplantación de identidad mediante el uso de un mecanismo técnico que simula a un banco para obtener información personal directamente de la víctima.

El spyware es malware que ingresa a la computadora personal de la víctima, a través de técnicas cibernéticas, para extraer información confidencial para reemplazar identidades personales y causar daños morales y económicos.

El skimming es otra técnica computarizada que usa más habilidades físicas y de distracción que cibernéticas para escanear tarjetas bancarias, donde, al igual que con los otros métodos computarizados mencionados anteriormente, se obtiene información confidencial y luego se usa a través del delito de suplantación de identidad para usar los datos obtenidos y causar pérdidas económicas directas a la víctima.

Siendo las anteriormente mencionadas practicas recurrentes en la sociedad peruana que cada vez van más en aumento.

VI. RECOMENDACIONES

Primera:

Llevar a cabo una capacitación continua y sistematica a la policía nacional y ministerios públicos sobre nuevos delitos cibernéticos, así mismo, es de menester incorporar nuevos métodos tecnológicos para poder acelerar la investigación fiscal e identificar claramente el tipo penal.

Segunda:

Establecer una actualización anual de la Ley 30096, tanto en cuantia de las penas como terminología que comprenda el tipo de delito, a fin de que se vayan incorporando los nuevos tipos de delitos informáticos que derivan del fraude y la suplantación de identidad informática y de esta forma efectivizar el actuar fiscal.

Tercera:

Aumentar el control tecnológico teniendo en cuenta que debe existir una cooperación integral entre el Ministerio Público y la Policía Nacional, de este modo uniicar esfuerzs para poder identificar a los autores de los delitos de fraude y la suplantación de identidad informática; y asi reducir la impunidad e inseguriad que sienten las victimas.

REFERENCIAS

Aguilar C. (2008). *El principio del interés del niño y la corte interamericana de derechos humanos. Revista del centro de estudios constitucionales de la universidad de Talca.* Año 6. N° 1. Recuperado el 15 de abril de 2016 de: http://www.cecoch.cl/website/www.cecoch.cl/uploads/pdf/revistas/2008-1/elprincipio11.pdf

Aguilar, B. (2008). *La Familia en el Código Civil Peruano.* (Ed). Lima: Ediciones Legales.

Álvarez, J.L. & Jürgenson, G. (2011). *Como hacer investigación cualitativa: Fundamentos y Metodología.* 1°ed. Barcelona. Ediciones Paidós Ibérica S.A.

Baeza, G. (2001). *El interés superior del niño: Derecho de rango constitucional, su recepción en la legislación nacional y aplicación en la jurisprudencia.* Revista Chilena de Derecho. Vol. 28. N° 2. Recuperado el 15 de abril de 2016 de: https://dialnet.unirioja.es/servlet/articulo?codigo=26503155

Cruz, L. (2011). *Patria potestad y guarda alternada y conjunta o compartida.* Recuperado el 11 de marzo de 2016 de: http://www.bibliojuridica.org/libros/1/434/11.pdf

Garay, A. (2009). *Custodia de los hijos cuando se da fin al matrimonio: Tenencia unilateral o tenencia compartida (Coparentalidad).* Lima. Grigley.

Grosman, C. (2006). *El cuidado de los hijos después del divorcio*. Recuperado el 11 de marzo de 2016 de_ http://www.derecho.uba.ar/multimedia/v_grosman_01.php

Hernández, Ch. (2006). *Contenido personal y patrimonial de la patria potestad y el derecho de comunicación y relación de los padres con sus hijos: Aspectos procesales y sustantivos*. Teleley. Recuperado el 11 de marzo de 2016 de: http://www.teleley.com/articulos/art_110106pc2.pdf.

Montero, S. (1984). *Derecho de Familia*. México. Porrúa S.A

Navarrete, Julio. (2003). *De la construcción del conocimiento social a la práctica de la investigación cualitativa*. Revista de investigaciones sociales de la UNMSM. Año VII. N° 11. Recuperado el 13 de mayo de 2016 de: http://revistasinvestigacion.unmsm.edu.pe/index.php/sociales/article/viewFile/8111/7078

Pérez, M. (2006, Mayo- Agosto). *Reflexiones en torno a la custodia de los hijos. La custodia compartida y las reformas de 2004.* Boletín Mexicano de Derecho Comparado. Vol. XXXIX. Número 116. Recuperado el 14 de abril de 2016 de: http://www.revistas.unam.mx/index.php/bmd/article/view/10652/99800

Placido. A. (2011). *Código Civil Comentado: Comentan 209 especialistas en las diversas materias del derecho civil.* T. III. Derecho de Familia (segunda parte). 3° ed. Lima. Gaceta Jurídica.

