UNIVERSIDAD INCA GARCILASO DE LA VEGA
ESCUELA DE POSGRADO

MAESTRÍA EN DERECHO PROCESAL PENAL CON MENCIÓN EN DESTREZAS Y TÉCNICAS DE LITIGACIÓN ORAL

TESIS

LA EVIDENCIA DIGITAL Y LOS DELITOS DE FRAUDE INFORMÁTICO TIPIFICADO EN EL CÓDIGO PROCESAL PENAL PERUANO

Presentado por:

JAIME JOEL MORALES VÁSQUEZ

ASESOR: DR. ROBERTO CARLOS MALAVER DANÓS

PARA OPTAR EL GRADO ACADÉMICO DE MAESTRO EN DERECHO PROCESAL PENAL CON MENCIÓN EN DESTREZAS Y TÉCNICAS DE LITIGACIÓN ORAL

LIMA – PERÚ
2021

Visualizador de documentos

Turnitin Informe de Originalidad

Procesado el: 13-jul.-2022 9:35 p. m. -05
Identificador: 1870288566
Número de palabras: 19910
Entregado: 1

TESIS DERECHO PROCESAL PENAL. DR MALAVER Por Jaime Joel Morales Vásquez

Índice de similitud	Similitud según fuente	
27%	Internet Sources:	30%
	Publicaciones:	0%
	Trabajos del estudiante:	8%

incluir citas Excluir bibliografía excluyendo las coincidencias < 3% modo:

ver informe en vista quickview (vista clásica) Change mode imprimir actualizar descargar

6% match (Internet desde 13-feb.-2022)
http://intra.uigv.edu.pe

4% match (Internet desde 27-may.-2020)
https://core.ac.uk/download/pdf/84496928.pdf

3% match (Internet desde 10-mar.-2022)
http://repositorio.uigv.edu.pe

3% match (Internet desde 15-feb.-2022)
http://repositorio.uigv.edu.pe

3% match (Internet desde 13-mar.-2022)
http://repositorio.uigv.edu.pe

3% match (Internet desde 07-ene.-2022)
http://repositorio.uigv.edu.pe

3% match (Internet desde 14-abr.-2021)
https://ius360.com/delitos-informaticos-cuales-son-los-principales-fraudes-informaticos-que-se-pueden-cometer-a-traves-del-e-commerce-oscar-zevallos-prado/

3% match (Internet desde 18-dic.-2018)
https://www.mpfn.gob.pe/Docs/0/files/manual_evidencia_digital.pdf

UNIVERSIDAD INCA GARCILASO DE LA VEGA ESCUELA DE POSGRADO MAESTRÍA EN DERECHO PROCESAL PENAL CON MENCIÓN EN DESTREZAS Y TÉCNICAS DE LITIGACIÓN ORAL TESIS LA EVIDENCIA DIGITAL Y LOS DELITOS DE FRAUDE INFORMÁTICO TIPIFICADO EN EL CÓDIGO PROCESAL PENAL PERUANO Presentado por: JAIME JOEL MORALES VÁSQUEZ ASESOR: DR. ROBERTO CARLOS MALAVER DANÓS PARA OPTAR EL GRADO ACADÉMICO DE MAESTRO EN DERECHO PROCESAL PENAL CON MENCIÓN EN DESTREZAS Y TÉCNICAS DE LITIGACIÓN ORAL LIMA – PERÚ 2021 ii DEDICATORIA A Dios, por cuidarme y guiarme hasta estas instancias de mi vida. iii AGRADECIMIENTOS A mi familia. A mis asesores y profesores de la escuela de postgrado de la UIGV, por compartir sus sabias enseñanzas y apoyarme incondicionalmente, para así lograr mí tan anhelado sueño iv ÍNDICE GENERAL DEDICATORIA ii
AGRADECIMIENTOS
.....
iii ÍNDICE GENERAL
.....iv
ÍNDICE DE CUADROS
.....vi
ÍNDICE DE FIGURAS
.....vii
INDICE DE TABLAS
.....viii

DEDICATORIA

A Dios, por cuidarme y guiarme hasta estas instancias de mi vida.

AGRADECIMIENTOS

A mi familia.

A mis asesores y profesores de la escuela de postgrado de la UIGV, por compartir sus sabias enseñanzas y apoyarme incondicionalmente, para así lograr mí tan anhelado sueño

ÍNDICE GENERAL

ÍNDICE DE CUADROS

ÍNDICE DE FIGURAS

INDICE DE TABLAS

INDICE DE ANEXOS

RESUMEN

El presente trabajo de investigación tuvo como objetivo, determinar la influencia de la Evidencia Digital en los Delitos de Fraude Informático tipificado en el Código Procesal Penal Peruano.

Respecto a los aspectos metodológicos del trabajo, el tipo de investigación fue el explicativo y el nivel aplicado.

La población está conformada por los operadores de justicia del distrito de Independencia, que se encuentran dentro de la Corte Superior de Justicia de Lima Norte, los que ascienden a 200 especialistas.

La muestra estuvo conformada por los 132 operadores de justicia del distrito de Independencia, a los cuales se les aplicó el instrumento que constó de 20 preguntas, utilizando la escala de Likert con alternativas de respuesta múltiple.

Se procedió a analizar los resultados, luego se realizó la contrastación de hipótesis, utilizando la prueba estadística conocida como coeficiente de correlación de Spearman, debido a que las variables de estudio son cualitativas.

Finalmente, se pudo determinar que la Evidencia Digital influye significativamente en los Delitos de Fraude Informático tipificado en el Código Procesal Penal Peruano.

***Palabras claves*:** Evidencia, evidencia digital, delitos, fraude, fraude tributario.

ABSTRACT

The objective of this research work was to determine the influence of Digital Evidence in Computer Fraud Crimes typified in the Peruvian Criminal Procedure Code.

Regarding the methodological aspects of the work, the type of research was explanatory and the level applied.

The population is made up of the logistics operators of the Independencia district, which are within the Superior Court of Justice of Lima Norte, which amount to 200 specialists.

The sample consisted of 132 justice operators from the district of Independencia, to whom the instrument that consisted of 20 questions was applied, using the Likert scale with multiple response alternatives.

The results were analyzed, then hypothesis testing was carried out, using the statistical test known as Spearman's correlation coefficient, since the study variables are qualitative.

Finally, it was determined that Digital Evidence significantly influences Computer Fraud Crimes typified in the Peruvian Criminal Procedure Code.

Key words: Evidence, digital evidence, crimes, fraud, tax fraud.

INTRODUCCIÓN

El 27 de julio del 2015, el gobierno promulgó el Decreto Legislativo 1182, una norma que en la práctica convierte a todos los ciudadanos en posibles criminales a los que hay que mantener vigilados. Fue publicado en el diario oficial El Peruano el decreto legislativo 1182. Norma que viene siendo llamada como 'Ley de Geolocalización' o Ley Stalker (acosador), y ha generado las críticas de un sector de la opinión pública. Este decreto fue inicialmente aceptado. El Gobierno asegura que es una medida potente contra la delincuencia, pero los críticos aseguran que amenaza la privacidad de las comunicaciones.

El Decreto Legislativo 1182 Busca regular el uso de los datos derivados de las telecomunicaciones para la identificación, localización y geolocalización de equipos de comunicación en la lucha contra la delincuencia y el crimen organizado. Crea un mecanismo mediante el cual la Policía puede enviar un pedido a cualquier empresa operadora para acceder a los datos de localización o geolocalización de teléfonos móviles o dispositivos electrónicos. Estos datos son enviados permanentemente por todos los teléfonos móviles conectados a una red de comunicaciones, incluso los que no son Smartphone, y constituyen un registro exacto de cualquier usuario. Según el nuevo Decreto, empresas como Movistar o Claro estarán inmediatamente obligadas a proporcionar acceso en tiempo real a la Policía Nacional. Para lograrlo, hasta ahora era necesaria una autorización judicial expresa. Sin embargo, bajo este nuevo sistema la Policía ya no necesitará obtener ningún tipo de autorización previa para acceder a esta información.

La ley tiene como objetivo prevenir y sancionar las conductas ilícitas que afectan los sistemas y datos informáticos, y otros bienes jurídicos de relevancia penal, realizadas con el uso de tecnologías de la información o de la comunicación Con este, aquel que ingresa sin

permisión al sistema informático, con violación de las medidas de seguridad, recibirá una pena de uno a cuatro años de prisión. En el caso de interceptación de datos informáticos en transmisiones no públicas, la sanción será no menor de tres ni mayor de seis años. El delito se aumenta a entre cinco y ocho años de cárcel cuando el delito recaiga en información clasificada como secreta, reservada o confidencial, y la pena es entre ocho y diez años de prisión cuando comprometa la defensa, seguridad o soberanía nacional. La ley agrega normas para informar los fraudes informáticos, la suplantación de identidad, interceptación telefónica, la función de la policía es el descubrimiento del delito de los delitos informáticos en que busca que se pueda reducirse la criminalidad en esta materia.

Es por esta razón, que la presente tesis, pretende determinar la influencia de la Evidencia Digital en los Delitos de Fraude Informático tipificado en el Código Procesal Penal Peruano.

El estudio fue elaborado en varios capítulos, estableciéndose así en el primero de ellos los fundamentos teóricos, donde se incluyen los antecedentes de la investigación, marco teórico, así como el marco conceptual correspondiente.

El segundo capítulo, que se titula el problema de la investigación, abarcó la descripción de la realidad problemática, delimitación de la investigación y planteamiento del problema, así como los objetivos, hipótesis y las variables e indicadores, luego concluyéndose con la justificación e importancia del estudio.

En el tercer capítulo, se muestra la metodología empleada, comprendiendo la misma el tipo y diseño, población y muestra, así como la técnica e instrumento de recolección de datos y las técnicas de procesamiento y análisis de datos.

En el cuarto capítulo, titulado presentación y análisis de resultados, se consideró la presentación de resultados, discusión de resultados y contrastar la hipótesis.

Finalmente, en el quinto capítulo se menciona las conclusiones que se arribaron durante el presente trabajo de investigación, así como también las recomendaciones que corresponda.

CAPITULO I. FUNDAMENTOS TEÓRICOS DE LA INVESTIGACIÓN

1.1 Marco Histórico

Evidencia digital

La tecnología forma parte importante de nuestra vida cotidiana en la medida que todos contamos con una cuenta de correo electrónico, utilizamos dispositivos electrónicos en nuestros trabajos tales como celulares, agendas electrónicas, relojes inteligentes, los cuales nos permiten controlar nuestro quehacer diario o, también, empleamos aplicaciones para interactuar con el resto de la comunidad.

No obstante, la delincuencia también se ha transformado empleando herramientas tecnológicas sofisticadas para la comisión de delitos; toda vez que, el perpetrador busca ocultar su identidad y maximizar sus ilícitas ganancias.

Por ello nuestro país se ha fortalecido en la lucha contra los delitos informáticos a través de la Ley Nº 30096 del 22 de octubre del 2013, lo cierto es que las Nuevas Tecnologías no son de uso exclusivo de los ciberdelincuentes pues se emplean para facilitar la comisión de delitos tradicionales.

Por ejemplo, en la investigación de un homicidio será importante conocer con quién o quiénes se comunicó al investigado antes y después del suceso. En una investigación de trata de personas, será útil conocer los perfiles que en las diversas redes sociales pueden administrar los imputados. En una investigación de lavado de activos, la información contable necesaria no se encontrará únicamente en libros o documentos físicos, el investigador debe saber que mucha información se encuentra en la nube y en dispositivos electrónicos.

Los operadores jurídicos también tienen a su disposición herramientas modernas para la investigación del delito; sin embargo, si no las emplean adecuadamente podrían generar la exclusión de importantes medios de prueba o el cuestionamiento de su actuación.

Fraude electrónico

Mediante la Ley Nº 30096, "Ley de Delitos Informáticos", cuya norma tipifica las conductas penalmente relevantes que afectan los sistemas y datos informáticos, la indemnidad y libertad sexuales, la intimidad y el secreto de las comunicaciones, el patrimonio y la fe pública, en los cuales el criminal utiliza la tecnología con la finalidad de cometer diferentes ilícitos penales.

En el año 2013 se publicó en nuestro país la Ley Nº 30096, "Ley de Delitos Informáticos", que tuvo por objeto prevenir y sancionar las conductas ilícitas que afectan los sistemas y datos informáticos, la indemnidad y libertad sexuales, la intimidad y el secreto de las comunicaciones, el patrimonio y la fe pública, en los cuales el delincuente utiliza la tecnología actual para cometer dichos ilícitos.

La mencionada norma sufrió una modificación mediante la Ley Nº 30171 publicada el año 2014, en la cual se agregó a los tipos penales acceso ilícito (artículo 2º), atentado a la integridad de datos informáticos y sistemas informáticos (artículos 3º y 4º), interceptación de datos informáticos (artículo 7º), fraude informático (artículo 8º) y abuso de mecanismos y dispositivos informáticos (artículo 10º) las palabras "deliberada e ilegítimamente", reafirmando que dichos tipos penales se cometen de forma dolosa, y se derogó el artículo 6º que tipificaba el tráfico ilegal de datos.

Ahora bien, es importante señalar que nuestros legisladores al momento de elaborar la mencionada Ley utilizaron como base el "Convenio sobre la Ciberdelincuencia" o más conocido como el "Convenio de Budapest".

Dicho Convenio que se firmó en el año 2001 y entró en vigor internacionalmente en el año 2004- es un tratado internacional creado por los países miembros del Consejo de Europa

“con el fin de hacer frente a los delitos informáticos a través de mecanismos de homologación de normas de derecho penal sustantivo, estandarización de procesos penales y cooperación internacional”.

Al respecto de este convenio, es muy curioso que recién en el año 2019 el Poder Legislativo lo haya aprobado por Resolución Legislativa N° 30913, de fecha 12 de febrero de 2019, y con fecha 10 de marzo de ese mismo año el Poder Ejecutivo lo ratificó mediante Decreto Supremo Nº 010-2019-RE, cuando desde el año 2013 ya existía una Ley de Delitos Informáticos en el país y donde el mencionado Convenio hubiera sido de mucha utilidad para que los operadores de justicia puedan tomar conciencia sobre la protección de la seguridad informática y la cultura digital que debe existir en el país.

1.2 Marco Teórico

Evidencia digital

La evidencia digital es todo registro informático almacenado en un dispositivo informático o que se transmite a través de una red informática y que pudiera tener valor probatorio para una investigación.

Se considera evidencia digital a cualquier información que, sujeta a una intervención humana, electrónica, y/o informática, ha sido extraída de cualquier clase de medio tecnológico informático computadoras, etc.

Técnicamente, es un tipo de evidencia física que está constituida por campos magnéticos y pulsos electrónicos que pueden ser recolectados y analizados con herramientas técnicas especiales. La importancia de la evidencia digital reside en la necesidad de demostrarle al juez la prueba fehaciente que convierte en responsable al sospechoso. Por eso, es fundamental la correcta selección de la prueba relevante por parte del experto para no ser sobre abundante o superflua.

El correcto tratamiento de la evidencia digital es fundamental para que sea admisible: haber sido obtenida respetando las garantías y procedimientos legales, basada en una previa

autorización judicial o del director de investigación, justificando su tratamiento en los procedimientos de obtención, preservación, análisis y presentación ante el tribunal, respetando la cadena de custodia, cuyos pasos deberá desprenderse de un manual de buenas prácticas.

Asimismo, deben poder justificarse todos los métodos y acciones realizadas en el tratamiento de la evidencia digital, a través de la demostración de la validación de los métodos utilizados y de los procesos realizados. También se deberá documentar las acciones realizadas y justificar todas las decisiones en las etapas del proceso, y se deben obtener los mismos resultados en caso de aplicar el mismo procedimiento, pero con herramientas diferentes, en cualquier momento.

Reconocimiento de la evidencia digital

Es importante clarificar los conceptos y describir la terminología adecuada que nos señale el rol que tiene un sistema informático dentro del iter criminis o camino del delito.

Esto a fin de encaminar correctamente el tipo de investigación, la obtención de indicios y posteriormente los elementos probatorios necesarios para sostener nuestro caso.

Es así que por ejemplo, el procedimiento de una investigación por homicidio que tenga relación con evidencia digital será totalmente distinto al que, se utilice en un fraude informático, por tanto el rol que cumpla el sistema informático determinara DONDE DEBE SER UBICADA Y COMO DEBE SER USADA LA EVIDENCIA.

Ahora bien para este propósito se han creado categorías a fin de hacer una necesaria distinción entre el elemento material de un sistema informático o hardware (evidencia electrónica) y la información contenida en este (evidencia digital).

Esta distinción es útil al momento de diseñar los procedimientos adecuados para tratar cada tipo de evidencia y crear un paralelo entre una escena física del crimen y una digital.

En este contexto el hardware se refiere a todos los componentes físicos de un sistema informático, mientras que la información, se refiere a todos los datos, programas almacenados y mensajes de datos trasmitidos usando el sistema informático.

Admisión de la prueba en el juicio

Los requisitos que debe cumplir una evidencia digital para ser admitida como prueba en un juicio son:

- Auténtica: debe haber sido obtenida y registrada en el lugar de los hechos y debe garantizarse la integridad de los archivos.
- Confiable: esta evidencia digital debe proceder de fuentes fiables. Es decir, es confiable si el sistema que la produjo no ha sido violado y funcionaba correctamente cuando se generó o guardó esa prueba.
- Integra: para que esa prueba sea suficiente debe estar completa.
- Cumplir las reglas del poder judicial: es necesario que esa evidencia sea acorde con las leyes y disposiciones vigentes en el ordenamiento jurídico.

Para proteger una evidencia digital es necesario realizar copias usando nuevos sistemas de almacenamiento y permitir el acceso a la misma únicamente a un perito informático.

Las evidencias digitales deben protegerse, controlarse, etiquetarse y controlarse. La responsabilidad corresponde al perito que las tenga en su poder o a la persona autorizada para custodiarlas.

La prueba dentro del proceso penal es de especial importancia, ya que desde ella se confirma o desvirtúa una hipótesis o afirmación precedente, se llega a la posesión de la verdad material.

Tecnologías de la Información y la Comunicación. - De esta manera se confirmará la existencia de la infracción y la responsabilidad de quienes aparecen en un inicio como presuntos responsables, todo esto servirá para que el Tribunal de Justicia alcance el conocimiento necesario y resuelva el asunto sometido a su conocimiento.

El objetivo de la Informática forense es el de recobrar los registros y mensajes de datos existentes dentro de un equipo informático, de tal manera que toda esa información digital, pueda ser usada como prueba ante un tribunal.

Dónde encontrar la evidencia digital

1. Dispositivos de almacenamiento informático Pueden ser:

• Unidades de disco rígido internas: discos de aluminio o vidrio, recubiertos de material ferro magnético, cabeza de lectura/escritura.

• Discos rígidos externos: requieren fuente de alimentación y un USB, FireWire, Ethernet, conexión inalámbrica.

2. Medios extraíbles: Son unidades de disco para almacenar, archivar y transportar datos, entre ellos:

• Pendrive (USB): Dispositivo de almacenamiento extraíble mediante conexión USB.

