UNIVERSIDAD PERUANA LOS ANDES
Facultad de Derecho y Ciencias Políticas
Escuela Profesional de Derecho

TESIS

Título	:	DELITOS INFORMATICOS Y LA EVIDENCIA DIGITAL EN EL PROCESO PERUANO DEL DISTRITO JUDICIAL DE JUNIN, 2020.
Para Optar	:	EL TITULO PROFESIONAL DE ABOGADO
Autores	:	BRUNO GALENO OLIVARES RAMON MARIBEL MARLENE CERAS RODRIGUEZ.
Línea de Investigación	:	DESARROLLO HUMANO Y DERECHOS
Asesor	:	MG. JORGE LUIS ESPEJO TORRES
Fecha de Inicio	:	02 DE ENERO DEL 2021.
Fecha de Culminación	:	09 DE AGOSTO DEL 2021.

HUANCAYO – PERÚ

2021

Dedicatoria:

A nuestros queridos padres, por su amor, trabajo y sacrificio en todos estos años, gracias a ellos hemos logrado llegar hasta aquí. Es un privilegio ser su hij(o)a.

Los Autores

Agradecimiento

A la Universidad Peruana Los Andes, Alma Mater donde realicé mis estudios superiores y adquirí mi formación como Abogada.

A los Distinguidos Catedráticos de la Universidad, a nuestro Asesor de Tesis, nuestro reconocimiento por el apoyo al elaborar la Tesis presente, por su orientación y supervisión en la elaboración de la presente investigación y por las recomendaciones lo cual nos hizo posible poder culminar la investigación la misma que será de utilidad para la sociedad.

A los distintos abogados litigantes, fiscales y asistentes de las Fiscalía Especializada, Jueces de los diferentes Juzgados de la Corte Superior de Justicia de Junín, en materia de Procesos Judiciales de tipo penal.

Introducción

La investigación de la presente tesis "Delitos informáticos y la evidencia digital en el proceso peruano del Distrito Judicial de Junín, 2020". La función más importante que otorga la Constitución Política del Perú a los jueces y magistrados en estos días en que las tecnologías informáticas definitivamente se pueden usar para el avance de la ciencia, pero también para causar perjuicio a terceros, sustraer patrimonios, bienes, alterar sistemas de seguridad, extraer, modificar y eliminar datos. Siendo nuestro problema general: ¿Cuál es la relación que se da entre los delitos informáticos y la evidencia digital en el proceso peruano del Distrito Judicial de Junín, 2020?

El juez que se encuentra ante la decisión de un hecho ocurrido habrá de posicionarse como tercero imparcial para dar sus decisiones, de forma objetiva e independiente, la situación que le encarga la Nación.

El objetivo general, que presentamos en el presente trabajo de investigación consiste en: Determinar la relación entre los delitos informáticos y la evidencia digital en el proceso peruano del Distrito Judicial de Junín, 2020.

De esta manera nos formulándonos la Hipótesis General: Existe una relación directa y significativa entre los delitos informáticos y la evidencia digital en el proceso peruano del Distrito Judicial de Junín, 2020.

Optando por la metodología amparado en el método científico, el método analítico sintético, la hermenéutica y la exegesis. Como Tipo principal estamos centrados en la Investigación básica pura, en los niveles de investigación, exploratorio, descriptivo y correlacional, con un diseño de investigación correlacional simple. Nuestra población está conformada por la policía, fiscales, operadores auxiliares de justicia.

Siendo la estructura del trabajo de investigación el siguiente:

En el Primer Capítulo desarrollamos el Planteamiento del Problema: donde detallamos la descripción, delimitación de la realidad problemática, la formulación del problema, justificación del estudio a nivel social, teórico, metodológico y los objetivos a alcanzar.

El Segundo Capítulo se refiere al Marco Teórico: realizando la elaboración de los antecedentes, bases teóricas, el marco conceptual., marco histórico y marco legal correspondiente.

El Tercer Capítulo las Hipótesis y Variables: señalando la hipótesis general y las hipótesis específicas, así como las variables y la operacionalización de variables.

El Cuarto Capítulo se refiere a la Metodología que se ve viene utilizando en la presente investigación se detalla el método de investigación, el tipo de investigación, nivel y diseño de investigación, así también la población y muestra, las técnicas e instrumento de recolección de datos, la técnica de procesamiento, análisis de datos y los aspectos éticos de la investigación.