Sayago, S. (2014, Diciembre). *El análisis del discurso como técnica de investigación cualitativa y cuantitativa de las ciencias sociales*. Cinta Moebio. Recuperado el 13 de mayo de 2016 de: http://www.redalyc.org/articulo.oa?id=10131417001

Serbia, J. (2007, Agosto). *Diseño, muestreo y análisis en la investigación cualitativa.* Revista académica de la facultad de ciencias sociales UNLZ. Vol.3. N° 7. Recuperado el 13 de mayo de 2016 de: http://www.cienciared.com.ar/ra/revista.php?wid=3&articulo=759&tipo=A&eid=7&sid=136&NombreSeccion=Articulos&Accion=Ver

Varsi, Enrique. (2004). *Divorcio, filiación y patria potestad.* Lima. Grijley

Velazco, M. (2014, Enero-Junio). *Distinción teórica del ejercicio y la titularidad de la patria potestad en interés del menor de edad.* Revista cubana de derecho. IV Época. N° 43. Recuperado el 02 de abril de 2016 de: http://www.lex.uh.cu/sites/default/files/12.-%20RCD%20No.%2043%20En-Jun%202014.pdf

Yarnoz- Yaben, Sagrario. (2010). *Hacia la coparentalidad post- divorcio: Percepción del apoyo de la ex pareja en progenitores divorciados españoles.* International Journal of Clinical and Health Psychology,Vol. 10. Núm. 2. Recuperado el 11 de marzo de 2016 de: http://www.redalyc.org/articulo.oa?id=33712250006

Consuelo Belloch Ortí (2012). Las tecnologías de la información y comunicación, Unidad de Tecnología Educativa. Universidad de Valencia (T.I.C.) : https://www.uv.es/~bellochc/pdf/pwtic1.pdf

Gómez, M. (2006) Introducción a la Metodología de la Investigación Científica. Córdova: Brujas

Hernández, R., Fernández, C y Baptista, L. (2014). Metodología de la investigación. (6ª ed.). México D.F: McGraw-Hill.

Hernández, R y Mendoza, C. (2018). Metodología de la investigación, las rutas cuantitativas cualitativas y mixtas. Ciudad de México.

Quintana, P.A (2006). Metodología de la investigación cualitativa. Revista de Psicología: Tópicos de la actualidad

ANEXOS

INSTRUMENTO DE RECOLECCIÓN DE DATOS ANEXO: 02

GUIA DE ENTREVISTA

Título: “Propuesta modificatoria de artículos 8 y 9 de Ley 30096 ante incremento de Delitos Informáticos.”

Entrevistado/a: ……..
Cargo/profesión/grado académico: ……
Institución: ……..

Categorías	subcategorías
Delito de suplantación de Identidad	Suplantación
	Identidad
	Regulación
Delito de Fraude Informático	Fraude
	Informática
	Regulación

OBJETIVO GENERAL

Analizar los artículos 8 y 9 y proponer una modificatoria ante incremento de Delitos Informáticos

1. En su opinión, ¿Cuáles considera usted que son las modificatorias que se deberían realizar a los delitos de fraude informático y suplantación de identidad en función a la Ley 30096?

_____
_____
_____
_____
_____

2. En referencia a la pregunta anterior, ¿Considera usted que estas modificatorias son necesarias debido a la mala aplicación de la norma o a la falta de capacitación por parte del Estado a los órganos judiciales?

_____
_____
_____
_____

OBJETIVO ESPECIFICO 1

Determinar la efectividad de los artículos 8 y 9 ante incremento de Delitos Informáticos

3. A su parecer, ¿A qué se debe la existencia de una deficiente investigación por parte del ministerio público con relación a los delitos de fraude informático y suplantación de identidad?

4. A su criterio, ¿La deficiente investigación del ministerio público en relación a los delitos de fraude informático y suplantación de identidad se debe a los diferentes vacíos legales y escasez normativa de la criminalidad informática?

5. Para usted, ¿Qué medidas debe implementar el Estado peruano para poder resolver mejor los casos de fraude informático y suplantación de identidad?

OBJETIVO ESPECIFICO 2

Establecer modificatorias de los artículos 8 y 9 ante incremento de Delitos Informáticos

6. En su opinión, ¿La falta de conocimiento y dominio en las investigaciones por delitos de fraude informático y suplantación de identidad se debe a que la normativa no está acorde a la realidad nacional?

_____
_____
_____
_____
_____
_____

7. De su respuesta anterior, ¿Qué se debería mejorar en la Ley de delitos informáticos en base a los delitos de fraude y suplantación de identidad informáticos?