• Tarjeta de memoria: dispositivo de almacenamiento de datos de uso en cámaras digitales, teléfonos celulares, reproductores de música digital, notebook, consolas de videojuego, PDAs, Smart TV. Posibles evidencias: mensajes de correo, historial de navegación de Internet, Chat de Internet, listas de registros, fotografías en distintos formatos de archivos (JPG, PNG, GIF, BMP, TIF), archivos de imágenes, documentos, archivos de texto, metadatos de archivos, claves en memoria, claves de encriptación, etc.

• Dispositivos portátiles

• Teléfonos celulares

• Smartwatches

• PDAs

• Dispositivos digitales multimedia

• Cámaras digitales • Sistemas de posicionamiento global (GPS)

• Reproductores

• Video filmadoras

• Localizador

• Sistemas en vehículos

• Cámaras de seguridad

Posibles evidencias: Listado de llamados, mensajes recibidos y enviados, páginas de Internet visitadas, datos de localización geográfica, aplicaciones de software, documentos, mensajes de correo, historial de navegación de Internet, chat de Internet, fotografías, archivos de imágenes, base de datos y registros, mensajes de voz, redes Wi-Fi detectadas.

Los cibercriminales intentan modificar o eliminar la evidencia digital variando el rastro. Pero eso no es suficiente para que puedan salir impunes porque:

- Puede obtenerse una copia exacta e irrefutable de esa evidencia digital.
- A través de herramientas de informática forense puede comprobarse el original con la evidencia digital y establecer si ha sido modificada.
- Es posible recuperar los discos duros, aunque se hayan borrado.

Principios del Peritaje:

1. Objetividad: Es un requisito que le compete tanto al fiscal que dirige la investigación y por ende elabora los puntos de pericia a realizarse, como al perito informático que analizará la información previamente identificada, asegurada, adquirida y preservada a los fines de su análisis.

2. Legalidad: El perito deberá ser preciso en sus conclusiones, en la metodología utilizada para arribar al resultado, y su actuación será acorde a la legislación de la actividad técnica-informática-pericial.

3. Idoneidad: Las herramientas informáticas utilizadas deberán ser idóneas y validadas para otorgar apoyatura a las conclusiones arribadas.

4. Inalterabilidad: Será fundamental el debido cumplimiento de la cadena de custodia que asegure que no ha existido alteración ni modificación en el peritaje.

Fraude electrónico

Antes de desarrollar los ilícitos de fraude informático y suplantación de identidad, es importante definir qué se entiende por delitos informáticos, los cuales son:

“aquellas conductas dirigidas a burlar los sistemas de dispositivos de seguridad, esto es, invasiones a computadoras, correos o sistemas de datas mediante una clave de acceso; conductas típicas que únicamente puede ser cometidas a través de la tecnología. En un sentido amplio, comprende a todas aquellas conductas en las que la Tecnología de la Información y

Comunicación (TIC) son el objetivo, el medio o el lugar de ejecución, aunque afecten a bienes jurídicos diversos (…)"

En cuanto al bien jurídico, se entiende que se protege

"en general (…) la información, pero está considerada de diferentes formas, ya sea como un valor económico, como un valor intrínseco a la persona, por su fluidez y tráfico jurídico, y finalmente por los sistemas que la procesan o automatizan";

En otras palabras, también se deben proteger los bienes jurídicos tradicionales afectados a través de este tipo de delitos como son: el patrimonio, la reserva y confidencialidad de los datos, la fe pública, la indemnidad sexual y otros, por lo que comparto la opinión de diversos autores que afirman que se trata de un delito pluriofensivo, pues afecta varios bienes jurídicos.

Habiendo explicado la definición de los delitos informáticos y el bien jurídico protegido, debemos desarrollar el delito de fraude informático, el cual se encuentra previsto en el artículo 8º de la Ley Nº 30096, que señala expresamente lo siguiente:

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

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

De la redacción del tipo penal, se advierte que este ilícito lo puede cometer cualquier persona y en cuanto al sujeto pasivo también puede ser cometido contra cualquier persona natural, persona jurídica, institución bancaria e incluso gobiernos que usan sistemas automatizados de información, conectados unos entre otros.

Asimismo, este delito sanciona las conductas de diseñar hacer un diseño, introducir entrar en un lugar, alterar estropear, dañar o descomponer, borrar desvanecer, suprimir hacer cesar, hacer desaparecer, clonar producir clones, interferir introducirse en la recepción de una señal y perturbarla o manipular intervenir con medios hábiles en la información un sistema informático todo dispositivo aislado o conjunto de dispositivos interconectados o relaciones entre sí, cuya función, o la de alguno de sus elementos, sea el tratamiento automatizado de datos en ejecución de un programa en perjuicio de un tercero.

Esta figura penal se clasifica como un delito de resultado, toda vez que no basta con realizar las conductas típicas mencionadas, sino que además es necesario que esa acción vaya seguida de un resultado separado de la misma conducta el cual es causar un perjuicio económico.

La redacción del tipo penal, deliberada e ilegítimamente nos evidencia que únicamente se puede cometer de forma dolosa, no cabiendo la comisión por culpa; es decir, el agente debe tener la conciencia y voluntad de diseñar, introducir, alterar borrar, suprimir, clonar, interferir o manipular de forma ilegítima un sistema informático.

El otro delito que desarrollaremos, suplantación de identidad, se encuentra previsto en el artículo 9º de la mencionada Ley, que señala lo siguiente:

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

En cuanto al sujeto activo, se advierte que este ilícito lo puede cometer cualquier persona y respecto al sujeto pasivo puede ser cometido contra cualquier persona natural o jurídica.

Asimismo, este delito sanciona la conducta de suplantar ocupar con malas artes el lugar de alguien la identidad de una persona natural o jurídica; en estos casos, el criminal

ocupa la identidad de una persona natural o jurídica mediante cuentas de correo o redes sociales falsas con la finalidad de engañar y perjudicar a la víctima.

Delito informático

Concepto:

Es toda aquella acción antijurídica que se realiza en el entorno digital, espacio digital o de Internet. Con el uso de las nuevas tecnologías en todas las esferas de la vida y el creciente número de usuarios, como consecuencia de la globalización digital de la sociedad, la delincuencia también se ha expandido a esa dimensión.

Gracias al anonimato y a la información personal que se guarda en el entorno digital, los delincuentes han ampliado su campo de acción y los delitos y amenazas a la seguridad se han incrementado exponencialmente.

Además de los ataques que tienen como objetivo destruir y dañar activos, sistemas de información u otros sistemas de computadoras, utilizando medios electrónicos y/o redes de Internet, se producen nuevos delitos contra la identidad, la propiedad y la seguridad de las personas, empresas e instituciones, muchos de ellos como consecuencia del valor que han adquirido los activos digitales para la big data empresarial y sus propietarios bien sean entes jurídicos o personas naturales.

Existen también otras conductas criminales que aunque no pueden considerarse como delito, se definen como ciberataques o abusos informáticos y forman parte de la criminalidad informática. La criminalidad informática consiste en la realización de un tipo de actividades que, reuniendo los requisitos que delimitan el concepto de delito, son llevados a cabo utilizando un elemento informático.

Nidia Callegari define al delito informático como “aquel que se da con la ayuda de la informática o de técnicas anexas”. Este concepto tiene la desventaja de solamente considerar como medio de comisión de esta clase de delitos a la informática, olvidándose la autora que también que lo informático puede ser el objeto de la infracción.

CALLEGARI, Nidia, Citada por Julio Telles Valdés. Ob. Cita.

Davara Rodríguez define al Delito informático como, la realización de una acción que, reuniendo las características que delimitan el concepto de delito, sea llevada a cabo utilizando un elemento informático y/o telemático, o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software.

Según Julio Téllez Valdés conceptualiza al delito informático en forma típica y atípica, entendiendo por la primera a "las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin" y por las segundas "actitudes ilícitas en que se tienen a las computadoras como instrumento o fin".

Como ya se señaló anteriormente, determinados enfoques doctrinales subrayarán que el delito informático, más que una forma específica de delito, supone una pluralidad de modalidades delictivas vinculadas, de algún modo con los computadores, a este respecto el profesor Romeo Casabona señala que el término Delito Informático debe usarse en su forma plural, en atención a que se utiliza para designar una multiplicidad de conductas ilícitas y no una sola de carácter general.

Se hablará de delito informático cuando nos estemos refiriendo a una de estas modalidades en particular.

Parker define a los delitos informáticos como "todo acto intencional asociado de una manera u otra a los computadores; en los cuales la víctima ha o habría podido sufrir una pérdida; y cuyo autor ha o habría podido obtener un beneficio", Parker además entrega una tabla en que la que se definen los delitos informáticos de acuerdo con los propósitos que se persiguen:

1. Propósito de investigación de la seguridad: abuso informático es cualquier acto intencional o malicioso que involucre a un computador como objeto, sujeto, instrumento o símbolo donde una víctima sufrió o podría haber sufrido una pérdida y el perpetrador obtuvo o pudo haber obtenido una ganancia (Parker, Nycum and Oura, 1973).

2. Propósito de investigación y acusación: delito informático es cualquier acto ilegal cuya perpetración, investigación o acusación exige poseer conocimientos de tecnología informática (Departamento de Justicia de Estados Unidos).

3. Propósito legal: delito informático es cualquier acto tal como está especificado en una ley sobre delito informático en la jurisdicción en que la norma se aplica.

4. Otros propósitos: abuso informático (sea cual sea su objetivo), es cualquier delito que no puede ser cometido sin computador.

Delito:

La teoría del delito es parte de la ciencia del derecho penal que se ocupa de explicar que es el delito en general, es decir, cuáles son las características que debe tener cualquier delito, esto facilita la averiguación de la presencia o ausencia del delito en cada caso concreto.

Este criterio suministro al legislador el poder ordenar una pena o dejar impune; de esta manera nació la necesidad de imponer sanciones, algunas veces un tanto drásticas, a aquellas conductas humanas que eran reprochables para la sociedad y que por ende contaminaban la vida armónica de los seres humanos.

El Derecho Penal se ha convertido con el pasar del tiempo en una herramienta efectiva que el legislador empezó a utilizar para ponerle orden a la sociedad. El concepto de delito se define desde diferentes perspectivas, pero todas apuntan a un mismo horizonte.

Según Franceso Carneluti, el delito es un producto de conflicto intersubjetivo de intereses, por eso el delito es un modo de ser de la sociedad, no del individuo.

CARNELUTTI, Francesco. El delito. Editorial Leyer. Bogotá D.C.:2005, Pg8.

Jackobs señala que “el delito es una comunicación defectuosa, una desautorización de la norma o falta de fidelidad a la misma. La norma es una expectativa social institucionalizada.

JACKOBS, Gunther. Strafrechtt Allgeimeiner Tell, Berlín, 1993, págs. 34 y 36, citado por Velásquez.

Para Carrara es “una infracción a la ley de un Estado, promulgada para proteger la

seguridad de los ciudadanos, resultante de un acto externo del hombre, positivo o negativo, moralmente imputable y políticamente dañosos".

El delito es una conducta del hombre que puede darse de forma positiva o negativa, dentro de la cantidad de comportamientos posibles de los seres humanas sólo algunas de estas se pueden llamar delitos. Para poder determinar aquellas conductas que deban ser calificadas como delitos debemos acudir al Código Penal donde el legislador ha identificado las conductas prohibidas cuya consecuencia es la imposición de una pena.

En consecuencia, no se hablará de delito mientras la conducta realizada no se encuentre tipificada como tal en el ordenamiento legal.

De este modo hablaremos de dos caracteres del delito: Genérico (i) Conducta y Especifico (Tipicidad), es decir podemos decir que la conducta típica es una especie del género conducta.

Sin embargo, con la sola característica de tipicidad no se individualiza la especie delito, puesto que no toda conducta típica es delito, ya que existen dentro del derecho penal circunstancias en las que opera una justificación como exclusión del carácter delictivo de la conducta típica tales como la legitima defensa o el estado de necesidad y, en general, de supuestos de "legítimo ejercicio de derecho".

En ese sentido, podemos decir que cuando la conducta típica no está permitida o tiene causal de justificación delictiva diremos que, además de típica, será también contraria al orden jurídico funcionando como unidad armónica.

Ciberdelitos

Las primeras definiciones acerca del Ciber Delito lo realizo Parker (1976) quien define el Ciber Crimen o Delito Informático como "cualquier incidente asociado con la tecnología de los ordenadores en el que la víctima sufrió o pudo haber sufrido un daño y el autor, intencionadamente, obtuvo o pudo haber obtenido un beneficio" (p.12).

Por esas mismas épocas Camacho (1987) considerando que no había una definición clara del ciber crimen considera a este hecho como:

“Toda acción dolosa que provoca un perjuicio a personas o entidades sin que necesariamente conlleve un beneficio material para su autor aun cuando no perjudique de forma directa o inmediata a la víctima y en cuya comisión intervienen necesariamente de forma activa dispositivos habitualmente utilizados en las actividades informáticas” (p.25).

Sin embargo, con la expansión universal del internet en los últimos 10 años ha dado paso a nuevos análisis y conceptos ajustados más a nuestra realidad actual.

En ese sentido Téllez-Valdez (2017) indica lo siguiente:

Un delito informático o ciberdelito es toda aquella acción antijurídica y culpable a través de vías informáticas o que tiene como objetivo destruir y dañar ordenadores, medios electrónicos y redes de Internet.

Debido a que la informática se mueve más rápido que la legislación, existen conductas criminales por vías informáticas que no pueden considerarse como delito, según la "Teoría del delito", por lo cual se definen como abusos informáticos, y parte de la criminalidad informática. (p.187)

En un sentido más amplio LINARES (2012) comprende al Ciber crimen como

“todas aquellas conductas en las que las TIC son el objetivo, el medio o el lugar de ejecución, aunque afecten a bienes jurídicos diversos; y que plantea problemas criminológicos y penales, originados por las características propias del lugar de comisión” (p .44)

Finalmente, tomando en consideración un entorno más cercano y ajustado a nuestra realidad como país, tomamos en consideración el aporte Villavicencio Terreros (2014) quien define el delito Informático como “aquellas conductas dirigidas a burlar los sistemas de dispositivos de seguridad, esto es, invasiones a computadoras, correos o sistemas de datas mediante una clave de acceso; conductas típicas que únicamente pueden ser cometidas a través de la tecnología” (p. 49).

De acuerdo con las definiciones encontradas y bibliografía consultada, llegamos a la conclusión que el ciber delito es un acto criminal realizad de manera digital en contra de una persona o entidad con el fin de obtener beneficio a raíz de dicho acto, así mismo podemos decir que no siempre genera un beneficio económico o material.

Así también podemos decir que los Ciberdelitos son actitudes contrarias a los intereses de las personas teniendo como instrumento o fin (concepto atípico) a las computadoras.

En la actualidad debe hablarse de ciberdelitos, pues este concepto sustantiva las consecuencias que se derivan de la peculiaridad que constituye la red digital como medio de comisión del hecho delictivo, y que ofrece contornos singulares y problemas propios, como por ejemplo la dificultad de determinar el lugar de comisión de tales hechos ilícitos, indispensable para la determinación de la jurisdicción y competencia penal, para su enjuiciamiento y aplicación de la correspondiente ley penal, los problemas para la localización y obtención de las pruebas de tales hechos delictivos, la insuficiente regulación legal de los ilícitos que pueden realizarse a través de la Red o de las diligencias procesales de investigación aplicables para el descubrimiento de los mismos –normativa igualmente desbordada por el imparable avance de las innovaciones tecnológicas, o, en fin, la significativa afectación que la investigación policial en Internet tiene sobre los derechos fundamentales de los ciudadanos.

La Organización de Naciones Unidas reconoce los siguientes tipos de delitos informáticos:

1. Fraudes cometidos mediante manipulación de computadoras; en este se reúne: la manipulación de datos de entrada (sustraer datos), manipulación de programas (modificar programas del sistema o insertar nuevos programas o rutinas), manipulación de los datos de salida (fijación de un objeto al funcionamiento de sistemas de información, el caso de los cajeros automáticos) y fraude efectuado por manipulación informática (se sacan pequeñas cantidades de dinero de unas cuentas a otras).

2. Manipulación de datos de entrada; como objetivo cuando se altera directamente los datos de una información computarizada. Como instrumento cuando se usan las computadoras como medio de falsificación de documentos.

3. Daños o modificaciones de programas o datos computarizados; entran tres formas de delitos: sabotaje informático (eliminar o modificar sin autorización funciones o datos de una computadora con el objeto de obstaculizar el funcionamiento) y acceso no autorizado a servicios y sistemas informáticos (ya sea por curiosidad, espionaje o por sabotaje).

La criminalidad informática incluye una amplia variedad de delitos informáticos. El fenómeno se puede analizar en dos grupos:

1. Informática como objeto del delito: Esta categoría incluye por ejemplo el sabotaje informático, la piratería informática, el hackeo, el crackeo y el DDNS (Denegación de servicio de nombres de dominio).

2. Informática como medio del delito: Dentro de este grupo se encuentra la falsificación de documentos electrónicos, cajeros automáticos y tarjetas de crédito, robo de identidad, phreaking, fraudes electrónicos y pornografía infantil.

Delitos Informáticos en el Perú

En el caso del Perú, los delitos informáticos se encuentran regulados en el Código Penal, en el Capítulo X referido a Delitos Informáticos.

Asimismo, la Ley N°30096, Ley de Delitos Informáticos establece las penalidades frente a la comisión de ciertos delitos de índole informáticos siendo el objetivo de esta ley prevenir y sancionar las conductas ilícitas que afectan los sistemas y datos informáticos y otros bienes jurídicos de relevancia penal, cometidas mediante la utilización de tecnologías de la información o de la comunicación, con la finalidad de garantizar la lucha eficaz contra la ciberdelincuencia.

El Estado Peruano ha creado la Secretaría de Gobierno Digital de la Presidencia del Consejo de ministros, la cual lidera los procesos de innovación tecnológica y de transformación digital del Estado. Es el ente rector del Sistema Nacional de Transformación Digital y administra las Plataformas Digitales del Estado Peruano.

Existen casos particulares sobre delitos informáticos en Perú, tal es el caso de la Sentencia del Tribunal Constitucional del Perú, del 21 de enero de 2004, Expediente Nº 1219-2003-HD/TC, caso Nuevo Mundo Holding S.A, referente al Recurso extraordinario interpuesto por Nuevo Mundo Holding S.A. (NMH) contra la resolución de la Tercera Sala Civil de la Corte Superior de Justicia de Lima, de fojas 597, su fecha 23 de enero del 2003, que declaró infundada la acción de hábeas data de autos. También en el Perú se emitió la Ley N° 29733 "Ley de Protección de Datos Personales" el día 03 de julio del 2011, con el cual se protegen los datos personales en los servicios informáticos.

1.3 Investigaciones relativas al objeto de estudio:

A continuación, se muestran las principales investigaciones relativas al objeto de estudio:

En primer lugar, se hará mención al antecedente **"La admisibilidad y el valor probatorio de la evidencia digital en el Sistema Jurídico Peruano 2018"** presentado el año 2019 para optar el grado académico de Maestro en Derecho Penal y Procesal Penal ante la Universidad César Vallejo por Miguel Osco.