En el Quinto Capítulo comprende los resultados, descripción de los resultados contrastación de hipótesis, Análisis y discusión de resultados, conclusiones, recomendaciones, referencias bibliográficas y anexos.

Contenido

Dedicatoria:.....2
Agradecimiento.....3
Introducción.....4
Contenido.....6
Contenido de tablas.....9
Contenido de Figuras.....10
Resumen.....11
Abstract.....12
1.1. Descripción de la realidad problemática.....13
1.2. Delimitación del Problema.....22
1.2.1. Delimitación espacial.....22
1.2.2. Delimitación social.....22
1.2.3. Delimitación conceptual.....23
1.3. Formulación del Problema.....23
1.3.1. Problema general.....23
1.3.2. Problemas específicos.....23
1.4. Justificación de la investigación.....23
1.4.1. Justificación social.....24
1.4.2. Justificación teórica.....24
1.4.3. Justificación metodológica.....25
1.4.4. Justificación constitucional.....26
1.5. Objetivos.....26
1.5.1. Objetivo general.....26
1.5.2. Objetivos específicos.....26
Capitulo II.....27
Marco Teórico.....27
2.1. Antecedentes.....27
2.1.1. Antecedentes internacionales.....27
2.1.2. Antecedentes nacionales.....33
2.2. Bases teóricas.....38
2.2.1. Delitos informáticos.....39
2.2.2. Evidencia digital-concepto.....64
2.3. Definición Conceptual.....83
2.4. Marco histórico.....86
2.5. Marco legal.....90
2.6. Derecho comparado.....102

Capitulo III. 108
Hipótesis y Variables 108
3.1. Hipótesis 108
3.1.1. Hipótesis General. 108
3.1.2. Hipótesis Específica(s). 108
3.2 Variables. 108
3.2.1. Variable Independiente: Delitos informáticos. 108
3.2.2. Variable dependiente: Evidencia digital. 110
3.3. Operacionalización de Variables. 111
Capitulo IV. 114
Metodología 114
4.1. Método de Investigación 114
4.1.1. Método General. 114
4.1.2. Método Específico. 114
4.2. Tipo de Investigación 115
4.3. Nivel de la Investigación. 115
4.4. Diseño de la Investigación 115
4.5. Población y Muestra 116
4.5.1. Población. 116
4.5.2. Muestra. 116
4.6. Técnicas e Instrumentos de recolección de datos. 117
4.6.1 Técnicas. 117
4.6.2. Instrumentos. 118
4.7. Técnicas de procesamiento y análisis de datos 119
4.8. Aspectos éticos de la investigación 120
Capitulo V 121
Resultados 121
5.1. Descripción de resultados. 121
5.1.1. Resultados de la Variable 1: Delitos Informáticos. 121
5.1.2. Resultados de la Variable 2: Evidencia Digital. 127
5.2. Constrastación de hipótesis 131
Discusión de Resultados 135
Conclusiones 139
Recomendaciones 140
Referencias Bibliográficas 141
Anexos 148
Anexo 1: Matriz de Consistencia 149

Anexo 02: Matriz de Operacionalización de Variables 151
Anexo 03: Matriz de Operacionalización del instrumento 154
Anexo 04: Instrumento de Recolección de datos 158
Anexo 05: Confiabilidad y validez del instrumento 160
Para el instrumento de la Variable 1: Delitos Informáticos 160
Para el instrumento de la Variable 2: Evidencia Digital 161
Anexo 06: Data de Procesamiento de Datos 163
Anexo 07: Consentimiento Informado 166
Anexo 08: Evidencia (Fotos) 167
Anexo 09: Fichas de Entrevista 171
Anexo 10: Jurisprudencia 176

Contenido de tablas

Tabla 1. Delitos Informáticos 121

Tabla 2. Hurto Informático 123

Tabla 3. Fraude Informático 124

Tabla 4. Estafa Informática 125

Tabla 5. Sabotaje Informático 126

Tabla 6. Evidencia Digital 127

Tabla 7. Valor Probatorio 128

Tabla 8. Alcances de Regulación 129

Tabla 9. Información Digital 130

Tabla 10. Correlaciones entre Delitos Informáticos y Evidencia Digital 131

Tabla 11. Correlaciones entre Delitos Informáticos y Valor Probatorio 132

Tabla 12. Correlaciones entre Delitos Informáticos y Alcances de la regulación 133