_____
_____
_____
_____
_____
_____

8. En conclusión, ¿Qué medidas debe tomar el Ministerio Publico y la Policía Nacional para aplicar correctamente la norma penal en relación a los delitos de fraude informático y suplantación de identidad?

_____
_____
_____
_____
_____
_____

FIRMA Y SELLO

Lima,…..de .....de 2022.

INSTRUMENTO DE RECOLECCION DE DATOS:

GUIA DE ENTREVISA

Título: “Propuesta modificatoria de artículos 8 y 9 de Ley 30096 ante incremento de Delitos Informáticos.”

Entrevistado/a: Miguel Hernán Sáenz Cabrera
Cargo/profesión/grado académico: Abogado
Institución: Abogado independiente

Categorías	subcategorías
Delito de suplantación de Identidad	Suplantación
	Identidad
	Regulación
Delito de Fraude Informático	Fraude
	Informática
	Regulación

OBJETIVO GENERAL

Analizar los artículos 8 y 9 y proponer una modificatoria ante incremento de Delitos Informáticos

9. En su opinión, ¿Cuáles considera usted que son las modificatorias que se deberían realizar a los delitos de fraude informático y suplantación de identidad en función a la Ley 30096?

   Considero que es necesaria una modificatoria ya que a mi parecer el incremento de los delitos informáticos se debe a las deficiencias en cuanto a las investigaciones fiscales, iniciando por la falta de capacitación hacia los órganos jurisdiccionales y una incorrecta aplicación de la normativa vigente, así como la falta de dominio de investigación en lo que respecta a criminalidad tecnológica

10. En referencia a la pregunta anterior, ¿Considera usted que estas modificatorias son necesarias debido a la mala aplicación de la norma o a la falta de capacitación por parte del Estado a los órganos judiciales?

Considero que no es necesaria una modificatoria y si una correcta capacitación

de los órganos judiciales.

OBJETIVO ESPECIFICO 1

Determinar la efectividad de los artículos 8 y 9 ante incremento de Delitos Informáticos

11. A su parecer, ¿A qué se debe la existencia de una deficiente investigación por parte del ministerio público con relación a los delitos de fraude informático y suplantación de identidad?

A la falta de reacción e inmediatez debido al desconocimiento sobre el manejo de la criminalidad tecnológica ya que no cuentan con una correcta estructura.

12. A su criterio, ¿La deficiente investigación del ministerio público en relación a los delitos de fraude informático y suplantación de identidad se debe a los diferentes vacíos legales y escasez normativa de la criminalidad informática?

Creo que es una parte del problema, pero lo principal es capacitar a los órganos jurisdiccionales para que sean efectivos ante este tipo de delitos.

13. Para usted, ¿Qué medidas debe implementar el Estado peruano para poder resolver mejor los casos de fraude informático y suplantación de identidad?

Se debe llevar una capacitación extensa a servidores y funcionarios públicos para avanzar combatiendo el ciberdelito e implementar nuevos recursos tecnológicos a favor del ministerio público.

OBJETIVO ESPECIFICO 2

Establecer modificatorias de los artículos 8 y 9 ante incremento de Delitos Informáticos

14. En su opinión, ¿La falta de conocimiento y dominio en las investigaciones por delitos de fraude informático y suplantación de identidad se debe a que la normativa no está acorde a la realidad nacional?

    Es más, una cuestión de capacitación ya que la normativa engloba correctamente la realidad nacional.

15. De su respuesta anterior, ¿Qué se debería mejorar en la Ley de delitos informáticos en base a los delitos de fraude y suplantación de identidad informáticos?
    A mi parecer no es necesaria implementar ninguna mejora en base a la realidad de este tipo de delitos

16. En conclusión, ¿Qué medidas debe tomar el Ministerio Publico y la Policía Nacional para aplicar correctamente la norma penal en relación a los delitos de fraude informático y suplantación de identidad?

    Se debe efectivizar el desempeño de los efectivos policiales, así como implementar nuevas herramientas tecnológicas que ayuden a reducir los plazos de las investigaciones para este tipo de delitos.

Miguel Hernán Sáenz Cabrera
ABOGADO
REG. CAI N°. 3381

FIRMA Y SELLO

DNI: 22301056

Título: “Propuesta modificatoria de artículos 8 y 9 de Ley 30096 ante incremento de Delitos Informáticos.”

Entrevistado/a: Zegarra Castañeda, Giany
Cargo/profesión/grado académico: Maestro en Derecho Penal
Institución: Abogado independiente

Categorías	subcategorías
Delito de suplantación de Identidad	Suplantación
	Identidad
	Regulación
Delito de Fraude Informático	Fraude
	Informática
	Regulación

OBJETIVO GENERAL

Analizar los artículos 8 y 9 y proponer una modificatoria ante incremento de Delitos Informáticos

1. En su opinión, ¿Cuáles considera usted que son las modificatorias que se deberían realizar a los delitos de fraude informático y suplantación de identidad en función a la Ley 30096?