El estudio tuvo como objetivo conocer y establecer los procedimientos en la investigación, manejo y traslado de la evidencia digital, dentro de la actividad probatoria que se fundamente, por un lado, teniendo en cuenta lo establecido por la ley, y por otro los procedimientos técnicos mediante el empleo de herramientas tecnológicas. El método empleado fue deductivo, el tipo de investigación fue básica, de nivel descriptivo, de enfoque cualitativo, de diseño no experimental. La población estuvo formada por fiscal representante

del Ministerio Publico, personal PNP especialista en delitos de alta tecnología representante de la Policía Nacional del Perú, y un experto de tecnologías en delitos financieros del sistema bancario. La técnica empleada para recolectar información fue la observación, entrevista, análisis documental y los instrumentos de recolección de datos fueron, cuestionarios, guía de observación, guía de entrevista. Se llegaron a las siguientes conclusiones: La prueba digital no solo es insuficiente, sino, no cuenta con un tratamiento especial en el Nuevo Código Procesal Penal del 2004, así como los operadores de justicia jueces, fiscales, abogados litigantes y el personal de la Policía Nacional no están capacitados en el manejo de procedimientos de hallazgo, recojo, tratamiento y traslado de las evidencias digitales (Osco, 2019).

Luego, se citará la investigación relacionada **"Aplicación de metodologías y herramientas de la informática forense para reducir el riesgo de la seguridad informática en la Dirección Nacional de Comunicación y Criminalística de la Policía Nacional Del Perú – Huaraz – 2015"** presentada el año 2017 para optar el grado de Maestro en Ciencias e Ingeniería ante la Universidad Nacional Santiago Antunez de Mayolo por Frans De la Cruz.

La investigación tuvo como objetivo aplicar metodologías y herramientas de la informática forense para lograr reducir la inseguridad informática tomando como lugar de aplicación la Dirección Nacional de Comunicación y Criminalística de la Policía Nacional del Perú – Huaraz. Investigación aplicada, descriptivo, de diseño no experimental transversal , la población de estudio para el trabajo de investigación estuvo comprendida por los trabajadores de la Dirección Nacional de Comunicaciones y Criminalística de la Policía Nacional del Perú, con una muestra de 45 trabajadores , el instrumento que se utilizó para la recolección de la información fue el cuestionario, la información se procesó mediante el programa SPSS V19, para el análisis de datos se utilizó el análisis estadístico, a través de la estadística descriptiva. El resultado de la investigación forense está relacionado con la seguridad informática en la Dirección Nacional de Comunicación y Criminalística de la PNP, los conocimientos de

metodologías y herramientas de la informática forense tienen una relación directa con la seguridad informática en un 89%. Se concluye ue el nivel de preparación para la informática forense y sus capacidades en el departamento de Dirección Nacional de Comunicación y Criminalística de la Policía Nacional del Perú en Huaraz es bajo tan solo representa un 20% que el personal no está capacitado para afrontar temas forenses (De la cruz, 2017).

Posteriormente, se mencionará el antecedente titulado **"Peritaje informático basado en una nueva metodología híbrida en 2M & J Ingenieros – Huaraz 2019"** presentado el año 2020 para optar el grado académico de Maestro en Gestión Tecnológica de la Información ante la Universidad Peruana de Ciencias e Informática por Cristhian Cacha.

El estudio tuvo como objetivo demostrar cual es el efecto de la informática forense basado en una nueva metodología híbrida en el Peritaje Informático en la Empresa 2M&J Ingenieros, 2019. Es una investigación aplicada, con diseño experimental, de manera específica, diseño preexperimental, en una muestra censal de 15 computadoras. Se aplicó la prueba del pretest al grupo único y, obtenidos los resultados se realizó la aplicación de la nueva metodología en actividades, para volver a ser evaluada en la fase de postest. En el tratamiento estadístico se utilizó el software SPSS 25. La descripción de los resultados se hizo desde una mirada descriptiva (Figuras y gráficas de barras) mientras en la parte inferencial se utilizó en el contraste de hipótesis la prueba no paramétrica de rangos con signos de Wilcoxon que se utiliza para muestras relacionadas. El resultado hallado demostró el efecto de la informática forense con la aplicación de una nueva metodología en la mejora del peritaje informático en la Empresa 2M&J INGENIEROS, 2019, al obtener un valor $Z = -3.425 < -1.96$ (95%), por lo que se evidencia diferencias significativas en el contraste de hipótesis en la fase de pretest y postest, al obtenerse un valor $p = 0\ .001 < 0.05$ (Cacha, 2020).

Por otra parte, se encuentra la investigación relacionada **"Diseño de una metodología de recolección de evidencia digital para análisis forense de unidades de disco duro, basada en la norma ISO/IEC 27037:2012"** presentada el año 2019 para optar el grado académico de Magister en Tecnologías de la Información ante la Universidad Internacional SEK, Ecuador por David Rosero.

La investigación tuvo como objetivo diseñar y difundir una metodología para manejo de evidencia digital contenida en unidades de almacenamiento, con énfasis en discos duros, basado en la Norma ISO/IEC 27037:2012, debido a que actualmente en Ecuador no se ha evidenciado un procedimiento normado o estandarizado para realizar actividades de manejo de evidencia digital por parte de los peritos informáticos calificados en el Consejo de la Judicatura, es por eso que se plantea una metodología orientada a la actuación pericial, dirigida a dispositivos actuales, con la cual se pretende mejorar la calidad de evidencia digital. Este trabajo inicia con el análisis de las metodologías de extracción de evidencia digital de discos duros en Argentina, España y Colombia. La metodología que se propone se basa en la Norma ISO/IEC 27037:2012 y en investigaciones provenientes de los países mencionados consta de seis fases que incluyen la ubicación, aseguramiento de la escena de los hechos, la identificación, recolección, preservación y análisis de la evidencia digital. Finalmente, se realiza una difusión a nivel nacional de la metodología a los peritos informáticos calificados en el Consejo de la Judicatura se tomó dos muestras de peritos informáticos, la primera para conocer los medios y herramientas que se utiliza actualmente en el manejo de evidencia digital, y la segunda muestra para la difusión de la metodología propuesta. Los resultados mediante un juicio de experto indican que la aplicación de la misma tiene ventajas competitivas respecto a otras metodologías; en otros resultados se muestra que la utilización de la metodología ayuda en la mejora de la calidad de evidencia digital para ser admitida en un proceso judicial por el hecho que cumple con los principios de relevancia, la confiabilidad y la suficiencia (Rosero, 2019).

A continuación, se hará referencia al antecedente **"Metodología de análisis forense informático para la obtención de evidencia digital en Base de Datos"** presentado el año 2019 para optar el grado académico de Maestra en Informática ante la Universidad Nacional de la Matanza, Argentina por Cintia Gioia.

El estudio tuvo como objetivo plantear el desafío de obtener evidencia digital válida como medio de prueba para su efectiva sanción dentro de un proceso judicial. Prevenir los riesgos de invalidar una prueba se convierte en una responsabilidad y un reto profesional. En este trabajo se propone una metodología forense específica para base de datos relacionales basada en una metodología forense informática general que guía, unifica y garantiza la confiabilidad de las actividades que realiza el perito informático centradas en la obtención y el análisis de evidencia digital. Asimismo, se plantea la obtención de evidencia digital a partir de la configuración y ejecución de auditorías de datos universales aplicables a cualquier motor de base de datos. La metodología planteada sobrepasa las limitaciones o retos tecnológicos individuales de cada tipo de base de datos y la dependencia de expertos en dichas tecnologías que ofrecen soluciones según su visión tecnócrata, en ocasiones incluso, sin garantizar la admisibilidad judicial de la evidencia digital (Gioia, 2019).

Por último, se presentará la investigación relacionada **"La recolección y custodia de las evidencias digitales del auditor forense en entidades financieras"** presentada el año 2019 para optar el grado académico de Maestro en Auditoría Forense ante la Universidad Mayor de San Andrés, Bolivia por Denys Buitrago.

La investigación tuvo como objetivo establecer la contaminación de las citadas evidencias digitales. La justificación del tema es el establecer los procedimientos correctos que deben tener en cuenta los Auditores Forenses en la recolección de la evidencia digital para que no se encuentren contaminadas y no sean pruebas ilegales. Se ingresa al marco teórico, la cual da una definición de que es la prueba, en este sentido es toda aquella documentación, declaración, pericia que da fe de un hecho acontecido. De las mismas formas

se realiza da un concepto de evidencia que es una certeza clara de un objeto o acto. Posteriormente se realiza una descripción de los principios de la prueba, la diferencia entre prueba y evidencia digital, la custodia de la evidencia, en este punto cabe aclarar que se tomó el procedimiento establecido en el Código de Procedimiento Penal, que cuando se comete un hecho delictivo el encargado de recolectar las pruebas en el marco de la legislación vigente es el Investigador de la Policía Boliviana. Se realiza una descripción de la prueba digital en Bolivia, donde no se establece un procedimiento específico para recolectar, debiendo ser tomada como una pericia la cual debe ser solicitada al Ministerio Público para que sea realizado por un personal especializado en la materia, existiendo también en el Código de Procedimiento Penal una contradicción entre la libertad probatoria y los medios de prueba descritos. Se toma en cuenta también la legislación comparada de Venezuela, Argentina, Chile y Colombia, este último país cuenta con una legislación muy avanzada en la recolección, custodia y valoración de las pruebas digitales dentro de los procesos penales (Buitrago, 2019).

1.4 Marco Conceptual

Base de datos

Conjunto completo de ficheros informáticos que reúnen informaciones generales o temáticas, que generalmente están a disposición de numerosos usuarios.

Delito informático

Julio Téllez Valdez (2007) en su libro derecho informático, enfoca el delito informático desde el punto de vista típico y atípico y lo define como “actitud contraria a los intereses de las personas en que se tiene a los computadores como instrumento o fin (concepto atípico) o las conductas típicas, antijurídica o culpables en las que se tienen los computadores como instrumento o fin (Ojeda Pérez, Rincón Rodríguez, Arias Flórez, & Daza Martínez, 2010).

Evidencia digital

Es un registro de la información guardada o difundida a través de un sistema informático que puede utilizarse como prueba en un proceso judicial. Es cualquier dato digital que pueda relacionar un delito con su víctima o con su autor

Informática forense

Aplicación de la ciencia para la identificación, recolección, examen y análisis de los datos, preservando correctamente su integridad, llevando a cabo a su vez una estricta cadena de custodia de la información.

Red social en internet

Las rede sociales son sitios web que ofrecen servicios y funcionalidades de comunicación diversos para mantener en contacto a los usuarios de la red. Se basan en un software especial que integra numerosas funciones individuales: blogs, wikis, foros, chat, mensajería, entre otros, en una misma interfaz y que proporciona la conectividad entre los diversos usuarios de la red.

Redes temáticas

Son similares a las anteriores, aunque se diferencian por el hecho de que suelen centrarse en un tema en concreto y proporcionan las funcionalidades necesarias para el mismo. Por ejemplo, una red de cine, una de informática, de algún tipo de deporte, etc.

Redes profesionales

Son una variedad especial de las anteriores, dedicadas exclusivamente al ámbito laboral, en todas sus vertientes. Pueden poner en contacto a aquellos que ofrecen trabajo con los que lo buscan, crear grupos de investigación, entre otros.

Mensaje de datos: Es toda aquella información visualizada, generada enviada, recibida, almacenada o comunicada por medios informáticos, electrónicos, ópticos, digitales o similares.

Sabotaje informático

El término sabotaje informático comprende todas aquellas conductas dirigidas a causar daños en el hardware o en el software de un sistema. (López Hernández, 2011).

Seguridad contra los delitos informáticos

La seguridad cibernética consiste en fomentar la confianza y la seguridad en el uso de las TIC para garantizar la confianza en la sociedad de la información. En consecuencia, podemos definirlo como todas las actividades y operaciones encaminadas a reducir y prevenir amenazas y vulnerabilidades, y tener políticas de protección;respuesta al incidente; Recuperación, aseguramiento de datos, aplicación de la ley y operaciones militares y de inteligencia relacionadas con la seguridad del espacio cibernético. (Mona Al-achkar Jabbour, 2016).

Sistema informático

Conjunto organizado de programas y bases de datos que se utilizan para, generar, almacenar, tratar de forma automatizada datos o información cualquiera que esta sea.

Soporte lógico

Cualquiera de los elementos (tarjetas perforadas, cintas o discos magnéticos, discos ópticos) que pueden ser empleados para registrar información en un sistema informático.

Soporte material: Es cualquier elemento corporal que se utilice para registrar toda clase de información.

1.5 Marco Legal

Error Judicial Inexcusable

Torres (2018) menciona que el Código Procesal Civil peruano, vigente desde el 28 de julio de 1993, establece en su artículo 509: “El Juez es civilmente responsable cuando en ejercicio de su función jurisdiccional causa daño a las partes o a terceros, al actuar con dolo o culpa inexcusable”.

Igualmente, este cuerpo legal determina en su artículo 516 la existencia de responsabilidad solidaria entre el Estado y el juez para el pago de los daños y perjuicios que pudieran resultar del actuar judicial.

De esta manera, el autor argumenta que se entiende que el litigante puede demandar civilmente al juez el pago de una indemnización sólo en caso haya sido perjudicado por dolo o culpa inexcusable en un proceso judicial. Al mismo tiempo, de resultar vencedor en el mencionado proceso civil, el litigante puede cobrar tal monto económico al juez o al estado de forma solidaria.

Torres sostiene que se debe considerar que este proceso civil es más restringido de lo que aparenta ya que el dolo y la culpa inexcusable esbozados se encuentran restringidos por el propio artículo 509 del C.P.C. de la siguiente forma:

"Dolo: i) falsedad, ii) fraude, o iii) si deniega justicia al rehusar u omitir un acto o realizar otro por influencia.

Culpa inexcusable: i) grave error de derecho, ii) interpretación insustentable de la ley o iii) causar indefensión al no analizar los hechos probados por el afectado".

Además, el autor asegura que existe una presunción de dolo o culpa inexcusable establecida en el artículo 510 del Código Procesal Civil. No obstante, se considera que esta también tiene una estricta aplicación. El mencionado artículo determina que:

"Cuando la resolución contraría el criterio del juez sustentado anteriormente en causa similar, salvo que motive los fundamentos del cambio.

Cuando el juez resuelve en discrepancia con la opinión del Ministerio Público o en discordia, según sea el caso, en temas sobre los que existe jurisprudencia obligatoria o uniforme, o en base a fundamentos insostenibles".

Responsabilidad de los Jueces

Torres considera que el proceso de responsabilidad civil de los jueces está se encuentra restringido a lo señalado precedentemente. En consecuencia, si un litigante resulta perjudicado

por una actuación judicial que, según las normas legales señaladas anteriormente, no califica o se presume como dolo o culpa inexcusable, queda impedido de activar válidamente un proceso de responsabilidad civil de los jueces, y, de esta manera, obtener indemnización por esta vía.

Por otra parte, en el marco de la responsabilidad civil del Estado por errores en actos judiciales, el autor destaca que la Constitución Política de 1993 del Estado peruano, ha definido el derecho de ser indemnizado por el error judicial a cargo del Estado en el artículo 139.7. No obstante, tal prerrogativa está circunscrita, al menos a primera vista, a las detenciones arbitrarias.

Torres enfatiza que aquel derecho constitucional ha adquirido el carácter de convencional al amparo del artículo 10 de la Convención Americana sobre Derechos Humanos de 1969, que precisa: "Toda persona tiene derecho a ser indemnizada conforme a la ley en caso de haber sido condenada en sentencia firme por error judicial".

De acuerdo con el autor, este derecho se encuentra delimitado por la Ley 24973 del 28 de diciembre de 1988, que indica en sus artículos 2 y 3 que los acreedores a este derecho son:

"Quienes han sido detenidos por causa injustificada, o que, existiendo esta, se exceden los límites fijados por la Constitución, especialmente cuando el detenido no es puesto a disposición del juez.

Quienes hayan sido condenados de forma errónea o arbitraria, siempre que así lo acredite el juicio de revisión realizado por la Corte Suprema.

Quienes hayan sido sometidos a prisión preventiva y obtienen posteriormente auto de archivo definitivo o absolución".

Asimismo, el autor refiere que el Tribunal Constitucional peruano estableció en 1999 que los beneficiarios de un indulto especial pueden pretender también una indemnización por parte del estado ya que este tipo de perdón presidencial constituye una forma de reconocimiento de error judicial. Esta situación implica la existencia de una detención arbitraria.

En ese sentido, Torres ratifica que una persona tiene derecho a ser indemnizada por el estado peruano cuando es detenida de forma ilegal o arbitraria. Además, independientemente de la existencia de dolo, culpa inexcusable o cualquier otro factor de atribución de responsabilidad.

En palabras del autor, según el ordenamiento jurídico actual se concluye que la indemnización de un litigante por la actuación judicial indebida la efectúa:

"El Estado y el juez de forma solidaria, cuando la conducta judicial califica o se presume como dolo o culpa inexcusable a la luz de los artículos 509 y 510 del C.P.C.

El Estado, cuando la persona es detenida ilegal o arbitrariamente, con independencia de la existencia de dolo o culpa".

Por otra parte, en caso un litigante se vea perjudicado por un acto judicial que no califique dentro de los parámetros anteriores, será impedido de demandar válidamente una indemnización (Torres, 2018).

CAPITULO II. EL PROBLEMA, OBJETIVOS, HIPÓTESIS Y VARIABLES

2.1 Planteamiento del problema

2.1.1 Descripción de la realidad problemática.

Fernández (2012) señala que el problema de investigación es lo que surge durante la observación en un determinado ambiente, no necesariamente un quehacer profesional. Por lo tanto, un problema es un vacío del conocimiento que se busca entender durante el transcurso de la investigación. (p.11).

Actualmente, en la esfera de la "informática y de las telecomunicaciones", la "tecnología de la información y comunicación" ha avanzado y desarrollado grandes transformaciones experimentales; la información sea almacenada, tratada o transmitida en forma ilícita por medio de los sistemas informáticos estarían atentando contra los derechos fundamentales; razón por el cual se ha promulgado la "Ley Nº 30096 - Ley de Delitos Informáticos, modificada por la Ley Nº 30171", entre los cuales se encuentran los siguientes "Delitos Informáticos": "delitos contra datos y sistemas informáticos, contra la indemnidad y libertad sexual, contra la intimidad y el secreto de las comunicaciones, contra el patrimonio, contra la fe pública".

Nos encontramos frente a una realidad en las investigaciones penales que nos enfrenta con la utilización de las nuevas tecnologías por parte de los delincuentes, circunstancia que requiere de un conocimiento profundizado de los investigadores y del personal policial actuante de estos mecanismos innovadores.

La obtención de información, como elementos de prueba para el éxito de una investigación criminal, exige de los investigadores encargados de la recolección, preservación,

análisis y presentación de la evidencia digital, una labor impecable que garantice su autenticidad e integridad, a fin de ser presentada por el fiscal en el juicio oral.

Es fundamental afianzar la relación entre policías y fiscales a fin de elaborar y coordinar, con dirección del fiscal, una estrategia de investigación en la que se discutan y optimicen los mecanismos de recolección de evidencia digital, las herramientas a utilizarse, con el objetivo que el pormenorizado trabajo realizado por los investigadores adquiera una legitimidad absoluta que, a la luz del procedimiento penal, pueda ser presentada ante el juez, en el juicio oral, con la solidez que ello requiere.

Es en base a esta realidad problemática, es que la presente investigación pretende determinar la influencia de la Evidencia Digital en los Delitos de Fraude Informático tipificado en el Código Procesal Penal Peruano.