Tabla 13. Correlaciones entre Delitos Informáticos y Alcances de la regulación 134

Contenido de Figuras

Figura 1. Procedimientos para el tratamiento de la evidencia 21

Figura 2 Delitos Informáticos 122

Figura 3. Hurto Informático 123

Figura 4. Fraude Informático 124

Figura 5. Estafa Informática 125

Figura 6. Sabotaje Informático 126

Figura 7. Evidencia Digital 127

Figura 8. Valor Probatorio 128

Figura 9. Alcances de Regulación 129

figura 10. Información Digital 130

Resumen

El tema de esta investigación fue Delitos Informáticos y La Evidencia Digital en el Proceso Peruano del Distrito Judicial de Junín, 2020, cuyo objetivo general fue Determinar la relación entre los delitos informáticos y la evidencia digital en el proceso peruano del Distrito Judicial de Junín, 2020. La metodología corresponde a un método científico, los métodos específicos son la observación y la experimentación, el tipo de investigación es básica, el nivel de investigación es: explorativa, descriptiva y correlacional; el diseño es el no experimental, con una muestra de 40 operadores de derecho del distrito judicial de Junín, 2020

Los resultados muestran que no existe una relación directa y significativa entre los delitos informáticos y la evidencia digital en el proceso peruano del Distrito Judicial de Junín, 2020. (p=0,952>0.05). Donde la mayoría de los operadores de derecho, consideran que el nivel en que se aplica la legislación para los delitos informáticos en el proceso peruano del distrito judicial de Junín, 2020 es medianamente suficiente (62.5%). Y la mayoría de los operadores de derecho, consideran que el nivel de evidencia digital en el proceso peruano del distrito judicial de Junín, 2020 es muy alto (40.0%).

Palabras clave: Delitos informáticos, evidencia digital, Proceso Peruano.

Los Autores

Abstract

The subject of this research was Computer Crimes and Digital Evidence in the Peruvian Process of the Junín Judicial District, 2020, whose general objective was to determine the relationship between computer crimes and digital evidence in the Peruvian process of the Junín Judicial District, 2020 The methodology corresponds to a scientific method, the specific methods are observation and experimentation, the type of research is basic, the level of research is: explorative, descriptive and correlational; the design is non-experimental, with a sample of 40 law operators from the judicial district of junin, 2020

The results show that there is no direct and significant relationship between computer crimes and digital evidence in the Peruvian process of the Junín Judicial District, 2020. ($p = 0.952 > 0.05$). Where the majority of law operators consider that the level at which the legislation for computer crimes is applied in the Peruvian process of the judicial district of Junín, 2020 is moderately sufficient (62.5%). And most of the law operators consider that the level of digital evidence in the Peruvian process of the judicial district of Junín, 2020 is very high (40.0%).

Keywords: Computer crimes, digital evidence, Peruvian Process.

The authors

Capítulo I

Planteamiento del Problema

1.1. Descripción de la realidad problemática.

Actualmente se mira o se ve que continuamente los modernos regímenes de información, las innovadoras técnicas, regímenes informáticos y específicamente las tecnologías de carácter informático ha ido progresando, donde coexisten varios versados en el asunto, quienes proyectan muchos softwares.

Puede evidenciarse como el uso o la utilización de computadoras de diferente característica, marca, tipo , dimensión, tanto en la clasificación , gestión de organizaciones empresariales, estatales, privativas en el estudio tecnológico y científica e inclusive en la ociosidad, viabiliza que la actividad informática sea indefectible y beneficiosa pero podrían ser esgrimidos por personas o individuos sin escrúpulos para realizar disímiles Delitos de carácter o de tipo Informático, ocurrencia que es producto del avance tecnológico de la informática, que se aplica actualmente en todos los quehaceres de la vida diaria.

Con el aumento y creación de las nuevas tecnologías de comunicación e interacción en la web, como redes sociales, aplicaciones y demás herramientas de comunicación digital, cada vez más se ha visto el aumento de los abusos en el uso de estos medios digitales, en tal sentido, uno de los principales problemas que trae es que personas inescrupulosas, tratan de ganarse la confianza del menor y de acceder a información esencial sobre ella para la posterior consumación del abuso, en este sentido, como producto del cambio tecnológico que ha repercutido en las diferentes formas de interacción social, antes la interacción social se orientaba exclusivamente en la interacción social física, sin embargo,

hoy en día ésta ha sido reemplazada por la interrelación de carácter o de tipo telemático y como producto de ello es que los comportamientos delictivos son aprovechados este contexto para actualizar sus actos delincuenciales.