Creo que como enfoque principal se debe dar una actualización de los delitos informáticos ya que están en constante cambio y la legislación actual no regula todas las nuevas modalidades que están surgiendo con los nuevos avances tecnológicos.

2. En referencia a la pregunta anterior, ¿Considera usted que estas modificatorias son necesarias debido a la mala aplicación de la norma o a la falta de capacitación por parte del Estado a los órganos judiciales?

Considero que ambas tienen incidencia debido que la normativa al no estar actualizada a la realidad social y tecnológica nacional, esto dificulta la labor de los órganos jurisdiccionales al momento de realizar las investigaciones, así como la falta de capacitación crea una falta de eficacia, ya que no se cuentan con los equipos necesarios para combatir este tipo de delitos.

OBJETIVO ESPECIFICO 1

Determinar la efectividad de los artículos 8 y 9 ante incremento de Delitos Informáticos

3. A su parecer, ¿A qué se debe la existencia de una deficiente investigación por parte del ministerio público con relación a los delitos de fraude informático y suplantación de identidad?

En gran parte es a la complejidad que contienen los delitos informáticos los cuales requieren necesariamente que estos sean ventilados ante una unidad especializada, en este caso la División de Investigación de Delitos de Alta Tecnología (DIVINDAT), ya que fuera de esta no se cuenta con los medios y la capacitación necesaria.

4. A su criterio, ¿La deficiente investigación del ministerio público en relación a los delitos de fraude informático y suplantación de identidad se debe a los diferentes vacíos legales y escasez normativa de la criminalidad informática?

Si, ya que hay nuevos medios de fraude tecnológico que aún no se encuentran regulados en la normativa actual, y por lo tanto no tiene una pena establecida que ayude a poder contrarrestar estos nuevos delitos en función a la criminalidad informática que observamos en la realidad nacional.

5. Para usted, ¿Qué medidas debe implementar el Estado peruano para poder resolver mejor los casos de fraude informático y suplantación de identidad?

Primeramente, se debe actualizar la normativa a la actualidad tecnológica se la sociedad en que nos desarrollamos, incorporando las diversas modalidades habidas y por haber; segundo, debería implementarse capacitaciones a los servidores y funcionarios públicos del Ministerio Publico y la Policía Nacional del Perú, a fin de aplicar la ciberseguridad de forma correcta y de este modo poder combatir los delitos informáticos.

OBJETIVO ESPECIFICO 2

Establecer modificatorias de los artículos 8 y 9 ante incremento de Delitos Informáticos

6. En su opinión, ¿La falta de conocimiento y dominio en las investigaciones por delitos de fraude informático y suplantación de identidad se debe a que la normativa no está acorde a la realidad nacional?

Si, y para ello se deben capacitar en las nuevas tecnológicas y en los derechos fundamentales, incrementando un mejor comercio electrónico, a través de las nuevas incorporaciones normativas que necesitan ser implementadas y capacitando a los operadores judiciales de acuerdo a la actual realidad informática de nuestro país.

7. De su respuesta anterior, ¿Qué se debería mejorar en la Ley de delitos informáticos en base a los delitos de fraude y suplantación de identidad informáticos?

Se debería implementar nuevos mecanismos de ciberseguridad a fin de tener la certeza de que estos podrán ejercer un correcto control tecnológico, así como establecer nuevas penas de acuerdo a las nuevas modalidades de delitos informáticos.

8. En conclusión, ¿Qué medidas debe tomar el Ministerio Publico y la Policía Nacional para aplicar correctamente la norma penal en relación a los delitos de fraude informático y suplantación de identidad?

Debe empezar mejorando los medios de identificación de fraude informático y su respuesta hacia ellos, mejorar la seguridad de datos e implementar una capacitación global sobre ciberseguridad.

DNI: 44300964

INSTRUMENTO DE RECOLECCION DE DATOS:

GUIA DE ENTREVISA

Título: “Propuesta modificatoria de artículos 8 y 9 de Ley 30096 ante incremento de Delitos Informáticos.”

Entrevistado/a: Zegarra Castañeda, Reimy
Cargo/profesión/grado académico: Maestro en Derecho Penal
Institución: Abogado independiente

Categorías	subcategorías
Delito de suplantación de Identidad	Suplantación
	Identidad
	Regulación
Delito de Fraude Informático	Fraude
	Informática
	Regulación

OBJETIVO GENERAL

Analizar los artículos 8 y 9 y proponer una modificatoria ante incremento de Delitos Informáticos

1. En su opinión, ¿Cuáles considera usted que son las modificatorias que se deberían realizar a los delitos de fraude informático y suplantación de identidad en función a la Ley 30096?