2.1.2 Definición del problema: General y Específicos.

2.1.2.1 Problema General

¿En qué medida influye la Evidencia Digital y los Delitos de Fraude Informático tipificado en el Código Procesal Penal Peruano?

2.1.2.2 Problemas Específicos (PE).

PE1. ¿En qué medida influye el nivel de Autenticidad de la Evidencia Digital en los Delitos de Fraude Informático tipificado en el Código Procesal Penal Peruano?

PE2. ¿En qué medida influye el nivel de Confiabilidad de la Evidencia Digital en los Delitos de Fraude Informático tipificado en el Código Procesal Penal Peruano?

PE3. ¿En qué medida influye el nivel de Completitud o Suficiencia de la Evidencia Digital en los Delitos de Fraude Informático tipificado en el Código Procesal Penal Peruano?

PE4. ¿En qué medida influye el nivel de Conocimiento de las Leyes de la Evidencia Digital en los Delitos de Fraude Informático tipificado en el Código Procesal Penal Peruano?

PE5. ¿En qué medida influye el nivel de Cumplimiento de las Leyes de la Evidencia Digital en los Delitos de Fraude Informático tipificado en el Código Procesal Penal Peruano?

2.2 Finalidad y objetivos de la investigación

2.2.1 Finalidad

El trabajo de investigación tiene como finalidad determinar la influencia de la Evidencia Digital en los Delitos de Fraude Informático tipificado en el Código Procesal Penal Peruano.

Es importante porque los resultados permitirán identificar las principales debilidades de los delitos de fraudes informáticos, de esta manera se propondrán alternativas de solución y estrategias para que mejore la seguridad informática y se hagan cumplir las leyes de código procesal penal peruano.

2.2.2 Objetivo General y Específicos

2.2.2.1 Objetivo General

Determinar la influencia de la Evidencia Digital en los Delitos de Fraude Informático tipificado en el Código Procesal Penal Peruano.

2.2.2.2 Objetivos Específicos

OE1. Determinar la influencia del nivel de Autenticidad de la Evidencia Digital en los Delitos de Fraude Informático tipificado en el Código Procesal Penal Peruano.

OE2. Determinar la influencia del nivel de Confiabilidad de la Evidencia Digital en los Delitos de Fraude Informático tipificado en el Código Procesal Penal Peruano.

OE_3. Determinar la influencia del nivel de Completitud o Suficiencia de la Evidencia Digital en los Delitos de Fraude Informático tipificado en el Código Procesal Penal Peruano.

OE_4. Determinar la influencia del nivel de Conocimiento de las Leyes de la Evidencia Digital en los Delitos de Fraude Informático tipificado en el Código Procesal Penal Peruano.

OE_5. Determinar la influencia del nivel de Cumplimiento de las Leyes de la Evidencia Digital en los Delitos de Fraude Informático tipificado en el Código Procesal Penal Peruano.

2.2.3 Delimitación del estudio.

La presente investigación con fines metodológicos tiene delimitados los siguientes aspectos:

Delimitación espacial. La investigación se desarrolló en los ambientes de los juzgados del distrito Independencia.

Delimitación temporal. El período que abarcó el presente estudio fue de enero a diciembre del año 2020.

Delimitación social. Se trabajó a nivel de las personas que han sido víctima de fraude informático en el distrito de Independencia, así como con los operadores de justicia del mencionado distrito judicial.

2.2.4 Justificación e importancia del estudio.

El desarrollo de la investigación estará encaminado a tratar de determinar la influencia de la Evidencia Digital en los Delitos de Fraude Informático tipificado en el Código Procesal Penal Peruano.

La investigación brindará aportes importantes que permitirán adoptar políticas y/o acciones encaminadas a mejorar las condiciones de seguridad informática, así como entender los derechos de los ciudadanos frente a cualquier fraude informático.

2.3 Hipótesis y variables

2.3.1 Supuestos teóricos.

En la actualidad, la informática (tecnología de la información) es uno de los instrumentos más utilizado en las actividades cotidianas que realiza el hombre; no obstante, este instrumento viene siendo utilizado en forma incorrecta motivo por el cual tiende a afectar ciertos derechos fundamentales.

Esta situación ha motivado en todo el planeta a realizar investigaciones al respecto y regular este tipo de conductas, todo esto con la finalidad de proteger derechos fundamentales.

Al respecto, algunas de las investigaciones que analizaron el tema en comento fueron: "Derecho Penal y Derecho de las Nuevas Tecnologías de la Información y Comunicación: Criminalidad Asociada a las Telecomunicaciones" (Guerra, 2011); "El Derecho a la Intimidad, la visión de la informática y el delito de los datos personales" (Riascos, 1999); "Derecho a la Intimidad en la estructura de la ley especial de intervención de telecomunicaciones" (Amaya, Avalos, y Jule 2012); "El derecho fundamental a la protección de datos personales en México: Análisis desde la influencia del ordenamiento jurídico español" (Guzmán, 2013); "La protección de datos personales en España: Evolución normativa y criterios de aplicación" (Zaballos, 2013).

Estas investigaciones demuestran que la tecnología de la información es de gran utilidad e influye sustancialmente en el desarrollo de las sociedades actuales, pero también la incorrecta utilización afecta derechos fundamentales, por tanto, es necesario estar atento con la finalidad de proteger dichos derechos fundamentales.

Si bien es cierto las tecnologías actualmente es de suma importancia para el desarrollo de las sociedades, también es importante la protección de los derechos fundamentales, esto

con la finalidad de convivir en bienestar y paz social; es en razón a ello que la "Organización para la Cooperación y Desarrollo Económico" (OCDE), y los estados vienen realizando denodados esfuerzos, con la finalidad de proteger la información contenida en sistemas informáticos, información que contiene datos (íntimos, privados o reservados) de suma importancia para las personas naturales o jurídicas.

Por tal motivo, se ha planteado las siguientes hipótesis que se muestran a continuación:

2.3.2 Hipótesis, principal y específicas.

2.3.2.1 Hipótesis principal (HP).

La Evidencia Digital influye significativamente en los Delitos de Fraude Informático tipificado en el Código Procesal Penal Peruano.

2.3.2.2 Hipótesis específicas (HE).

HE$_1$. El nivel de Autenticidad de La Evidencia Digital influye significativamente en los Delitos de Fraude Informático tipificado en el Código Procesal Penal Peruano.

HE$_2$. El nivel de Confiabilidad de La Evidencia Digital influye significativamente en los Delitos de Fraude Informático tipificado en el Código Procesal Penal Peruano.

HE$_3$. El nivel de Completitud o Suficiencia de La Evidencia Digital influye significativamente en los Delitos de Fraude Informático tipificado en el Código Procesal Penal Peruano.

HE$_4$. El nivel de Conocimiento de las Leyes de La Evidencia Digital influye significativamente en los Delitos de Fraude Informático tipificado en el Código Procesal Penal Peruano.

HE$_5$. El nivel de Cumplimiento de las Leyes de La Evidencia Digital influye significativamente en los Delitos de Fraude Informático tipificado en el Código Procesal Penal Peruano.

2.3.3 Variables e indicadores.

2.3.3.1 Variables

VI. (X) Evidencia Digital. (variable independiente)

VD. (Y) Delitos de Fraude Informático. (variable dependiente)

2.3.3.2 Operacionalización de las variables

Cuadro 1

Variables e Indicadores

VARIABLE	INDICADORES
Evidencia Digital (X) (variable independiente)	• X_1: Nivel de autenticidad. • X_2: Nivel de confiabilidad. • X_3: Nivel de completitud o suficiencia. • X_4: Nivel de conocimiento de las leyes. • X_5: Nivel de cumplimiento de las leyes.
Delitos de Fraude Informático (Y) (variable dependiente)	• Y_1: Nivel de seguridad informática. • Y_2: Política de uso de la información. • Y_3: Derecho a la Propiedad intelectual. • Y_4: Nivel de acceso a material inadecuado. • Y_5: Nivel de plagio y sus modalidades.

Fuente: Autor de la tesis (2021)

CAPITULO III. MÉTODOS, TÉCNICAS E INSTRUMENTOS

3.1 Población y muestra

3.1.1 Población.

El distrito de Independencia alberga 8 salas superiores (4 penales permanentes, 2 penales transitorias y 2 civiles), 7 juzgados civiles, 7 juzgados de familia, 1 juzgado laboral y 14 juzgados penales.

La población de operadores de justicia asciende aproximadamente a 200 personas.

3.1.2 Muestra

Para determinar la muestra óptima a investigar se utilizó la siguiente fórmula, representada por el estadístico:

$$n = \frac{N * Z_{\alpha}^{2} p * q}{d^{2} * (N-1) + Z_{\alpha}^{2} * p * q}$$

dónde:

- p : probabilidad de éxito representada por el 50% (0.5) encuesta (Se asume p = 50%)
- q : Proporción de fracaso (Se asume 1-p = 50%)
- d : Margen de error 5% seleccionado por el investigador
- N : Población (200)
- n= Tamaño de la muestra
- Z= Distribución Estándar (1.96 con un N.C 95%)

n = 132

3.2 Tipo, Nivel, Método y Diseño de Investigación

3.2.1 Tipo de investigación.

El tipo fue el Explicativo.

3.2.2 Nivel de Investigación.

El nivel de la investigación fue el aplicado

3.2.3 Método y Diseño.

3.2.3.1 Método.

El método utilizado fue el Ex Post Facto

3.2.3.2 Diseño.

El diseño fue correlacional. Se tomó una muestra en la cual

$$\mathbf{M = Oy\ (f)\ Ox_1}$$

Donde:

M = Muestra.

O = Observación.

f = En función de.

X_1 = Evidencia digital.

Y_1 = Delitos de Fraude Informático.

3.3 Técnica (s) e instrumento (s) de recolección de datos

3.3.1 Técnicas.

La principal técnica que se utilizó en el presente estudio fue la encuesta.

3.3.2 Instrumentos.

Como instrumento de recolección de datos se utilizó el cuestionario que, por intermedio de una encuesta de preguntas, en su modalidad cerradas, se tomarán a la muestra señalada.

3.4 Procesamiento de datos

La fiabilidad del instrumento dirigido a los 132 operadores de justicia de la Corte Superior de Justicia de Lima Norte es considerada como consistencia interna de la prueba, alfa de Cronbach (α=0,828) la cual es considerada como buena (según Hernández Sampieri, 2005).

Esta confiabilidad se ha determinado en relación con los 20 ítems centrales de la encuesta, lo cual quiere decir que la encuesta realizada ha sido confiable, válida y aplicable. El cuadro 2 muestra los resultados del coeficiente de confiabilidad alfa de Cronbach.

3.4.1 Confiabilidad del Instrumento.

Cuadro 2

Estadístico de Fiabilidad Sobre el Instrumento

Resumen del proceso			
		N	**%**
Casos	Validados	132	100,0
	Excluidos	0	0
	Total	**132**	**100,0**

Resultado Estadístico	
Alfa de Cronbach	N° de elementos
0,828	20

CAPITULO IV. PRESENTACIÓN Y ANÁLISIS DE LOS RESULTADOS

4.1 Presentación de resultados

A continuación, se muestran los resultados de la encuesta realizada a 132 operadores de justicia de la Corte Superior de Justicia de Lima Norte - diciembre 2020.

La misma tiene por finalidad determinar la influencia de la Evidencia Digital en los Delitos de Fraude Informático tipificado en el Código Procesal Penal Peruano.

Tabla 1

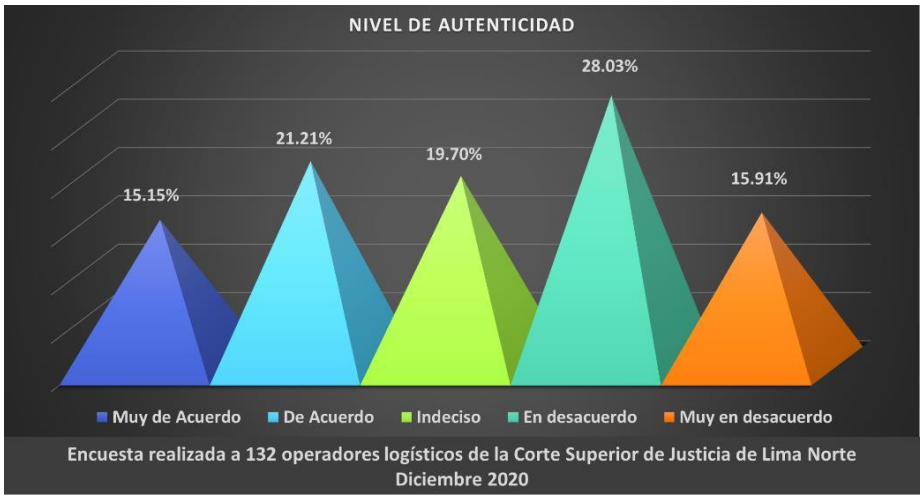
Nivel de Autenticidad

Respuestas	Cantidad	Porcentaje
Muy de Acuerdo	20	15.15%
De Acuerdo	28	21.21%
Indeciso	26	19.70%
En desacuerdo	37	28.03%
Muy en desacuerdo	21	15.91%
N° de Respuestas	**132**	**100.00%**

Encuesta realizada a 132 operadores de justicia de la Corte Superior de Justicia de Lima Norte - Diciembre 2020

Figura 1

Nivel de Autenticidad



Como se aprecia en la Tabla 1, muestran los principales resultados de la encuesta realizada a 132 operadores de justicia de la Corte Superior de Justicia de Lima Norte - Diciembre 2020, de los operadores de justicia encuestados manifiestan respecto a si considera que es adecuado el nivel de autenticidad en la evidencia digital en los delitos de fraude informático tipificado en el código procesal penal peruano; 37 operadores de justicia refieren que están en desacuerdo, lo que representa el 28.03%, 28 operadores de justicia que se encuentran de acuerdo, lo que representa el 21.21%, 26 operadores de justicia que están indecisos, lo que representa el 19.70%, 21 operadores de justicia que señalaron estar muy en desacuerdo, lo que representa el 15.91% y 20 operadores de justicia que indicaron que se encuentran muy de acuerdo, lo que representa el 15.15%.

Es decir, el 43.94% está en desacuerdo respecto a si considera que es adecuado el nivel de autenticidad en la evidencia digital en los delitos de fraude informático tipificado en el código procesal penal peruano.

Tabla 2

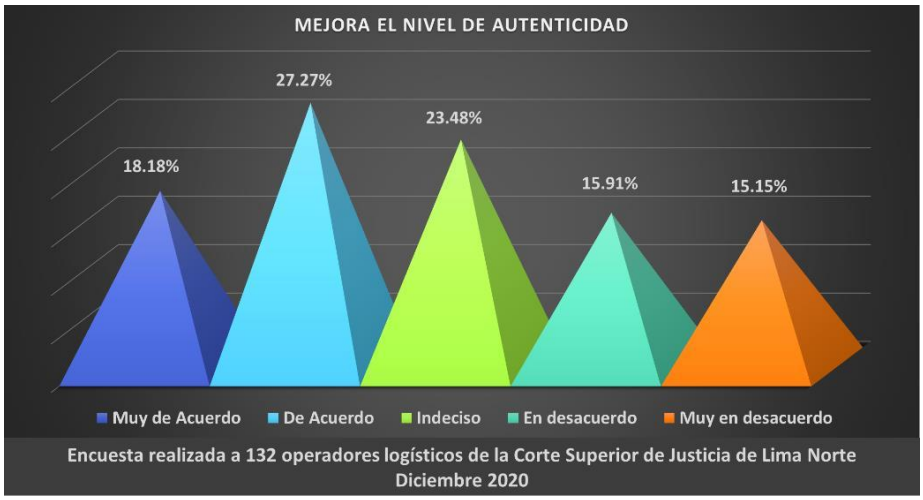
Mejora el Nivel de Autenticidad

Respuestas	Cantidad	Porcentaje
Muy de Acuerdo	24	18.18%
De Acuerdo	36	27.27%
Indeciso	31	23.48%
En desacuerdo	21	15.91%
Muy en desacuerdo	20	15.15%
N° de Respuestas	**132**	**100.00%**

Encuesta realizada a 132 operadores de justicia de la Corte Superior de Justicia de Lima Norte - Diciembre 2020

Figura 2

Mejora el Nivel de Autenticidad



Como se aprecia en la Tabla 2, muestran los principales resultados de la encuesta realizada a 132 operadores de justicia de la Corte Superior de Justicia de Lima Norte - Diciembre 2020, de los operadores de justicia encuestados manifiestan respecto a si considera que pude mejorar el nivel de autenticidad en la evidencia digital en los delitos de fraude informático tipificado en el código procesal penal peruano; 36 operadores de justicia que se encuentran de acuerdo, lo que representa el 27.27%, 31 operadores de justicia que están

indecisos, lo que representa el 23.48%, 24 operadores de justicia que indicaron que se encuentran muy de acuerdo, lo que representa el 18.18%, 21 operadores de justicia refieren que están en desacuerdo, lo que representa el 15.91% y 20 operadores de justicia que señalaron estar muy en desacuerdo, lo que representa el 15.15%.

Es decir, el 45.45% está de acuerdo respecto a si considera que pude mejorar el nivel de autenticidad en la evidencia digital en los delitos de fraude informático tipificado en el código procesal penal peruano.

Tabla 3

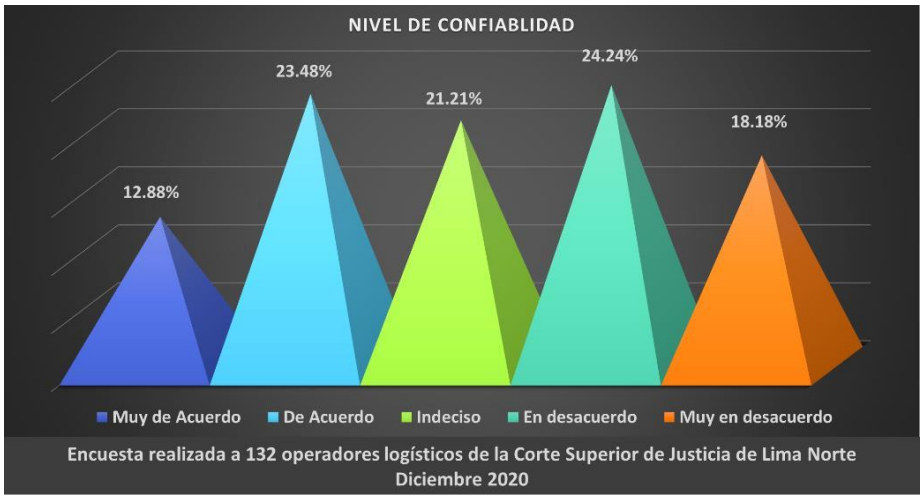
Nivel de Confiablidad

Respuestas	Cantidad	Porcentaje
Muy de Acuerdo	17	12.88%
De Acuerdo	31	23.48%
Indeciso	28	21.21%
En desacuerdo	32	24.24%
Muy en desacuerdo	24	18.18%
N° de Respuestas	**132**	**100.00%**

Encuesta realizada a 132 operadores de justicia de la Corte Superior de Justicia de Lima Norte - Diciembre 2020

Figura 3

Nivel de Confiablidad



Como se aprecia en la Tabla 3, muestran los principales resultados de la encuesta realizada a 132 operadores de justicia de la Corte Superior de Justicia de Lima Norte - Diciembre 2020, de los operadores de justicia encuestados manifiestan respecto a si considera que es adecuado el nivel de confiabilidad en la evidencia digital en los delitos de fraude informático tipificado en el código procesal penal peruano; 32 operadores de justicia refieren que están en desacuerdo, lo que representa el 24.24%, 31 operadores de justicia que se encuentran de acuerdo, lo que representa el 23.48%, 28 operadores de justicia que están indecisos, lo que representa el 21.21%, 24 operadores de justicia que señalaron estar muy en desacuerdo, lo que representa el 18.18% y 17 operadores de justicia que indicaron que se encuentran muy de acuerdo, lo que representa el 12.88%.