Así, el uso de las computadoras en el contorno multisectorial principalmente en el sector financiero y de seguros, incita a la aparición de modernas maneras de crimen, de estos modernos "malhechores de computadoras". De este modo a nivel mundial la actividad informática se vuelve, en un campo extenso lleno de probabilidades de las personas incursos en estos temas para el porvenir, y no podemos negar el avance en el progreso de la sociedad actual; pero, contrariamente a lo manifestado este avance se vuelve en un elemento de "riesgo", porque incita a innovadoras maneras de criminalidad, mediante el manejo criminal de las computadoras.

Por estos razonamientos, se establecen en referencia contigua de este estudio, aquellas investigaciones interrelacionados con los delitos o crímenes de tipo informático y el amparo penal de la vida íntima. Por ello conseguiremos en la actual indagación una herramienta tecnológica de científico de provecho para los especialistas de justicia que ejerzan sobre la averiguación y juzgamiento de los diferentes delitos de tipo o de particularidad informática conformado por policías, Ministerio Público y Juzgadores en el Distrito Judicial de Junín y consecuentemente consideramos que el estudio vendrá a ser aporte para la colectividad científica con relación a la técnica computarizada.

Estas evidencias digitales, al quedar en el sistema electrónico, y muchas veces no descubiertas o en otras obtenidas en la investigación, sin prever ni garantizar los derechos a la intimidad y privacidad, tanto de la víctima como del investigado, más cuando, dichas obtenciones no son realizadas por las personas idóneas, para conservar y proteger la información para que no sea alterada, en tal sentido, es necesario hacer una investigación al

respecto, especialmente relativo al tratamiento jurídico y probatorio que se le está dando a las evidencias digitales, especialmente en los delitos contra la indemnidad y libertad sexual.

El crimen en la actualidad ya supero todos los esquemas con la llegada de la tecnología. La aparición del internet ha permitido globalizar las oportunidades para llevar a cabo estos delitos, trasladándolo a puntos impensados del planeta tierra. Este comportamiento va en incremento muy rápidamente, siendo mayores los casos que se dan día con día, convirtiéndose en un desafío tanto como para la policía y las autoridades judiciales el combatirla.

En este orden de ideas, el problema de la ciberdelincuencia ha aumentado y está desarrollando nuevos sofisticados modos de operación, es difícil descubrir las malas intenciones de personas que se aprovechan de la gran ventaja que ofrece los sistemas informáticos, frente a esta realidad el derecho penal de muchos países han quedado imposibilitados de descubrir a estos facinerosos que se ocultan de muchas formas, nuestro Código Penal tiene ciertos vacíos a pesar de las modificatorias introducidas en forma genérica en relación a la ciberdelincuencia no basta, por lo que el derecho penal requiere aplicar normas más drásticas y alta preparación al personal que se encuentra investigando estos casos. Nuestro país no está exento de esta gran responsabilidad mundial, por ende, la real importancia de esta problemática es estar a la vanguardia con las nuevas actualizaciones y los nuevos tipos de estrategias cometidas por los autores de los delitos informáticos.

Visto que tecnología de la información ha planteado nuevos desafíos y la adaptación de las profesiones a la era digital. Es decir, a nivel mundial, en todas las áreas, en todas las profesiones, como un índice de conectividad va a estar ligados a la informática y en consecuencia usaran los accesos a intemet como herramienta para estar acorde con las nuevas tecnologías.

Como acote principal se busca la especialización de índole policiaca, es por ello que tenemos en nuestro país a la DIVINDAT (División de Delitos de Alta Tecnología de la PNP), donde investigar crímenes sofisticados y la correcta recolección de evidencia es circunstancial para armar el caso y presentarlo ante los fiscales y jueces, esta es una tarea demasiado importante para los investigadores.

En esta posición una verdadera problemática de índole operática es el Volumen de datos a analizar, donde no se abastecen en lo absoluto el personal de la DIVINDAT. Esto combinado con la problemática de la cooperación entre entidades de telecomunicaciones y la Policía Nacional Policita, limitando el accionar al ser una gestión sumamente lenta. Con demasiadas barreras burocráticas.