Principalmente las modificatorias que se deberían aplicar son en cuanto a la pena y a la actualización de los ilícitos informáticos, ya que la actual Ley 30096 no contempla las nuevas y diversas formas tecnológicas derivados de los delitos de fraude informático y suplantación de identidad.

2. En referencia a la pregunta anterior, ¿Considera usted que estas modificatorias son necesarias debido a la mala aplicación de la norma o a la falta de capacitación por parte del Estado a los órganos judiciales?

En opinión creo que es el conjunto de ambas ya que por una parte al existir ciertos vacíos legales generados de que la norma, no se regula correctamente las nuevas modalidades de ciberdelitos que van surgiendo y no se toma en cuenta el avance tecnológico constante esto en correlación con la poca capacitación que tiene el personal de los órganos judiciales llevan a que no puedan llevar a cabo una correcta

investigación.

OBJETIVO ESPECIFICO 1

Determinar la efectividad de los artículos 8 y 9 ante incremento de Delitos Informáticos

3. A su parecer, ¿A qué se debe la existencia de una deficiente investigación por parte del ministerio público con relación a los delitos de fraude informático y suplantación de identidad?

A mi parecer esto se debe a que no se puede llevar a cabo una correcta investigación por parte de los órganos judiciales ya que la norma no tiene en cuenta los nuevos alcances de los delitos de suplantación y fraude informático.

4. A su criterio, ¿La deficiente investigación del ministerio público en relación a los delitos de fraude informático y suplantación de identidad se debe a los diferentes vacíos legales y escasez normativa de la criminalidad informática?

Considero que si ya que no está contemplada en la actual normativa los nuevos medios utilizados en la actualidad para los delitos de suplantación y fraude informático.

5. Para usted, ¿Qué medidas debe implementar el Estado peruano para poder resolver mejor los casos de fraude informático y suplantación de identidad?

Indudablemente llevar a cabo una capacitación de los funcionarios y servidores públicos con el fin de que estos puedan tener un mejor entendimiento y panorama sobre los ciber delitos, igualmente por parte del estado peruano es necesario orientar a la población mediante programas para que tomen el resguardo necesario al momento de utilizar los diversos medios tecnológicos que se han vuelto algo indispensable para nuestro día a día.

OBJETIVO ESPECIFICO 2

Establecer modificatorias de los artículos 8 y 9 ante incremento de Delitos Informáticos

6. En su opinión, ¿La falta de conocimiento y dominio en las investigaciones por delitos de fraude informático y suplantación de identidad se debe a que la normativa no está acorde a la realidad nacional?

Opino que si ya que para abordar las nuevas modalidades y los actuales delitos informáticos se deben contar con nuevas herramientas y la realidad nacional nos muestra que los organismos jurídicos están desfasados en ese aspecto, ya que no hay una adecuación al constante cambio tecnológico que se genera.

7. De su respuesta anterior, ¿Qué se debería mejorar en la Ley de delitos informáticos en base a los delitos de fraude y suplantación de identidad informáticos?

Como objetivo primordial debería estar el implementar mejores mecanismos de ciberseguridad, así como la promulgación de leyes adecuadas a las nuevas conductas no tipificadas derivada de estos dos delitos que son los más recurrentes en nuestra sociedad, así mismo implementar sanciones más severas.

8. En conclusión, ¿Qué medidas debe tomar el Ministerio Publico y la Policía Nacional para aplicar correctamente la norma penal en relación a los delitos de fraude informático y suplantación de identidad?

Principalmente implementar nuevas herramientas de apoyo para agilizar la identificación de aquellos que utilizan los medios tecnológicos para delinquir y de esta manera brindar mayor resguardo a las víctimas que resultas perjudicadas de los delitos informáticos de fraude y suplantación.

DNI: 44258291

INSTRUMENTO DE RECOLECCION DE DATOS:

GUIA DE ENTREVISA

Título: “Propuesta modificatoria de artículos 8 y 9 de Ley 30096 ante incremento de Delitos Informáticos.”

Entrevistado/a: Luis Alberto, Moreira Saldaña.
Cargo/profesión/grado académico: Abogado
Institución: Abogado independiente

Categorías	subcategorías
Delito de suplantación de Identidad	Suplantación
	Identidad
	Regulación
Delito de Fraude Informático	Fraude
	Informática
	Regulación

OBJETIVO GENERAL

Analizar los artículos 8 y 9 y proponer una modificatoria ante incremento de Delitos Informáticos

1. En su opinión, ¿Cuáles considera usted que son las modificatorias que se deberían realizar a los delitos de fraude informático y suplantación de identidad en función a la Ley 30096?