Es decir, el 42.42% está en desacuerdo respecto a si considera que es adecuado el nivel de confiabilidad en la evidencia digital en los delitos de fraude informático tipificado en el código procesal penal peruano.

Tabla 4

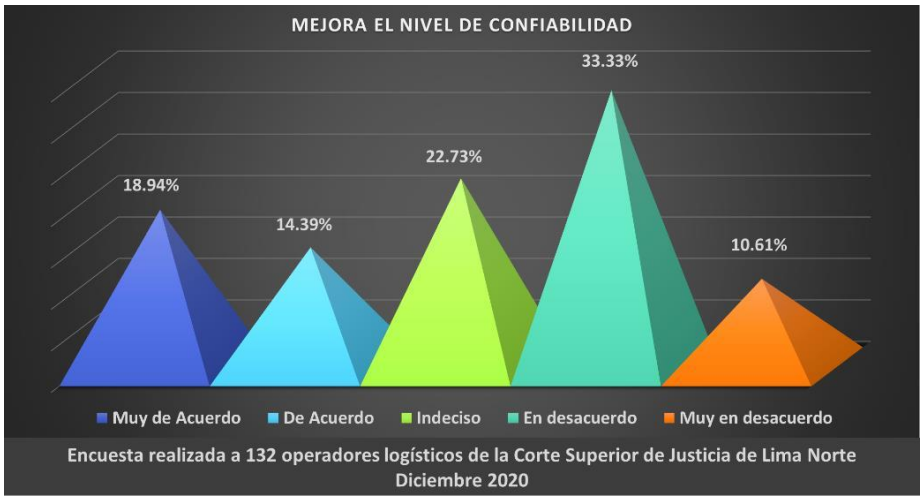
Mejora el Nivel de Confiabilidad

Respuestas	Cantidad	Porcentaje
Muy de Acuerdo	25	18.94%
De Acuerdo	19	14.39%
Indeciso	30	22.73%
En desacuerdo	44	33.33%
Muy en desacuerdo	14	10.61%
N° de Respuestas	**132**	**100.00%**

Encuesta realizada a 132 operadores de justicia de la Corte Superior de Justicia de Lima Norte - Diciembre 2020

Figura 4

Mejora el Nivel de Confiabilidad



Como se aprecia en la Tabla 4, muestran los principales resultados de la encuesta realizada a 132 operadores de justicia de la Corte Superior de Justicia de Lima Norte - Diciembre 2020, de los operadores de justicia encuestados manifiestan respecto a si considera que pude mejorar el nivel de confiabilidad en la evidencia digital en los delitos de fraude informático tipificado en el código procesal penal peruano; 44 operadores de justicia refieren que están en desacuerdo, lo que representa el 33.33%, 30 operadores de justicia que están

indecisos, lo que representa el 22.73%, 25 operadores de justicia que indicaron que se encuentran muy de acuerdo, lo que representa el 18.94%, 19 operadores de justicia que se encuentran de acuerdo, lo que representa el 14.39% y 14 operadores de justicia que señalaron estar muy en desacuerdo, lo que representa el 10.61%.

Es decir, el 43.94% está en desacuerdo respecto a si considera que pude mejorar el nivel de confiabilidad en la evidencia digital en los delitos de fraude informático tipificado en el código procesal penal peruano.

Tabla 5

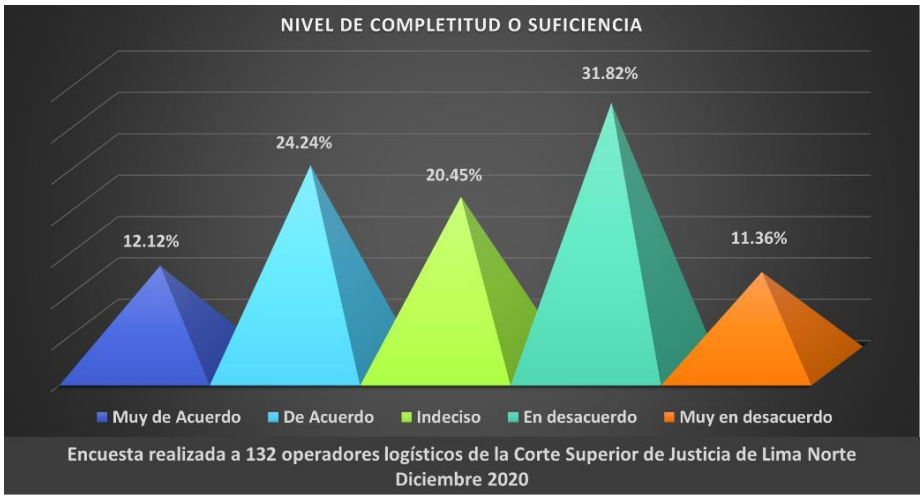
Nivel de Completitud o Suficiencia

Respuestas	Cantidad	Porcentaje
Muy de Acuerdo	16	12.12%
De Acuerdo	32	24.24%
Indeciso	27	20.45%
En desacuerdo	42	31.82%
Muy en desacuerdo	15	11.36%
N° de Respuestas	**132**	**100.00%**

Encuesta realizada a 132 operadores de justicia de la Corte Superior de Justicia de Lima Norte - Diciembre 2020

Figura 5

Nivel de Completitud o Suficiencia



Como se aprecia en la Tabla 5, muestran los principales resultados de la encuesta realizada a 132 operadores de justicia de la Corte Superior de Justicia de Lima Norte - Diciembre 2020, de los operadores de justicia encuestados manifiestan respecto a si considera que es adecuado el nivel de completitud o suficiencia en la evidencia digital en los delitos de fraude informático tipificado en el código procesal penal peruano; 42 operadores de justicia refieren que están en desacuerdo, lo que representa el 31.82%, 32 operadores de justicia que se encuentran de acuerdo, lo que representa el 24.24%, 27 operadores de justicia que están indecisos, lo que representa el 20.45%, 16 operadores de justicia que indicaron que se encuentran muy de acuerdo, lo que representa el 12.12% y 15 operadores de justicia que señalaron estar muy en desacuerdo, lo que representa el 11.36%.

Es decir, el 43.18% está en desacuerdo respecto a si considera que es adecuado el nivel de completitud o suficiencia en la evidencia digital en los delitos de fraude informático tipificado en el código procesal penal peruano.

Tabla 6

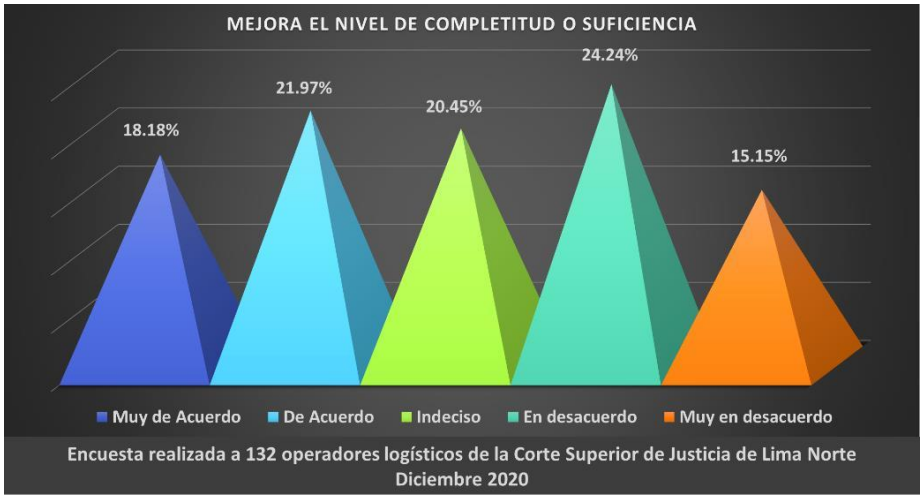
Mejora el Nivel de Completitud o Suficiencia

Respuestas	Cantidad	Porcentaje
Muy de Acuerdo	24	18.18%
De Acuerdo	29	21.97%
Indeciso	27	20.45%
En desacuerdo	32	24.24%
Muy en desacuerdo	20	15.15%
N° de Respuestas	**132**	**100.00%**

Encuesta realizada a 132 operadores de justicia de la Corte Superior de Justicia de Lima Norte - Diciembre 2020

Figura 6

Mejora el Nivel de Completitud o Suficiencia



Como se aprecia en la Tabla 6, muestran los principales resultados de la encuesta realizada a 132 operadores de justicia de la Corte Superior de Justicia de Lima Norte - Diciembre 2020, de los operadores de justicia encuestados manifiestan respecto a si considera que pude mejorar el nivel de completitud o suficiencia en la evidencia digital en los delitos de fraude informático tipificado en el código procesal penal peruano; 32 operadores de justicia refieren que están en desacuerdo, lo que representa el 24.24%, 29 operadores de justicia que se

encuentran de acuerdo, lo que representa el 21.97%, 27 operadores de justicia que están indecisos, lo que representa el 20.45%, 24 operadores de justicia que indicaron que se encuentran muy de acuerdo, lo que representa el 18.18% y 20 operadores de justicia que señalaron estar muy en desacuerdo, lo que representa el 15.15%.

Es decir, el 40.15% está de acuerdo respecto a si considera que pude mejorar el nivel de completitud o suficiencia en la evidencia digital en los delitos de fraude informático tipificado en el código procesal penal peruano.

Tabla 7

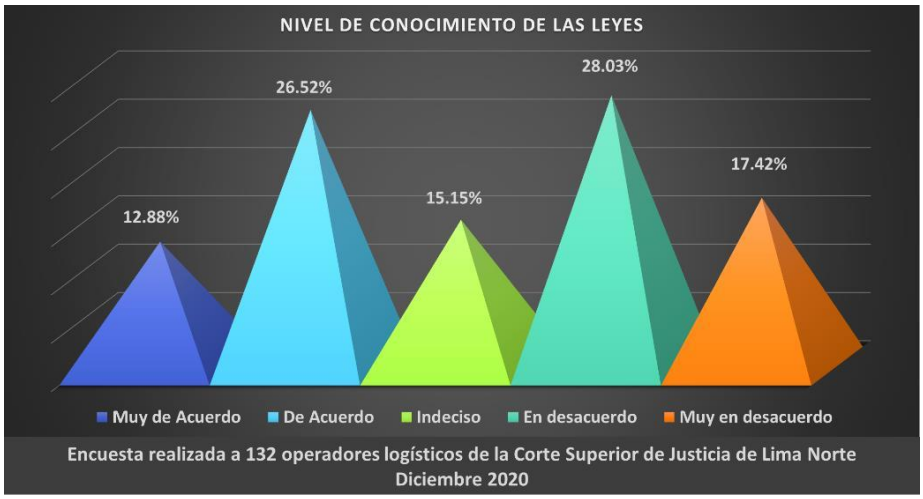
Nivel de Conocimiento de las Leyes

Respuestas	Cantidad	Porcentaje
Muy de Acuerdo	17	12.88%
De Acuerdo	35	26.52%
Indeciso	20	15.15%
En desacuerdo	37	28.03%
Muy en desacuerdo	23	17.42%
N° de Respuestas	**132**	**100.00%**

Encuesta realizada a 132 operadores de justicia de la Corte Superior de Justicia de Lima Norte - Diciembre 2020

Figura 7

Nivel de Conocimiento de las Leyes



Como se aprecia en la Tabla 7, muestran los principales resultados de la encuesta realizada a 132 operadores de justicia de la Corte Superior de Justicia de Lima Norte - Diciembre 2020, de los operadores de justicia encuestados manifiestan respecto a si considera que es adecuado el nivel de conocimiento de las leyes en los delitos de fraude informático tipificado en el código procesal penal peruano; 37 operadores de justicia refieren que están en desacuerdo, lo que representa el 28.03%, 35 operadores de justicia que se encuentran de acuerdo, lo que representa el 26.52%, 23 operadores de justicia que señalaron estar muy en desacuerdo, lo que representa el 17.42%, 20 operadores de justicia que están indecisos, lo que representa el 15.15% y 17 operadores de justicia que indicaron que se encuentran muy de acuerdo, lo que representa el 12.88%.

Es decir, el 45.45% está en desacuerdo respecto a si considera que es adecuado el nivel de conocimiento de las leyes en los delitos de fraude informático tipificado en el código procesal penal peruano.

Tabla 8

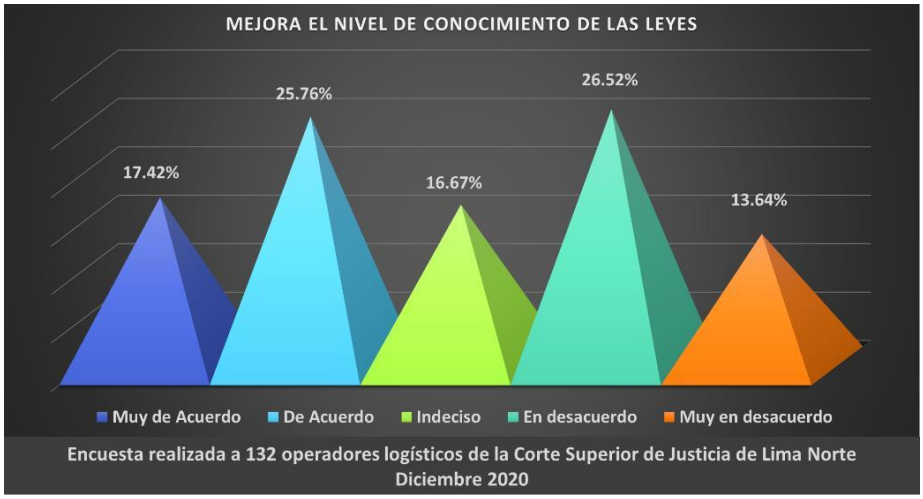
Mejora el Nivel de Conocimiento de las Leyes

Respuestas	Cantidad	Porcentaje
Muy de Acuerdo	23	17.42%
De Acuerdo	34	25.76%
Indeciso	22	16.67%
En desacuerdo	35	26.52%
Muy en desacuerdo	18	13.64%
N° de Respuestas	**132**	**100.00%**

Encuesta realizada a 132 operadores de justicia de la Corte Superior de Justicia de Lima Norte - Diciembre 2020

Figura 8

Mejora el Nivel de Conocimiento de las Leyes



Como se aprecia en la Tabla 8, muestran los principales resultados de la encuesta realizada a 132 operadores de justicia de la Corte Superior de Justicia de Lima Norte - Diciembre 2020, de los operadores de justicia encuestados manifiestan respecto a si considera que pude mejorar el nivel de conocimiento de las leyes en los delitos de fraude informático tipificado en el código procesal penal peruano; 35 operadores de justicia refieren que están en desacuerdo, lo que representa el 26.52%, 34 operadores de justicia que se encuentran de

acuerdo, lo que representa el 25.76%, 23 operadores de justicia que indicaron que se encuentran muy de acuerdo, lo que representa el 17.42%, 22 operadores de justicia que están indecisos, lo que representa el 16.67% y 18 operadores de justicia que señalaron estar muy en desacuerdo, lo que representa el 13.64%.

Es decir, el 43.18% está de acuerdo respecto a si considera que pude mejorar el nivel de conocimiento de las leyes en los delitos de fraude informático tipificado en el código procesal penal peruano.

Tabla 9

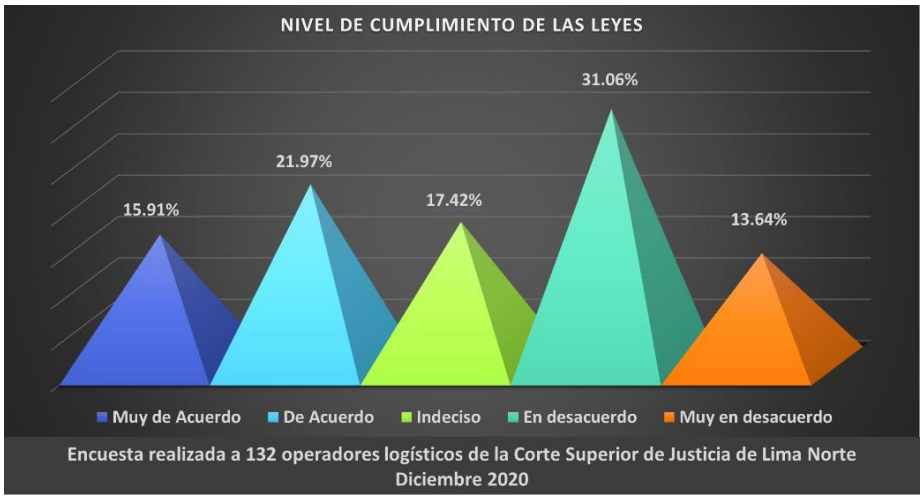
Nivel de Cumplimiento de las Leyes

Respuestas	Cantidad	Porcentaje
Muy de Acuerdo	21	15.91%
De Acuerdo	29	21.97%
Indeciso	23	17.42%
En desacuerdo	41	31.06%
Muy en desacuerdo	18	13.64%
N° de Respuestas	**132**	**100.00%**

Encuesta realizada a 132 operadores de justicia de la Corte Superior de Justicia de Lima Norte - Diciembre 2020

Figura 9

Nivel de Cumplimiento de las Leyes



Como se aprecia en la Tabla 9, muestran los principales resultados de la encuesta realizada a 132 operadores de justicia de la Corte Superior de Justicia de Lima Norte - Diciembre 2020, de los operadores de justicia encuestados manifiestan respecto a si considera que es adecuado el nivel de cumplimiento de las leyes en los delitos de fraude informático tipificado en el código procesal penal peruano; 41 operadores de justicia refieren que están en desacuerdo, lo que representa el 31.06%, 29 operadores de justicia que se encuentran de acuerdo, lo que representa el 21.97%, 23 operadores de justicia que están indecisos, lo que representa el 17.42%, 21 operadores de justicia que indicaron que se encuentran muy de acuerdo, lo que representa el 15.91% y 18 operadores de justicia que señalaron estar muy en desacuerdo, lo que representa el 13.64%.

Es decir, el 44.70% está en desacuerdo respecto a si considera que es adecuado el nivel de cumplimiento de las leyes en los delitos de fraude informático tipificado en el código procesal penal peruano.