Por otro lado, tenemos la cooperación internacional, que también no es lo suficientemente eficiente y necesita pulirse inmediatamente, para la obtención y cruce real de información y así tener la situación real del caso en concreto. Esto en un caso puede retardar el análisis y tomar demasiado tiempo en la resolución de una investigación.

Aquí, el desenvolvimiento de la Informática Forense cobra un papel protagónico. Es donde la problemática se anida. Visto que por más que se desarrolle un informe de primera por un perito informático autorizado, al ser este informe llevado al Fiscal y finalmente al Juez, por más traducción que tenga, no va ser comprendido correctamente, visto que tanto el Fiscal, como el Juez no tienen los conocimientos necesarios en informática y de esa manera hacer la correcta identificación del Autor del delito informático. Es decir, no toda la problemática está orientada a temas operativos o de naturaleza técnica, sino problemas relacionados a procedimientos, políticas, especialización, cooperación, entre otros que afectan la investigación, como el proceso judicial.

Para empezar, debemos entender que el sujeto que comete el delito no es un tipo común que sale a la calle, lo encuentran hurtando, puede ser señalado; este criminal está detrás de una cadena de números, está detrás de una red, un servidor, que maneja dispositivos que se convierten en prueba. Que estas pruebas pueden ser auto alterables, o auto destructibles, programadas anticipadamente, llegando a ser dispositivos volátiles.

Por ello nunca se va a saber a ciencia cierta que ocurre en ese dispositivo si no tiene un trato especial. Es decir, la prueba digital es muy poderosa si es correctamente obtenida, lo da todo, el cómo, el cuándo y porque se realizaron los hechos. Pero no basta con ser correctamente obtenida, sino correctamente manejada con la adecuada cadena de custodia e interpretada y es donde entran a tallar los Jueces y Fiscales.

Centrando la realidad problemática, estamos frente a un tipo de conducta indebida que usualmente queda impune, esto por la falta de preparación y conocimiento de nuestras autoridades tanto judicial como policial, las cuales les falta las herramientas y procedimientos correctos para investigar este tipo de delitos.

Por ello instrumentalizar un procedimiento o un método adecuado para manejar investigaciones relacionadas con equipos informáticos, cumpliendo con la premisa de que estas prácticas deben ser aceptadas y puestas en acción de forma universal y respetando el debido proceso en el Proceso Penal Peruano es necesario y de aplicación inmediata en vista que este comportamiento social evoluciona muy rápidamente.

Existen diferentes particularidades donde los delincuentes cibernéticos consiguen ejecutar delitos frente al régimen informático alterando los sistemas , así como ejecutar infracciones contra la pertenencia, utilizando fraude informático, sustracciones, estafas, pero asimismo se consigue realizar delitos frente a la intimidad de los individuos, entidades y el Estado, en este factor, las chicas y medianas organizaciones empresariales son las más

sensibles debido a que no refieren con un régimen de ciberseguridad, en las nubes y las plataformas.

Se ha determinado de conformidad a recientes estudios que los crímenes de carácter informático contra el patrimonio se ejecutan afectando a los individuos naturales inclusive a personas jurídicas, en la peculiaridad de estafa y actos fraudulentos de carácter informático, los equivalentes pasan desapercibido como consecuencia del trato jurídico de carácter penal que las naciones le proporcionan a estos comportamientos ilícitos, asimismo por las específicas particularidades que diferencias a estos comportamientos, como la situación de los sujetos activos los cuales poseen una gran sapiencia de gran escala en la informática, es por ello que se conocen en la actualidad de moderno o innovadores delitos de tipo informático que transitan desapercibidos siendo dificultosos de descubrimientos, peque a que son denunciados de manera continua, los papás y las mamás de los hogares se hallan impotentes en vigilar a sus descendencias que se enrolan en estas bandas criminales. Por lo que urge una mayor preparación de la Policía Nacional del Perú y los Fiscales que ejercen la investigación, en especial en nuestra incontrastable ciudad de Huancayo se viene incrementándose la ciberdelincuencia de manera alarmante, es más por los jóvenes que de manera incauta caen en sus redes de manera muy sencilla.

Se ha conseguido verificar que los progresos tecnológicos son usados o esgrimidos para favorecerse ilegalmente, intermediarios por intermedio de la reproducción de tarjeras financieras, variación o infracción de regímenes informáticos con la finalidad de favorecerse de las trasferencias de caudales o dineros ajenos por intermedio del manejo de regímenes informáticos de aseguramiento.