Lo primero sería implementar penas más severas para este tipo de ilícitos penales, así como el realizar una actualización periódica de las diversas conductas derivadas las cuales no están correctamente reguladas por la normativa peruana.

2. En referencia a la pregunta anterior, ¿Considera usted que estas modificatorias son necesarias debido a la mala aplicación de la norma o a la falta de capacitación por parte del Estado a los órganos judiciales?

En mi opinión se debe a la falta de capacitación por parte del estado peruano ya que los órganos judiciales no cuentan con la instrucción necesaria para poder afrontar esta clase de delitos ya que esto genera que no haya una adecuada coordinación.

.

OBJETIVO ESPECIFICO 1

Determinar la efectividad de los artículos 8 y 9 ante incremento de Delitos Informáticos

3. A su parecer, ¿A qué se debe la existencia de una deficiente investigación por parte del ministerio público con relación a los delitos de fraude informático y suplantación de identidad?

Se debe a la carencia de herramientas para llevar a cabo una correcta investigación ya que solo existe una unidad especializada y ello no da abasto para combatir la ciberdelincuencia eficazmente y llevar una correcta investigación.

.

4. A su criterio, ¿La deficiente investigación del ministerio público en relación a los delitos de fraude informático y suplantación de identidad se debe a los diferentes vacíos legales y escasez normativa de la criminalidad informática?

Si, ya que lo que se refiere a fraude y suplantación de identidad informática considero que la ley no da el alcance necesario y no se lleva a cabo un correcto desarrollo de sus verbos rectores

5. Para usted, ¿Qué medidas debe implementar el Estado peruano para poder resolver mejor los casos de fraude informático y suplantación de identidad?

Debe poner a disposición equipos tecnológicos de vanguardia para poder seguir una correcta investigación teniendo en cuenta la naturaleza de este tipo de delitos.

OBJETIVO ESPECIFICO 2

Establecer modificatorias de los artículos 8 y 9 ante incremento de Delitos Informáticos

6. En su opinión, ¿La falta de conocimiento y dominio en las investigaciones por delitos de fraude informático y suplantación de identidad se debe a que la normativa no está acorde a la realidad nacional?

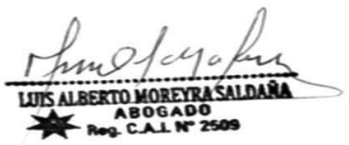
En mi opinión si, ya que al momento de la creación de la ley de delitos informáticos estos no eran algo habitual en el día a día, sin embargo, con los diversos avances tecnológicos estos han tomado una relevancia y cotidianeidad que ha dejado desfasada la normativa actual en gran medida.

7. De su respuesta anterior, ¿Qué se debería mejorar en la Ley de delitos informáticos en base a los delitos de fraude y suplantación de identidad informáticos?

Se deberían complementar con artículos mediante los cuales se establezca de forma estructurada para poder facilitar la investigación tanto del personal policial como del ministerio público.
.

8. En conclusión, ¿Qué medidas debe tomar el Ministerio Publico y la Policía Nacional para aplicar correctamente la norma penal en relación a los delitos de fraude informático y suplantación de identidad?

Se debería realizar un análisis de la realidad nacional para complementar la normativa actual, así como realizar capacitación para mejorar la reacción de la PNP y el ministerio público y de esta forma encuadrar a los partícipes con los elementos que el tipo penal requiere.



VALIDACION DE INSTRUMENTO ANEXO: 03

UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE DERECHO Y HUMANIDADES
ESCUELA PROFESIONAL DE DERECHO

VALIDACIÓN DE INSTRUMENTO

I. DATOS GENERALES

I.1. Apellidos y Nombres: Sayritupac Centeno, Dieter

I.2. Cargo e institución donde labora: Fiscal Adjunto Superior Penal – Ministerio Público

I.3. Nombre del instrumento motivo de evaluación: Guía de Entrevista y Guía de Análisis Documental.