Tabla 10

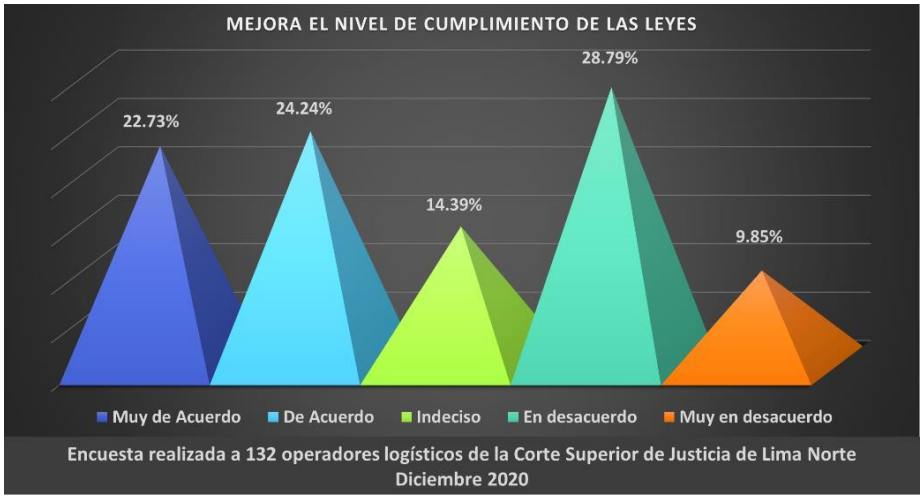
Mejora el Nivel de Cumplimiento de las Leyes

Respuestas	Cantidad	Porcentaje
Muy de Acuerdo	30	22.73%
De Acuerdo	32	24.24%
Indeciso	19	14.39%
En desacuerdo	38	28.79%
Muy en desacuerdo	13	9.85%
N° de Respuestas	**132**	**100.00%**

Encuesta realizada a 132 operadores de justicia de la Corte Superior de Justicia de Lima Norte - Diciembre 2020

Figura 10

Mejora el Nivel de Cumplimiento de las Leyes



Como se aprecia en la Tabla 10, muestran los principales resultados de la encuesta realizada a 132 operadores de justicia de la Corte Superior de Justicia de Lima Norte - Diciembre 2020, de los operadores de justicia encuestados manifiestan respecto a si considera que pude mejorar el nivel de cumplimiento de las leyes en los delitos de fraude informático tipificado en el código procesal penal peruano; 38 operadores de justicia refieren que están en desacuerdo, lo que representa el 28.79%, 32 operadores de justicia que se encuentran de

acuerdo, lo que representa el 24.24%, 30 operadores de justicia que indicaron que se encuentran muy de acuerdo, lo que representa el 22.73%, 19 operadores de justicia que están indecisos, lo que representa el 14.39% y 13 operadores de justicia que señalaron estar muy en desacuerdo, lo que representa el 9.85%.

Es decir, el 46.97% está de acuerdo respecto a si considera que pude mejorar el nivel de cumplimiento de las leyes en los delitos de fraude informático tipificado en el código procesal penal peruano.

Tabla 11

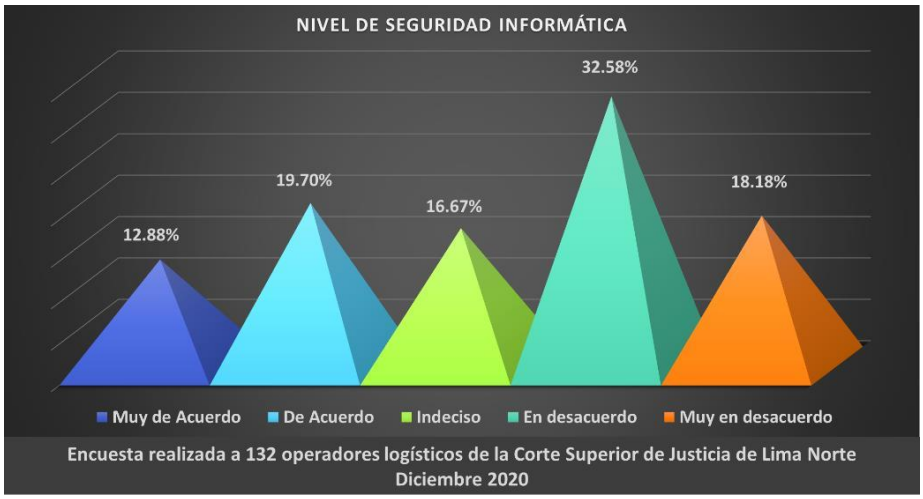
Nivel de Seguridad Informática

Respuestas	Cantidad	Porcentaje
Muy de Acuerdo	17	12.88%
De Acuerdo	26	19.70%
Indeciso	22	16.67%
En desacuerdo	43	32.58%
Muy en desacuerdo	24	18.18%
N° de Respuestas	**132**	**100.00%**

Encuesta realizada a 132 operadores de justicia de la Corte Superior de Justicia de Lima Norte - Diciembre 2020

Figura 11

Nivel de Seguridad Informática



Como se aprecia en la Tabla 11, muestran los principales resultados de la encuesta realizada a 132 operadores de justicia de la Corte Superior de Justicia de Lima Norte - Diciembre 2020, de los operadores de justicia encuestados manifiestan respecto a si considera que es adecuado el nivel de seguridad informática en los delitos de fraude informático tipificado en el código procesal penal peruano; 43 operadores de justicia refieren que están en desacuerdo, lo que representa el 32.58%, 26 operadores de justicia que se encuentran de acuerdo, lo que representa el 19.70%, 24 operadores de justicia que señalaron estar muy en desacuerdo, lo que representa el 18.18%, 22 operadores de justicia que están indecisos, lo que representa el 16.67% y 17 operadores de justicia que indicaron que se encuentran muy de acuerdo, lo que representa el 12.88%.

Es decir, el 50.76% está en desacuerdo respecto a si considera que es adecuado el nivel de seguridad informática en los delitos de fraude informático tipificado en el código procesal penal peruano.

Tabla 12

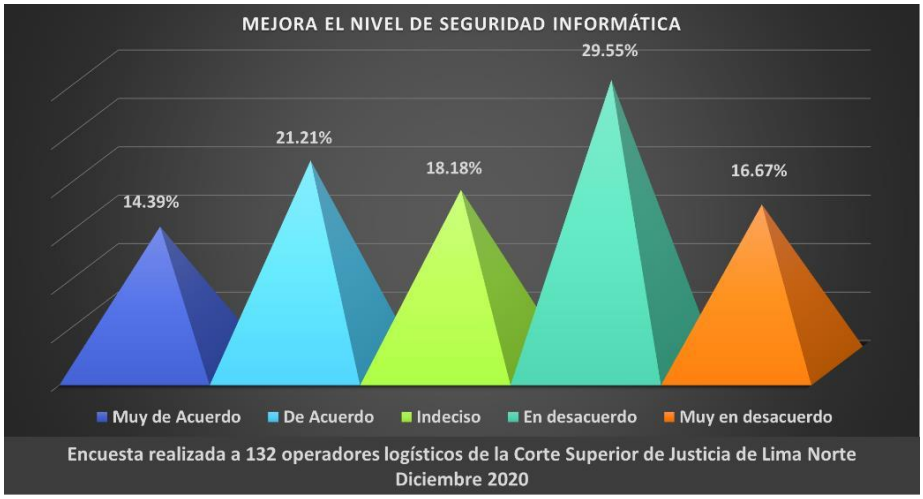
Mejora el Nivel de Seguridad Informática

Respuestas	Cantidad	Porcentaje
Muy de Acuerdo	19	14.39%
De Acuerdo	28	21.21%
Indeciso	24	18.18%
En desacuerdo	39	29.55%
Muy en desacuerdo	22	16.67%
N° de Respuestas	**132**	**100.00%**

Encuesta realizada a 132 operadores de justicia de la Corte Superior de Justicia de Lima Norte - Diciembre 2020

Figura 12

Mejora el Nivel de Seguridad Informática



Como se aprecia en la Tabla 12, muestran los principales resultados de la encuesta realizada a 132 operadores de justicia de la Corte Superior de Justicia de Lima Norte - Diciembre 2020, de los operadores de justicia encuestados manifiestan respecto a si considera que pude mejorar el nivel de seguridad informática en los delitos de fraude informático tipificado en el código procesal penal peruano; 39 operadores de justicia refieren que están en desacuerdo, lo que representa el 29.55%, 28 operadores de justicia que se encuentran de

acuerdo, lo que representa el 21.21%, 24 operadores de justicia que están indecisos, lo que representa el 18.18%, 22 operadores de justicia que señalaron estar muy en desacuerdo, lo que representa el 16.67% y 19 operadores de justicia que indicaron que se encuentran muy de acuerdo, lo que representa el 14.39%.

Es decir, el 46.21% está en desacuerdo respecto a si considera que pude mejorar el nivel de seguridad informática en los delitos de fraude informático tipificado en el código procesal penal peruano.

Tabla 13

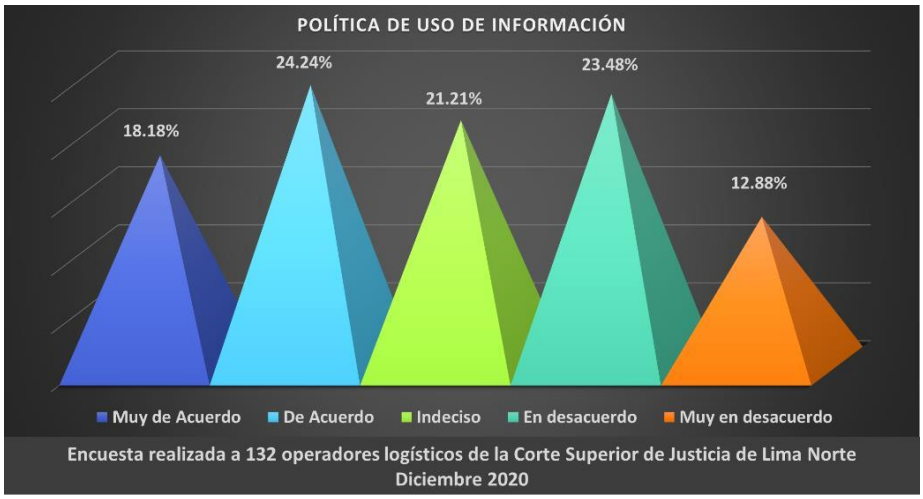
Política de Uso de Información

Respuestas	Cantidad	Porcentaje
Muy de Acuerdo	24	18.18%
De Acuerdo	32	24.24%
Indeciso	28	21.21%
En desacuerdo	31	23.48%
Muy en desacuerdo	17	12.88%
N° de Respuestas	**132**	**100.00%**

Encuesta realizada a 132 operadores de justicia de la Corte Superior de Justicia de Lima Norte - Diciembre 2020

Figura 13

Política de Uso de Información



Como se aprecia en la Tabla 13, muestran los principales resultados de la encuesta realizada a 132 operadores de justicia de la Corte Superior de Justicia de Lima Norte - Diciembre 2020, de los operadores de justicia encuestados manifiestan respecto a si considera que es adecuada la política de uso de información en los delitos de fraude informático tipificado en el código procesal penal peruano; 32 operadores de justicia que se encuentran de acuerdo, lo que representa el 24.24%, 31 operadores de justicia refieren que están en desacuerdo, lo que representa el 23.48%, 28 operadores de justicia que están indecisos, lo que representa el 21.21%, 24 operadores de justicia que indicaron que se encuentran muy de acuerdo, lo que representa el 18.18% y 17 operadores de justicia que señalaron estar muy en desacuerdo, lo que representa el 12.88%.

Es decir, el 42.42% está de acuerdo respecto a si considera que es adecuada la política de uso de información en los delitos de fraude informático tipificado en el código procesal penal peruano.

Tabla 14

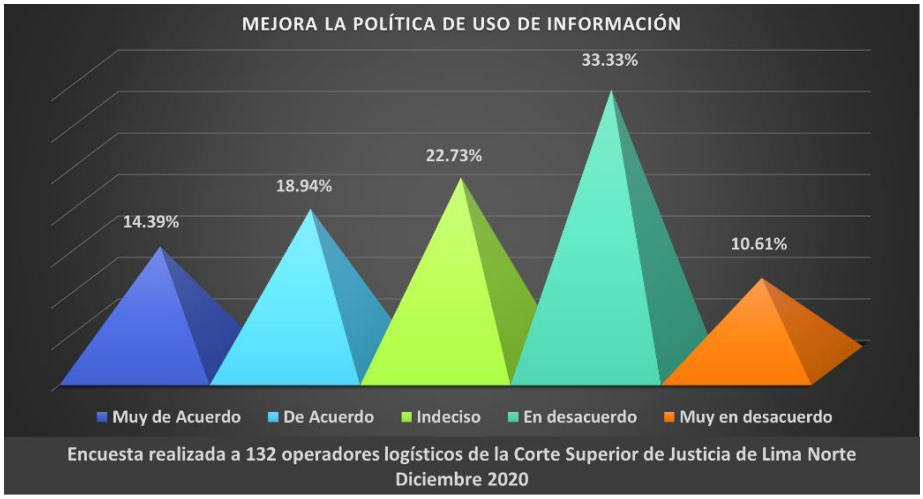
Mejora la Política de Uso de Información

Respuestas	Cantidad	Porcentaje
Muy de Acuerdo	19	14.39%
De Acuerdo	25	18.94%
Indeciso	30	22.73%
En desacuerdo	44	33.33%
Muy en desacuerdo	14	10.61%
N° de Respuestas	**132**	**100.00%**

Encuesta realizada a 132 operadores de justicia de la Corte Superior de Justicia de Lima Norte - Diciembre 2020

Figura 14

Mejora la Política de Uso de Información



Como se aprecia en la Tabla 14, muestran los principales resultados de la encuesta realizada a 132 operadores de justicia de la Corte Superior de Justicia de Lima Norte - Diciembre 2020, de los operadores de justicia encuestados manifiestan respecto a si considera que pude mejorar la política de uso de información en los delitos de fraude informático tipificado en el código procesal penal peruano; 44 operadores de justicia refieren que están en desacuerdo, lo que representa el 33.33%, 30 operadores de justicia que están indecisos, lo que

representa el 22.73%, 25 operadores de justicia que se encuentran de acuerdo, lo que representa el 18.94%, 19 operadores de justicia que indicaron que se encuentran muy de acuerdo, lo que representa el 14.39% y 14 operadores de justicia que señalaron estar muy en desacuerdo, lo que representa el 10.61%.

Es decir, el 43.94% está en desacuerdo respecto a si considera que pude mejorar la política de uso de información en los delitos de fraude informático tipificado en el código procesal penal peruano.

Tabla 15

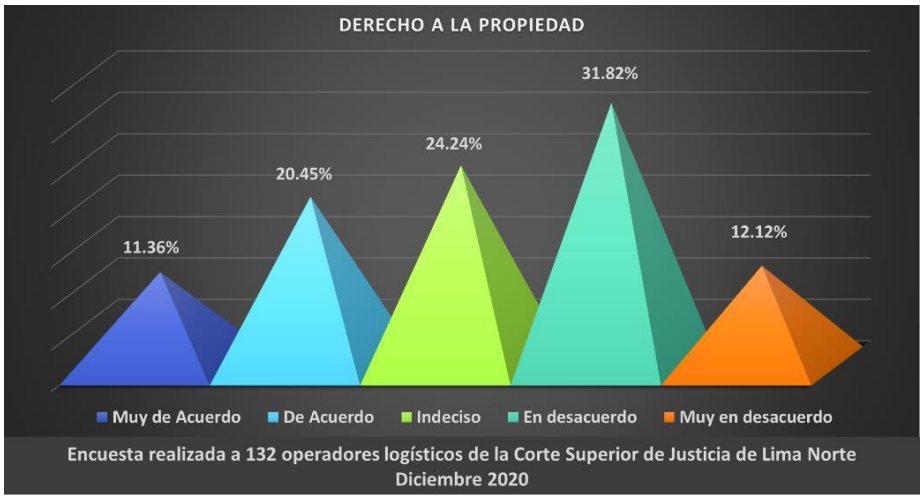
Derecho a la Propiedad

Respuestas	Cantidad	Porcentaje
Muy de Acuerdo	15	11.36%
De Acuerdo	27	20.45%
Indeciso	32	24.24%
En desacuerdo	42	31.82%
Muy en desacuerdo	16	12.12%
N° de Respuestas	**132**	**100.00%**

Encuesta realizada a 132 operadores de justicia de la Corte Superior de Justicia de Lima Norte - Diciembre 2020

Figura 15

Derecho a la Propiedad



Como se aprecia en la Tabla 15, muestran los principales resultados de la encuesta realizada a 132 operadores de justicia de la Corte Superior de Justicia de Lima Norte - Diciembre 2020, de los operadores de justicia encuestados manifiestan respecto a si considera que es adecuado el derecho a la propiedad intelectual en los delitos de fraude informático tipificado en el código procesal penal peruano; 42 operadores de justicia refieren que están en desacuerdo, lo que representa el 31.82%, 32 operadores de justicia que están indecisos, lo que representa el 24.24%, 27 operadores de justicia que se encuentran de acuerdo, lo que representa el 20.45%, 16 operadores de justicia que señalaron estar muy en desacuerdo, lo que representa el 12.12% y 15 operadores de justicia que indicaron que se encuentran muy de acuerdo, lo que representa el 11.36%.

Es decir, el 43.94% está en desacuerdo respecto a si considera que es adecuado el derecho a la propiedad intelectual en los delitos de fraude informático tipificado en el código procesal penal peruano.

Tabla 16

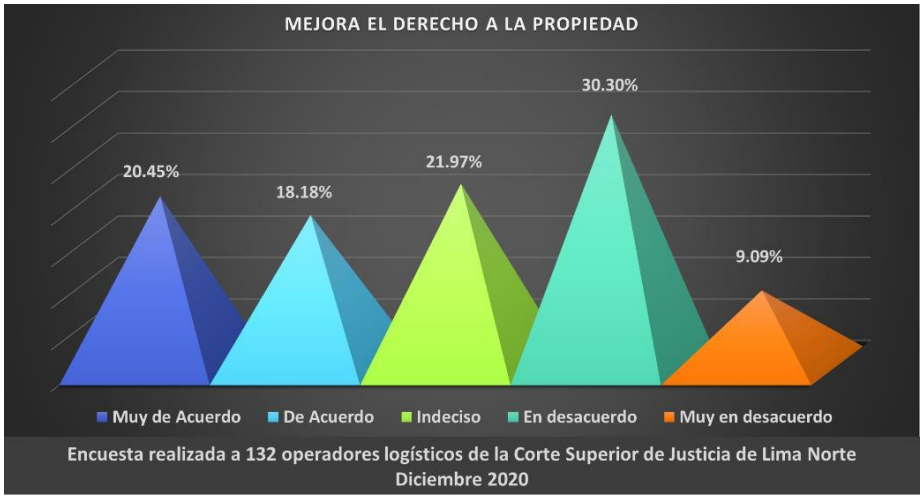
Mejora el Derecho a la Propiedad

Respuestas	Cantidad	Porcentaje
Muy de Acuerdo	27	20.45%
De Acuerdo	24	18.18%
Indeciso	29	21.97%
En desacuerdo	40	30.30%
Muy en desacuerdo	12	9.09%
N° de Respuestas	**132**	**100.00%**

Encuesta realizada a 132 operadores de justicia de la Corte Superior de Justicia de Lima Norte - Diciembre 2020

Figura 16

Mejora el Derecho a la Propiedad



Como se aprecia en la Tabla 16, muestran los principales resultados de la encuesta realizada a 132 operadores de justicia de la Corte Superior de Justicia de Lima Norte - Diciembre 2020, de los operadores de justicia encuestados manifiestan respecto a si considera que pude mejorar el derecho a la propiedad intelectual en los delitos de fraude informático tipificado en el código procesal penal peruano; 40 operadores de justicia refieren que están en desacuerdo, lo que representa el 30.30%, 29 operadores de justicia que están indecisos, lo que

representa el 21.97%, 27 operadores de justicia que indicaron que se encuentran muy de acuerdo, lo que representa el 20.45%, 24 operadores de justicia que se encuentran de acuerdo, lo que representa el 18.18% y 12 operadores de justicia que señalaron estar muy en desacuerdo, lo que representa el 9.09%.