I.4. Autor(A) de Instrumento: **HUAYCA JIMENEZ HAMER GUILLERMO**

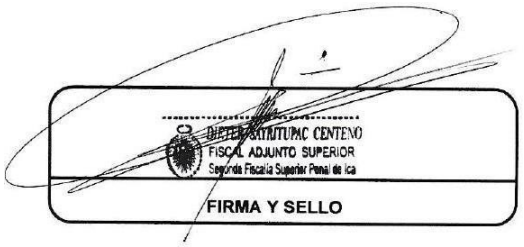
II. ASPECTOS DE VALIDACIÓN

CRITERIOS	INDICADORES	INACEPTABLE						MINIMAMENTE ACEPTABLE			ACEPTABLE			
		40	45	50	55	60	65	70	75	80	85	90	95	100
1. CLARIDAD	Esta formulado con lenguaje comprensible.												X	
2. OBJETIVIDAD	Esta adecuado a las leyes y principios científicos.												X	
3. ACTUALIDAD	Esta adecuado a los objetivos y las necesidades reales de la investigación.											X		
4. ORGANIZACIÓN	Existe una organización lógica.											X		
5. SUFICIENCIA	Toma en cuenta los aspectos metodológicos esenciales												X	
6. INTENCIONALIDAD	Esta adecuado para valorar las variables de la Hipótesis.												X	
7. CONSISTENCIA	Se respalda en fundamentos técnicos y/o científicos.												X	
8. COHERENCIA	Existe coherencia entre los problemas objetivos, hipótesis, variables e indicadores.											X		
9. METODOLOGÍA	La estrategia responde una metodología y diseño aplicados para lograr probar las hipótesis.												X	
10. PERTINENCIA	El instrumento muestra la relación entre los componentes de la investigación y su adecuación al Método Científico.												X	

III. OPINIÓN DE APLICABILIDAD

- El Instrumento cumple con los Requisitos para su aplicación — X
- El Instrumento no cumple con Los requisitos para su aplicación

IV. PROMEDIO DE VALORACIÓN: 93.5 %



Lima, 0... de. 1T-f9.. 2022 .

VALIDACIÓN DE INSTRUMENTO

I. DATOS GENERALES

I.1. Apellidos y Nombres: Dr. Paulett Hauyon, David Saul

I.2. Cargo e institución donde labora: Docente de la Universidad Cesar Vallejo – Sede Lima

I.3. Nombre del instrumento motivo de evaluación: Guía de Entrevista y Guía de Análisis Documental.

I.4. Autor(A) de Instrumento: **HUAYCA JIMENEZ HAMER GUILLERMO**

II. ASPECTOS DE VALIDACIÓN

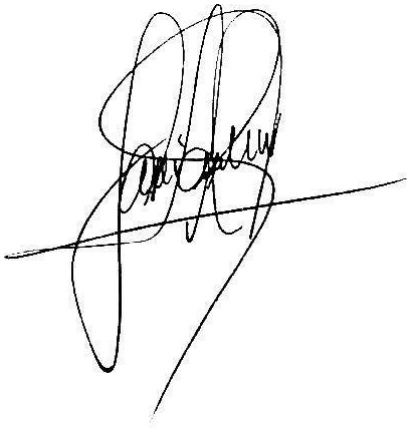
CRITERIOS	INDICADORES	INACEPTABLE						MINIMAMENTE ACEPTABLE			ACEPTABLE			
		40	45	50	55	60	65	70	75	80	85	90	95	100
1. CLARIDAD	Esta formulado con lenguaje comprensible.											x		
2. OBJETIVIDAD	Esta adecuado a las leyes y principios científicos.											x		
3. ACTUALIDAD	Esta adecuado a los objetivos y las necesidades reales de la investigación.											x		
4. ORGANIZACIÓN	Existe una organización lógica.											x		
5. SUFICIENCIA	Toma en cuenta los aspectos metodológicos esenciales											x		
6. INTENCIONALIDAD	Esta adecuado para valorar las variables de la Hipótesis.											x		
7. CONSISTENCIA	Se respalda en fundamentos técnicos y/o científicos.											x		
8. COHERENCIA	Existe coherencia entre los problemas objetivos, hipótesis, variables e indicadores.											x		
9. METODOLOGÍA	La estrategia responde una metodología y diseño aplicados para lograr probar las hipótesis.											x		
10. PERTINENCIA	El instrumento muestra la relación entre los componentes de la investigación y su adecuación al Método Científico.											x		

III. OPINIÓN DE APLICABILIDAD

- El Instrumento cumple con los Requisitos para su aplicación	**X**
- El Instrumento no cumple con Los requisitos para su aplicación	

IV. PROMEDIO DE VALORACIÓN:

90 %



Lima, 28 de Julio de 2022.

VALIDACIÓN DE INSTRUMENTO

V. DATOS GENERALES

V.1. Apellidos y Nombres: Dr. Cesar Jesús Martin, Salcedo Tonemas

V.2. Cargo e institución donde labora: Docente de la Universidad Tecnologica del Perú – Sede Ica

V.3. Nombre del instrumento motivo de evaluación: Guía de Entrevista y Guía de Análisis Documental.