Es decir, el 39.39% está en desacuerdo respecto a si considera que pude mejorar el derecho a la propiedad intelectual en los delitos de fraude informático tipificado en el código procesal penal peruano.

Tabla 17

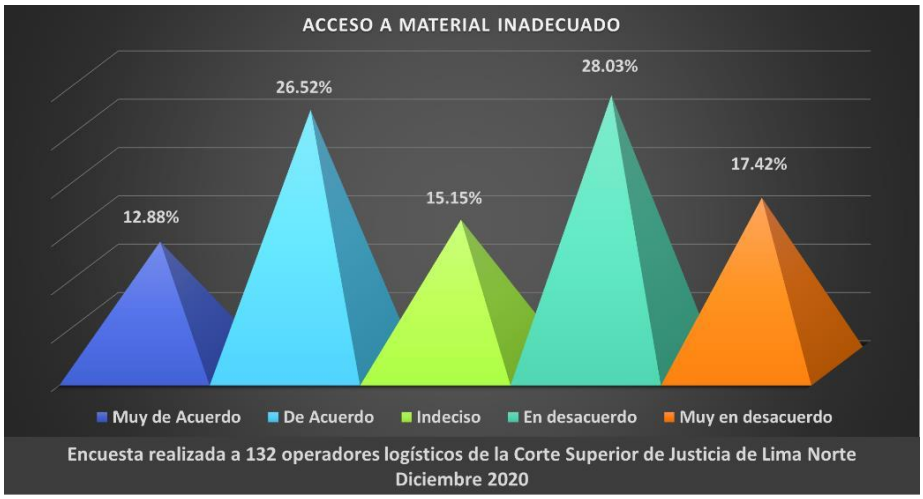
Acceso a Material Inadecuado

Respuestas	Cantidad	Porcentaje
Muy de Acuerdo	17	12.88%
De Acuerdo	35	26.52%
Indeciso	20	15.15%
En desacuerdo	37	28.03%
Muy en desacuerdo	23	17.42%
N° de Respuestas	**132**	**100.00%**

Encuesta realizada a 132 operadores de justicia de la Corte Superior de Justicia de Lima Norte - Diciembre 2020

Figura 17

Acceso a Material Inadecuado



Como se aprecia en la Tabla 17, muestran los principales resultados de la encuesta realizada a 132 operadores de justicia de la Corte Superior de Justicia de Lima Norte - Diciembre 2020, de los operadores de justicia encuestados manifiestan respecto a si considera que es frecuente el acceso a material inadecuado en los delitos de fraude informático tipificado en el código procesal penal peruano; 37 operadores de justicia refieren que están en desacuerdo, lo que representa el 28.03%, 35 operadores de justicia que se encuentran de acuerdo, lo que representa el 26.52%, 23 operadores de justicia que señalaron estar muy en desacuerdo, lo que representa el 17.42%, 20 operadores de justicia que están indecisos, lo que representa el 15.15% y 17 operadores de justicia que indicaron que se encuentran muy de acuerdo, lo que representa el 12.88%.

Es decir, el 45.45% está en desacuerdo respecto a si considera que es frecuente el acceso a material inadecuado en los delitos de fraude informático tipificado en el código procesal penal peruano.

Tabla 18

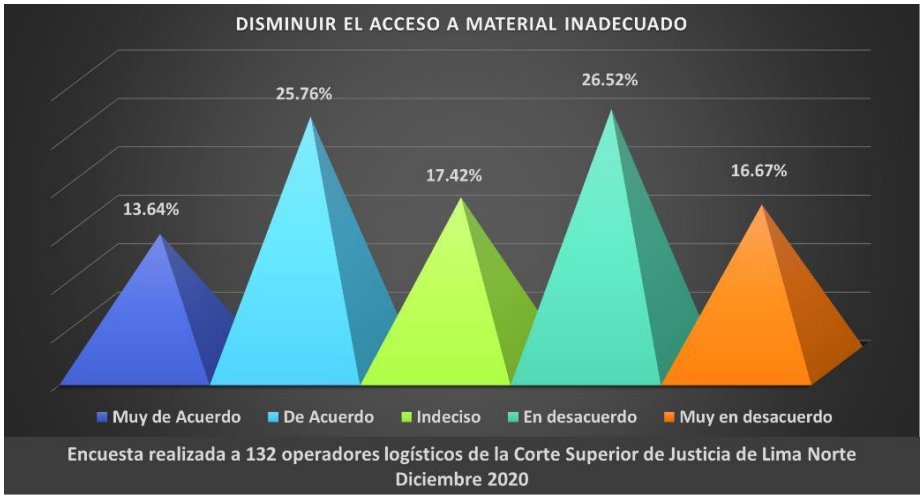
Disminuir el Acceso a Material Inadecuado

Respuestas	Cantidad	Porcentaje
Muy de Acuerdo	18	13.64%
De Acuerdo	34	25.76%
Indeciso	23	17.42%
En desacuerdo	35	26.52%
Muy en desacuerdo	22	16.67%
N° de Respuestas	**132**	**100.00%**

Encuesta realizada a 132 operadores de justicia de la Corte Superior de Justicia de Lima Norte - Diciembre 2020

Figura 18

Disminuir el Acceso a Material Inadecuado



Como se aprecia en la Tabla 18, muestran los principales resultados de la encuesta realizada a 132 operadores de justicia de la Corte Superior de Justicia de Lima Norte - Diciembre 2020, de los operadores de justicia encuestados manifiestan respecto a si considera que pude disminuir el nivel de acceso a material inadecuado en los delitos de fraude informático tipificado en el código procesal penal peruano; 35 operadores de justicia refieren que están en desacuerdo, lo que representa el 26.52%, 34 operadores de justicia que se

encuentran de acuerdo, lo que representa el 25.76%, 23 operadores de justicia que están indecisos, lo que representa el 17.42%, 22 operadores de justicia que señalaron estar muy en desacuerdo, lo que representa el 16.67% y 18 operadores de justicia que indicaron que se encuentran muy de acuerdo, lo que representa el 13.64%.

Es decir, el 43.18% está en desacuerdo respecto a si considera que pude disminuir el nivel de acceso a material inadecuado en los delitos de fraude informático tipificado en el código procesal penal peruano.

Tabla 19

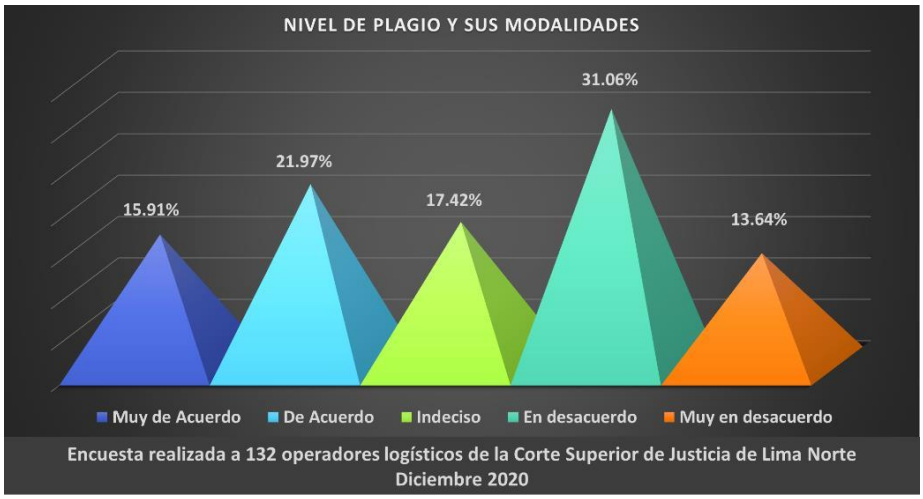
Nivel de Plagio y sus Modalidades

Respuestas	Cantidad	Porcentaje
Muy de Acuerdo	21	15.91%
De Acuerdo	29	21.97%
Indeciso	23	17.42%
En desacuerdo	41	31.06%
Muy en desacuerdo	18	13.64%
N° de Respuestas	**132**	**100.00%**

Encuesta realizada a 132 operadores de justicia de la Corte Superior de Justicia de Lima Norte - Diciembre 2020

Figura 19

Nivel de Plagio y sus Modalidades



Como se aprecia en la Tabla 19, muestran los principales resultados de la encuesta realizada a 132 operadores de justicia de la Corte Superior de Justicia de Lima Norte - Diciembre 2020, de los operadores de justicia encuestados manifiestan respecto a si considera que es frecuente el nivel de plagio y sus modalidades en los delitos de fraude informático tipificado en el código procesal penal peruano; 41 operadores de justicia refieren que están en desacuerdo, lo que representa el 31.06%, 29 operadores de justicia que se encuentran de acuerdo, lo que representa el 21.97%, 23 operadores de justicia que están indecisos, lo que representa el 17.42%, 21 operadores de justicia que indicaron que se encuentran muy de acuerdo, lo que representa el 15.91% y 18 operadores de justicia que señalaron estar muy en desacuerdo, lo que representa el 13.64%.

Es decir, el 44.70% está en desacuerdo respecto a si considera que es frecuente el nivel de plagio y sus modalidades en los delitos de fraude informático tipificado en el código procesal penal peruano.

Tabla 20

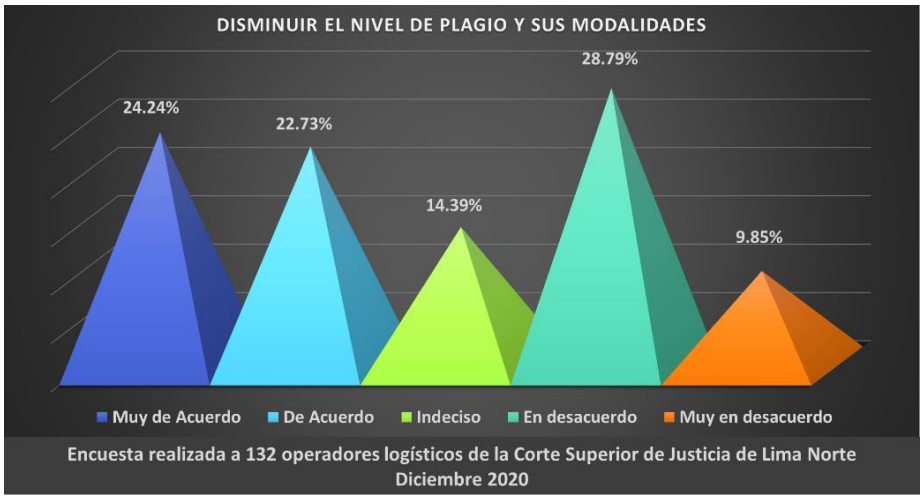
Disminuir el Nivel de Plagio y sus Modalidades

Respuestas	Cantidad	Porcentaje
Muy de Acuerdo	32	24.24%
De Acuerdo	30	22.73%
Indeciso	19	14.39%
En desacuerdo	38	28.79%
Muy en desacuerdo	13	9.85%
N° de Respuestas	**132**	**100.00%**

Encuesta realizada a 132 operadores de justicia de la Corte Superior de Justicia de Lima Norte - Diciembre 2020

Figura 20

Disminuir el Nivel de Plagio y sus Modalidades



Como se aprecia en la Tabla 20, muestran los principales resultados de la encuesta realizada a 132 operadores de justicia de la Corte Superior de Justicia de Lima Norte - Diciembre 2020, de los operadores de justicia encuestados manifiestan respecto a si considera que pude disminuir el nivel de plagio y sus modalidades en los delitos de fraude informático tipificado en el código procesal penal peruano; 38 operadores de justicia refieren que están en desacuerdo, lo que representa el 28.79%, 32 operadores de justicia que indicaron que se encuentran muy de acuerdo, lo que representa el 24.24%, 30 operadores de justicia que se

encuentran de acuerdo, lo que representa el 22.73%, 19 operadores de justicia que están indecisos, lo que representa el 14.39% y 13 operadores de justicia que señalaron estar muy en desacuerdo, lo que representa el 9.85%.

Es decir, el 46.97% está de acuerdo respecto a si considera que pude disminuir el nivel de plagio y sus modalidades en los delitos de fraude informático tipificado en el código procesal penal peruano.

4.2 Contrastación de hipótesis

Para realizar la contrastación de la Hipótesis, se utilizó el Coeficiente de correlación de Spearman, ρ (ro) que es una medida de correlación entre dos variables, como lo son las variables materia del presente estudio. Luego, el valor de p permitió tomar la decisión estadística correspondiente a cada una de las hipótesis formuladas.

El coeficiente de correlación de Spearman da un rango que permite identificar fácilmente el grado de correlación (la asociación o interdependencia) que tienen dos variables mediante un conjunto de datos de estas, de igual forma permite determinar si la correlación es positiva o negativa (si la pendiente de la línea correspondiente es positiva o negativa).

El estadístico ρ viene dado por la expresión:

$$\rho = 1 - \frac{6 \sum D^2}{N(N^2 - 1)}$$

Donde D es la diferencia entre los correspondientes estadísticos de orden de x - y. N es el número de parejas.

Prueba de hipótesis específicas

1. **Hipótesis específica 1:**

H_1: El nivel de Autenticidad de La Evidencia Digital influye significativamente en los Delitos de Fraude Informático tipificado en el Código Procesal Penal Peruano.

Ho: El nivel de Autenticidad de La Evidencia Digital NO influye significativamente en los Delitos de Fraude Informático tipificado en el Código Procesal Penal Peruano.

1. **Nivel de confianza:** 99%, NIVEL DE SIGNIFICACIÓN: 1%
2. **Estadístico de prueba:** Coeficiente de correlación de Spearman

Tabla 21

Correlación de Spearman - hipótesis especifica 1

			Nivel de autenticidad	Delitos de Fraude Informático
Spearman's rho	Nivel de autenticidad	Correlation Coefficient	1,000	0,816
		Sig. (2-tailed)		0,000
		N	132	132
	Delitos de Fraude Informático	Correlation Coefficient	0,816	1,000
		Sig. (2-tailed)	0,000	
		N	132	132

3. **Decisión:** Dado que p<0.01 se rechaza la Ho
4. **Conclusión:** Utilizando el coeficiente de correlación de Spearman para determinar si existe asociación o interdependencia entre las variables del estudio, se puede comprobar que existe evidencia significativa que el nivel de Autenticidad de La

Evidencia Digital influye significativamente en los Delitos de Fraude Informático tipificado en el Código Procesal Penal Peruano.

1. **Hipótesis específica 2:**

H_2: El nivel de Confiabilidad de La Evidencia Digital influye significativamente en los Delitos de Fraude Informático tipificado en el Código Procesal Penal Peruano.

Ho: El nivel de Confiabilidad de La Evidencia Digital NO influye significativamente en los Delitos de Fraude Informático tipificado en el Código Procesal Penal Peruano.

2. **Nivel de confianza:** 99%, NIVEL DE SIGNIFICACIÓN: 1%
3. **Estadístico de prueba:** Coeficiente de correlación de Spearman

Tabla 22

Correlación de Spearman - hipótesis especifica 2

			Nivel de confiabilidad	Delitos de Fraude Informático
Spearman's rho	Nivel de confiabilidad	Correlation Coefficient	1,000	0,821
		Sig. (2-tailed)		0,000
		N	132	132
	Delitos de Fraude Informático	Correlation Coefficient	0,821	1,000
		Sig. (2-tailed)	0,000	
		N	132	132

4. **Decisión:** Dado que p<0.01 se rechaza la Ho
5. **Conclusión:** Utilizando el coeficiente de correlación de Spearman para determinar si existe asociación o interdependencia entre las variables del estudio, se puede comprobar que existe evidencia significativa que el nivel de confiabilidad de La

Evidencia Digital influye significativamente en los Delitos de Fraude Informático tipificado en el Código Procesal Penal Peruano.

1. **Hipótesis específica 3:**

H_3: El nivel de Completitud o Suficiencia de La Evidencia Digital influye significativamente en los Delitos de Fraude Informático tipificado en el Código Procesal Penal Peruano.

Ho: El nivel de Completitud o Suficiencia de La Evidencia Digital NO influye significativamente en los Delitos de Fraude Informático tipificado en el Código Procesal Penal Peruano.

2. **Nivel de confianza:** 99%, NIVEL DE SIGNIFICACIÓN: 1%
3. **Estadístico de prueba:** Coeficiente de correlación de Spearman

Tabla 23

Correlación de Spearman - hipótesis especifica 3

			Nivel de completitud o suficiencia	Delitos de Fraude Informático
Spearman's rho	Nivel de completitud o suficiencia	Correlation Coefficient	1,000	0,827
		Sig. (2-tailed)		0,000
		N	132	132
	Delitos de Fraude Informático	Correlation Coefficient	0,827	1,000
		Sig. (2-tailed)	0,000	
		N	132	132

4. **Decisión:** Dado que p<0.01 se rechaza la Ho

5. **Conclusión:** Utilizando el coeficiente de correlación de Spearman para determinar si existe asociación o interdependencia entre las variables del estudio, se puede comprobar que existe evidencia significativa que el nivel de completitud o suficiencia de La Evidencia Digital influye significativamente en los Delitos de Fraude Informático tipificado en el Código Procesal Penal Peruano.

1. **Hipótesis específica 4:**

H_4: El nivel de conocimiento de las leyes de La Evidencia Digital influye significativamente en los Delitos de Fraude Informático tipificado en el Código Procesal Penal Peruano.

Ho: El nivel de conocimiento de las leyes de La Evidencia Digital NO influye significativamente en los Delitos de Fraude Informático tipificado en el Código Procesal Penal Peruano.

2. **Nivel de confianza:** 99%, NIVEL DE SIGNIFICACIÓN: 1%
3. **Estadístico de prueba:** Coeficiente de correlación de Spearman

Tabla 24

Correlación de Spearman - hipótesis especifica 4

			Nivel de conocimiento de las leyes	Delitos de Fraude Informático
Spearman's rho	Nivel de conocimiento de las leyes	Correlation Coefficient	1,000	0,824
		Sig. (2-tailed)		0,000
		N	132	132
	Delitos de Fraude Informático	Correlation Coefficient	0,824	1,000
		Sig. (2-tailed)	0,000	
		N	132	132

4. **Decisión:** Dado que p<0.01 se rechaza la Ho
5. **Conclusión:** Utilizando el coeficiente de correlación de Spearman para determinar si existe asociación o interdependencia entre las variables del estudio, se puede comprobar que existe evidencia significativa que el nivel de conocimiento de las leyes de La Evidencia Digital influye significativamente en los Delitos de Fraude Informático tipificado en el Código Procesal Penal Peruano.

1. **Hipótesis específica 5:**

H_5: El nivel de cumplimiento de las leyes de La Evidencia Digital influye significativamente en los Delitos de Fraude Informático tipificado en el Código Procesal Penal Peruano.

Ho: El nivel de cumplimiento de las leyes de La Evidencia Digital NO influye significativamente en los Delitos de Fraude Informático tipificado en el Código Procesal Penal Peruano.

2. Nivel de confianza: 99%, NIVEL DE SIGNIFICACIÓN: 1%

3. Estadístico de prueba: Coeficiente de correlación de Spearman

Tabla 25

Correlación de Spearman - hipótesis especifica 5

			Nivel de cumplimiento de las leyes	Delitos de Fraude Informático
Spearman's rho	Nivel de cumplimiento de las leyes	Correlation Coefficient	1,000	0,836
		Sig. (2-tailed)		0,000
		N	132	132
	Delitos de Fraude Informático	Correlation Coefficient	0,836	1,000
		Sig. (2-tailed)	0,000	
		N	132	132

4. Decisión: Dado que $p<0.01$ se rechaza la Ho

5. Conclusión: Utilizando el coeficiente de correlación de Spearman para determinar si existe asociación o interdependencia entre las variables del estudio, se puede comprobar que existe evidencia significativa que el nivel de cumplimiento de las leyes de La Evidencia Digital influye significativamente en los Delitos de Fraude Informático tipificado en el Código Procesal Penal Peruano.

Luego de haber comprobado las cinco hipótesis específicas, se comprobó la hipótesis general:

La Evidencia Digital influye significativamente en los Delitos de Fraude Informático tipificado en el Código Procesal Penal Peruano.

4.3 Discusión de resultados

Luego de analizar las encuestas aplicadas a los 132 operadores de justicia de la Corte Superior de Justicia de Lima Norte, se encontraron similitudes con las siguientes investigaciones:

A nivel nacional tenemos los datos Temperini, Marcelo Gabriel en su estudio titulado "Delitos Informáticos en Latinoamérica: Un estudio de derecho comparado. 1ra. Parte". De acuerdo con diferentes estudios actuales, los delitos informáticos son los de mayor crecimiento en los últimos años, con una proyección cada vez mayor.

La posibilidad de su comisión a través de Internet permite que, sin mayores complicaciones, el delincuente pueda estar en un determinado país, utilizar servicios de otro, para finalmente atacar a una o más víctimas de un tercer país interviniente.

A modo de conclusión se lograron obtener estadísticas actualizadas con un ranking de países de acuerdo al estado de situación en la regulación penal de los delitos informáticos más importantes, así como la lista de delitos informáticos menos sancionados (Temperini, 2013).

En 1991 se describieron los virus peruanos. Al igual que la corriente búlgara, en 1991 apareció en el Perú el primer virus local, autodenominado „Mensaje y que no era otra cosa que una simple mutación del virus "Jerusalem-B" y al que su autor le agregó una ventana con su nombre y número telefónico. Los virus con apellidos como Espejo, Martínez y Aguilar fueron variantes del Jerusalem-B y prácticamente se difundieron a nivel nacional.

Continuando con la lógica del tedio, en 1993 empezaron a crearse y diseminarse especies nacionales desarrolladas con creatividad propia, siendo alguno de ellos sumamente originales, como los virus Katia, Rogué o F03241 y los polimórficos Rogué II y Please Wait (que formateaba el disco duro). La creación de los virus locales ocurre en cualquier país y el Perú no podía ser la excepción.

Comparando los resultados de las anteriores investigaciones con el presente estudio, se puede demostrar que, la Evidencia Digital influye significativamente en los Delitos de Fraude Informático tipificado en el Código Procesal Penal Peruano.

CAPITULO V. CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

1. Se determinó que el nivel de Autenticidad de la Evidencia Digital influye significativamente en los Delitos de Fraude Informático tipificado en el Código Procesal Penal Peruano.
2. Se determinó que el nivel de Confiabilidad de la Evidencia Digital influye significativamente en los Delitos de Fraude Informático tipificado en el Código Procesal Penal Peruano.
3. Se determinó que el nivel de Completitud o Suficiencia de la Evidencia Digital influye significativamente en los Delitos de Fraude Informático tipificado en el Código Procesal Penal Peruano.
4. Se determinó que el nivel de Conocimiento de las Leyes de la Evidencia Digital influye significativamente en los Delitos de Fraude Informático tipificado en el Código Procesal Penal Peruano.
5. Se determinó que el número de delitos de corrupción de funcionarios se relacionan significativamente con la estabilidad social del Perú.
6. Se determinó que el nivel de Cumplimiento de las Leyes de la Evidencia Digital influye significativamente en los Delitos de Fraude Informático tipificado en el Código Procesal Penal Peruano.

5.2 Recomendaciones

1. Fortalecer el nivel de autenticidad de la evidencia digital, utilizando procesos tecnológicos acordes a la investigación, de tal manera minimizar los fraudes electrónicos en nuestro país.

2. La evidencia digital, además de ser adecuada y eficiente, debe considerarse como un elemento de suma importancia para la comprobación de la comisión de delitos informáticos, lo que no impide que ellos puedan ser probados por otros medios. Sin embargo, esto puede ser mucho más difícil si no se cuenta con este elemento probatorio.
3. La evidencia digital efectivamente es adecuada y eficiente para esta finalidad toda vez que al representar la información contenida en los sistemas informáticos afectados, o en los cuales se realizó la conducta, su presencia es útil para brindar certeza frente a la afectación al bien jurídico informático protegido por este tipo de delitos, así como para establecer lo relativo al uso de sistemas informáticos para la comisión del delito.
4. Es necesaria que la legislación penal, en materia de delitos informáticos sea revisada constantemente, debido a que el avance de las tecnologías de la información y la comunicación es acelerado.
5. Debe incluirse en la legislación penal, la tipificación del delito informático, como la apropiación de la información y la intimidad personal en las redes sociales y debe considerárselo acto antijurídico y ser causa de sanción.
6. Difundir la presente investigación, de tal manera, que todos los interesados en el tema tengan una referencia o fuente de consulta respecto a la evidencia digital en los delitos de fraude electrónico, los cuales últimamente han crecido considerablemente.

BIBLIOGRAFÍA

Acurio del pino, Santiago. Delitos Informáticos: Generalidades. pp. 20-21 Consulta: 19 de mayo de 2020 https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf.

Álvarez Marañón, G., & Pérez García, P. P. (2004). Seguridad informática para la empresa y particulares. Madrid: McGraw-Hill.

Buitrago, D. (2019). La recolección y custodia de las evidencias digitales del auditor forense en entidades financieras. Obtenido de https://repositorio.umsa.bo/bitstream/handle/123456789/21000/DAF-V-II%20016-2019%20%E2%80%9CLA%20RECOLECCI%C3%93N%20Y%20CUSTODIA%20DE%20LAS%20EVIDENCIAS%20DIGITALES%20DEL%20AUDITOR%20FORENSE%20EN%20ENTIDADES%20FINANCIERAS%E2%80%9D.pdf

Cacha, C. (2020). Peritaje informático basado en una nueva metodología híbrida en 2M & J Ingenieros – Huaraz 2019. Obtenido de http://repositorio.upci.edu.pe/bitstream/handle/upci/137/T-CACHA_ARANA_CRISTHIAN.pdf

Campos, M. A. (07 de abril de 2015). Historia del delito informático. Recuperado el 01 de setiembre de 2016, de http://delitosinformaticospe.blogspot.pe/2015/04/historia-del-delitoinformatico.html

De la Cruz, F. (2017). Aplicación de metodologías y herramientas de la informática forense para reducir el riesgo de la seguridad informática en la Dirección Nacional de Comunicación y Criminalística de la Policía Nacional Del Perú – Huaraz – 2015. Obtenido de http://repositorio.unasam.edu.pe/bitstream/handle/UNASAM/2626/T033_41010567_M.pdf

Estrada Garavilla, M. (12 de Junín de 2011). DELITOS INFORMÁTICOS. Recuperado el 01 de setiembre de 2016, de: https://www.unifr.ch/ddp1/derechopenal/articulos/a_20080526_32.pdf.

Gioia, C. (2019). Metodología de análisis forense informático para la obtención de evidencia digital en Base de Datos. Obtenido de https://repositoriocyt.unlam.edu.ar/bitstream/123456789/850/1/MI-Gioia.pdf

Guerrero Argote, Carlos. De Budapest al Perú: Análisis sobre el proceso de implementación

del Convenio de Ciberdelincuencia impacto en el corto, mediano y largo plazo. Editorial: Derechos Digitales América Latina, 2018, p.4.

López Hernández, M. A. (12 de junio de 2011). SEGURIDAD INFORMATICA. Recuperado el 01 de setiembre de 2016, de: http://alejandr00022.blogspot.pe/p/seguridad-informatica.html.

Mona Al-achkar Jabbour. (1 de febrero de 2016). Seguridad Cibernética contra delitos informáticos. Obtenido de: http://worldjusticeproject.org/blog/importance-cyber-security Ojeda.

Osco, M. (2019). La admisibilidad y el valor probatorio de la evidencia digital en el Sistema Jurídico Peruano 2018. Obtenido de https://repositorio.ucv.edu.pe/handle/20.500.12692/26623

Pérez, J. E. (2010). Delitos informáticos y entorno jurídico vigente en Colombia. cuad. contab, 11(28), 41-66.

Ojeda Pérez, J. E., Rincón Rodríguez, F., Arias Flórez, M. E., & Daza Martínez, L. A. (2010). Delitos informáticos y entorno jurídico vigente en Colombia. Cuaderno de contabilidad, 49.

Oxman, N. (2013). Estafas informáticas a través de Internet: acerca de la imputación penal del "phishing" y el "pharming". Revista de Derecho de la Pontificia Universidad Católica de Valparaíso, 41(1), 211 - 262.

Palazzi, P. A. (2000). Delitos Informáticos Ad-Hoc. Buenos Aires. RIQUERT, M. A. (2011). ESTADO DE LA LEGISLACIÓN CONTRA LA DELINCUENCIA INFORMÁTICA EN EL MERCOSUR. Recuperado el 01 de agosto de 2016, de: https://www.unifr.ch/ddp1/derechopenal/articulos/a_20080526_88.pd

Rodríguez Arbeláez, J. D. (12 de junio de 2011). Análisis de los delitos informáticos presentes en las redes sociales en Colombia para el año 2011 y su regulación. Recuperado el 31 de agosto de 2016, de: http://bdigital.ces.edu.co:8080/repositorio/bitstream/10946/1334/2/Delitos%20en%20las%20Redes%20Sociales.pdf.

Rosero, D. (2019). Diseño de una metodología de recolección de evidencia digital para análisis forense de unidades de disco duro, basada en la norma ISO/IEC 27037:2012. Obtenido de https://node2.123dok.com/dt02pdf/123dok_es/001/083/1083939.pdf.pdf

Supo, J. (2014). Recuperado el 24 de mayo de 2016, de Niveles de Investigación:

http://seminariosdeinvestigacion.com/niveles-deinvestigacion/

Villavicencio Terreros, Felipe. Delitos Informáticos. Revista IUS ET VERITAS. Lima, 2014, N° 49, pp. 286-287

ANEXOS

Anexo 1 Matriz de coherencia interna

Título	Definición del Problema	Objetivos	Formulación de Hipótesis	Clasificación de variables	Definición Operacional	Metodología	Población, Muestra y Muestreo	Técnica e Instrumento
LA EVIDENCIA DIGITAL Y LOS DELITOS DE FRAUDE INFORMÁTICO TIPIFICADO EN EL CÓDIGO PROCESAL PENAL PERUANO	**Problema general** ¿En qué medida influye la Evidencia Digital y los Delitos de Fraude Informático tipificado enel Código Procesal Penal Peruano? **Problemas Específicos** ¿En qué medida influye el nivel de Autenticidad de la Evidencia Digital en los Delitos de Fraude Informático tipificado enel Código Procesal Penal Peruano? ¿En qué medida influye el nivel de Confiabilidad de la Evidencia Digital en los Delitos de Fraude Informático tipificado enel Código Procesal Penal Peruano? ¿En qué medida influye el nivel de Completitud o Suficiencia de la Evidencia Digital en los Delitos de Fraude Informático tipificado enel Código Procesal Penal Peruano?	**Objetivo General:** Determinar la influencia de la Evidencia Digital en los Delitos de Fraude Informático tipificado en el Código Procesal Penal Peruano. **Objetivos Específicos:** Determinar la influencia del nivel de Autenticidad de la Evidencia Digital en los Delitos de Fraude Informático tipificado en el Código Procesal Penal Peruano. Determinar la influencia del nivel de Confiabilidad de la Evidencia Digital en los Delitos de Fraude Informático tipificado en el Código Procesal Penal Peruano. Determinar la influencia del nivel de Completitud o Suficiencia de la Evidencia Digital en los Delitos de Fraude Informático tipificado en el Código Procesal Penal Peruano.	**Hipótesis Principal:** La Evidencia Digital influye significativamente en los Delitos de Fraude Informático tipificado en el Código Procesal Penal Peruano. **Hipótesis Específicas:** El nivel de Autenticidad de La Evidencia Digital influye significativamente en los Delitos de Fraude Informático tipificado en el Código Procesal Penal Peruano. El nivel de Confiabilidad de La Evidencia Digital influye significativamente en los Delitos de Fraude Informático tipificado en el Código Procesal Penal Peruano. El nivel de Completitud o Suficiencia de La Evidencia Digital influye significativamente en los Delitos de Fraude Informático tipificado en el Código Procesal Penal Peruano. El nivel de Conocimiento de las Leyes de La Evidencia Digital influye significativamente en los Delitos de Fraude Informático	**Variables:** a) Evidencia Digital	➢ **Nivel de autenticidad.** ➢ **Nivel de confiabilidad.** ➢ **Nivel de completitud o suficiencia.** ➢ **Nivel de conocimiento de las leyes.** ➢ **Nivel de cumplimiento de las leyes.**	**Tipo:** De acuerdo con el tipo de investigación, el presente estudio es de tipo Aplicado. **Nivel:** Explicativo. **Método:** En la presente investigación se utilizó el método Ex Post Facto. **Diseño Correlacional:** Su diseño se representa así: $M = Oy\ (f)\ Ox_1$	**Población:** 200 operadores de justicia. **Muestra:** 132 operadores de justicia. **Muestreo** Se utilizó el muestreo probabilístico.	**Técnica** La principal técnica que se utilizará en el presente estudio fue la encuesta. **Instrumento** Cuestionario que, por intermedio de una encuesta de preguntas, ensu modalidad cerradas, se tomó a la muestra señalada.

Título	Definición del Problema	Objetivos	Formulación de Hipótesis	Clasificación de variables	Definición Operacional	Metodología	Población, Muestra y Muestreo	Técnica e Instrumento
	¿En qué medida influye el nivel de Conocimiento de las Leyes de la Evidencia Digital en los Delitos de Fraude Informático tipificado en el Código Procesal Penal Peruano? ¿En qué medida influye el nivel de Cumplimiento de las Leyes de la Evidencia Digital en los Delitos de Fraude Informático tipificado en el Código Procesal Penal Peruano?	Determinar la influencia del nivel de Conocimiento de las Leyes de la Evidencia Digital en los Delitos de Fraude Informático tipificado en el Código Procesal Penal Peruano. Determinar la influencia del nivel de Cumplimiento de las Leyes de la Evidencia Digital en los Delitos de Fraude Informático tipificado en el Código Procesal Penal Peruano.	tipificado en el Código Procesal Penal Peruano. El nivel de Cumplimiento de las Leyes de La Evidencia Digital influye significativamente en los Delitos de Fraude Informático tipificado en el Código Procesal Penal Peruano.	b) Delitos de Fraude Informático	➢ **Nivel de seguridad informática.** ➢ **Política de uso de la información.** ➢ **Derecho a la propiedad intelectual.** ➢ **Nivel de acceso a material inadecuado.** ➢ **Nivel de plagio y sus modalidades.**			

Anexo 2 Instrumento de Recolección de Datos (Encuesta)

Objetivo: Determinar la relación del Error Judicial Inexcusable con la Responsabilidad de los Jueces de la Oficina Desconcentrada de Control de la Magistratura (ODECMA) de Lima Centro.

PREGUNTAS	MA	A	I	D	MD
1. ¿Considera que es adecuado el nivel de autenticidad en la Evidencia Digital en los Delitos de Fraude Informático tipificado en el Código Procesal Penal Peruano?					
2. ¿Considera que pude mejorar el nivel de autenticidad en la Evidencia Digital en los Delitos de Fraude Informático tipificado en el Código Procesal Penal Peruano?					
3. ¿Considera que es adecuado el nivel de confiabilidad en la Evidencia Digital en los Delitos de Fraude Informático tipificado en el Código Procesal Penal Peruano?					
4. ¿Considera que pude mejorar el nivel de confiabilidad en la Evidencia Digital en los Delitos de Fraude Informático tipificado en el Código Procesal Penal Peruano?					
5. ¿Considera que es adecuado el nivel de completitud o suficiencia en la Evidencia Digital en los Delitos de Fraude Informático tipificado en el Código Procesal Penal Peruano?					
6. ¿Considera que pude mejorar el nivel de completitud o suficiencia en la Evidencia Digital en los Delitos de Fraude Informático tipificado en el Código Procesal Penal Peruano?					
7. ¿Considera que es adecuado el nivel de conocimiento de las leyes en los Delitos de Fraude Informático tipificado en el Código Procesal Penal Peruano?					
8. ¿Considera que pude mejorar el nivel de conocimiento de las leyes en los Delitos de Fraude Informático tipificado en el Código Procesal Penal Peruano?					

PREGUNTAS	MA	A	I	D	MD
9. ¿Considera que es adecuado el nivel de cumplimiento de las leyes en los Delitos de Fraude Informático tipificado en el Código Procesal Penal Peruano?					
10. ¿Considera que pude mejorar el nivel de cumplimiento de las leyes en los Delitos de Fraude Informático tipificado en el Código Procesal Penal Peruano?					
11. ¿Considera que es adecuado el nivel de seguridad informática en los Delitos de Fraude Informático tipificado en el Código Procesal Penal Peruano?					
12. ¿Considera que pude mejorar el nivel de seguridad informática en los Delitos de Fraude Informático tipificado en el Código Procesal Penal Peruano?					
13. ¿Considera que es adecuada la política de uso de información en los Delitos de Fraude Informático tipificado en el Código Procesal Penal Peruano?					
14. ¿Considera que pude mejorar la política de uso de información en los Delitos de Fraude Informático tipificado en el Código Procesal Penal Peruano?					
15. ¿Considera que es adecuado el derecho a la propiedad intelectual en los Delitos de Fraude Informático tipificado en el Código Procesal Penal Peruano?					
16. ¿Considera que pude mejorar el derecho a la propiedad intelectual en los Delitos de Fraude Informático tipificado en el Código Procesal Penal Peruano?					
17. ¿Considera que es frecuente el acceso a material inadecuado en los Delitos de Fraude Informático tipificado en el Código Procesal Penal Peruano?					

PREGUNTAS	MA	A	I	D	MD
18. ¿Considera que pude disminuir el nivel de acceso a material inadecuado en los Delitos de Fraude Informático tipificado en el Código Procesal Penal Peruano?					
19. ¿Considera que es frecuente el nivel de plagio y sus modalidades en los Delitos de Fraude Informático tipificado en el Código Procesal Penal Peruano?					
20. ¿Considera que pude disminuir el nivel de plagio y sus modalidades en los Delitos de Fraude Informático tipificado en el Código Procesal Penal Peruano?					