V.4. Autor(A) de Instrumento: **HUAYCA JIMENEZ HAMER GUILLERMO**

VI. ASPECTOS DE VALIDACIÓN

CRITERIOS	INDICADORES	INACEPTABLE						MINIMAMENTE ACEPTABLE			ACEPTABLE			
		40	45	50	55	60	65	70	75	80	85	90	95	100
1. CLARIDAD	Esta formulado con lenguaje comprensible.												x	
2. OBJETIVIDAD	Esta adecuado a las leyes y principios científicos.												x	
3. ACTUALIDAD	Esta adecuado a los objetivos y las necesidades reales de la investigación.												x	
4. ORGANIZACIÓN	Existe una organización lógica.												x	
5. SUFICIENCIA	Toma en cuenta los aspectos metodológicos esenciales												x	
6. INTENCIONALIDAD	Esta adecuado para valorar las variables de la Hipótesis.												x	
7. CONSISTENCIA	Se respalda en fundamentos técnicos y/o científicos.												x	
8. COHERENCIA	Existe coherencia entre los problemas objetivos, hipótesis, variables e indicadores.												x	
9. METODOLOGÍA	La estrategia responde una metodología y diseño aplicados para lograr probar las hipótesis.												x	
10. PERTINENCIA	El instrumento muestra la relación entre los componentes de la investigación y su adecuación al Método Científico.												x	

VII. OPINIÓN DE APLICABILIDAD

- El Instrumento cumple con los Requisitos para su aplicación
- El Instrumento no cumple con Los requisitos para su aplicación

X

95 %

VIII. PROMEDIO DE VALORACIÓN:

Lima, 04 de Agosto de 2022.

MATRIZ DE CATEGORIZACIÓN APRIORÍSTICA ANEXO: 04

Propuesta modificatoria de artículos 8 y 9 de Ley 30096 ante incremento de Delitos Informáticos.	Problema general Analizar los artículos 8 y 9 y proponer una modificatoria ante incremento de Delitos Informáticos Problemas específicos ¿Es eficiente la Ley 30096 ante incremento de Delitos Informáticos con respecto a los artículos 8 y 9?	Objetivo general Analizar los artículos 8 y 9 y proponer una modificatoria ante incremento de Delitos Informáticos Objetivos específicos 1.- Determinar la efectividad de los artículos 8 y 9 ante incremento de	Hipótesis general Existe la necesidad de realizar una modificatoria de los artículos 8 y 9 y ante incremento de Delitos Informáticos en base a la ley 30096 Hipótesis Especifica 1.- Existe la necesidad de determinar la efectividad de los artículos 8 y 9 de la ley 30096, ante incremento de Delitos Informáticos en la sociedad actual 2.- Existe la necesidad de establecer modificatorias a la ley 30096 en base a los	Categorías 1. Delito de suplantación de Identidad 2. Delito de Fraude Informático	Sub categorías 1.1. Suplantación 1.2. Identidad 1.3. Regulación 2.1. Fraude 2.2. Informática 2.3. Regulación	Tipo: Básica Nivel: Descriptivo Diseño: Fenomenológico Enfoque: Cualitativo Escenario de estudio y participantes: ● A nivel nacional, Acuerdos plenarios y expertos. Técnicas e instrumentos: Técnicas

	¿Son necesarias modificatorias de los artículos 8 y 9 ante incremento de Delitos Informáticos?	Delitos Informáticos 2.- Establecer modificatorias de los artículos 8 y 9 ante incremento de Delitos Informáticos	artículos 8 y 9 ante el incremento de Delitos Informáticos en la sociedad actual.	3.Tecnologias de la Información	3.1. Tecnología 3.2. Información	**1)** Entrevista. - Instrumentos **1)** Guía de entrevista Métodos de análisis de investigación ● Fenomenológico

UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE DERECHO Y HUMANIDADES

ESCUELA PROFESIONAL DE DERECHO

Declaratoria de Autenticidad del Asesor

Yo, ESPINOZA AZULA CESAR NAPOLEON, docente de la FACULTAD DE DERECHO Y HUMANIDADES de la escuela profesional de DERECHO de la UNIVERSIDAD CÉSAR VALLEJO SAC - LIMA ESTE, asesor de Tesis titulada: "Propuesta modificatoria de artículos 8 y 9 de Ley 30096 ante incremento de Delitos Informáticos.", cuyo autor es HUAYCA JIMENEZ HAMER GUILLERMO, constato que la investigación tiene un índice de similitud de 27.00%, 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.

LIMA, 02 de Noviembre del 2022

Apellidos y Nombres del Asesor:	**Firma**
ESPINOZA AZULA CESAR NAPOLEON **DNI:** 43443442 **ORCID:** 0000-0002-9928-0422	Firmado electrónicamente por: CESPINOZAZUL el 04-11-2022 10:16:16

Código documento Trilce: TRI - 0436948

INVESTIGA UCV