Según el examen bancario y económico de las disímiles naciones del universo en términos de carácter comercial, las organizaciones empresariales que no encuentran en la red

escuetamente no coexisten y conservan quebranto frente a los que se hallan dispuestos en internet, en consecuencia las interrelaciones comerciales de heterogénea naturaleza constantemente va en incremento, pero, consiguientemente la restricción de ejecutar operaciones utilizando la técnica electrónica para los robos informáticos que logren perturbar a los beneficiarios debido a que las virtuales plataformas , para materializar las transacciones es importante otorgar los archivos y claves de la tarjeta de carácter electrónico, consiguiendo ser esgrimidas los datos que se suministran o facilitan de modo sano; para que se cometan hurtos o robos de carácter sistemático del dinero o caudal de la tarjeta, o el total del dinero acumulado o ahorrado sin poder recoger el producto conseguido o el servicio que primigerniamente ha sido contratado, habiendo el beneficiario víctima del delito de estafa, debido a que se le estimuló en error al momento del ofrecimiento de un determinado servicio o bien y consiguiendo que se desglose del patrimonio.

El derecho penal vigente en la actualidad cumple un rol muy importante para sancionar los delitos informáticos, que necesita de exhaustividad y sistematicidad en la apreciación de los comportamientos que perturban bienes jurídicos que son tutelados de modo penal, o sea los bienes de todo individuo.

En nuestro país y es más en nuestra Región Centro de acuerdo a la estadística proporcionada por el Instituto Nacional de Estadística e Informática, las denuncias realizadas por los delitos informáticos en los periodos 2018 al 2020, existen muchas denuncias que llegan a las diversas comisarias, al Centro Emergencia Mujer y las Fiscalías de la ciudad de Huancayo, pero jamás son resueltos; porque se requiere de una buena y eficiente preparación de la Policía Nacional del Perú y de los Señores Fiscales.

Con las reformas interpuestas recientemente se ve que el acrecentamiento de los casos inscritos de los delitos de tipo o de carácter informático, de conformidad a las

informaciones de la Fiscalía, se ha acrecentado de modo considerable, por ello existe una multiplicidad de denuncias que han sido presentadas recientemente en el Ministerio Público , y si no se posee un correcto aspecto regulativa de modo conveniente para castigarlos penalmente, es indudable que va permanecer impune, debido que en la ley penal del Perú no coexiste un regulatorio de carácter expreso de sabotaje, estafa y hurto informático, contrariamente a lo mencionado, se ha interpuesto fraude informático como un delito de tipo o de carácter genérico, generando mayor ambigüedad interpretativa facilitando una sancionabilidad que incumba a la conducta penal de tipo o de carácter relevante y regañada por la sociedad.

El art. 8 de la Ley N° 30096 relacionados los delitos de carácter informático se tipifica un solitario modo de este tipo de delitos que va en contra del patrimonio, denominado "fraude informático", dicha norma genéricamente no consiente concretar y comprobar de modo pleno los comportamientos en el tipo penal, mediante, la subsunción del comportamiento penal. No es bastante los planteamientos que se desea conseguir, derrochándose bríos y trabajo que está realizando la PNP. (Policía Nacional**).**

Otro de los problemas a nivel nacional en el Perú , e incluso que va trasuntando a nivel internacional es la investigación y sanción de los delitos informáticos, toda vez que los ciberdelincuentes tienen la plena posibilidad de cometer actos ilícitos estando físicamente en un país del Continente europeo , puede hacer daño a la persona o empresa que se encuentra en el Continente, y lo peor es que se pueden programar ataques masivos que en tiempo real puede tener efectos en diferentes países, entonces el problema se hace viral , se hace imposible que nuestro país tendría facultades de investigar y sancionar dichos ilícitos, pues la respuesta no es nada fácil, en la medida que, sea uno o el otro país, requiere la colaboración y cooperación nacional e internacional.

Sobre este inconveniente o contrariedad ¿Qué alternativas de solución se ha planeado en el Perú?, ¿Nuestras leyes penales están adecuados para indagar y castigar los delitos informáticos en el Perú?, ¿Qué soluciones se están formulando tremendamente a pesar de coexistir pruebas digitales? éstas y otras preguntas o incógnitas requieren contestaciones perentorias, en un período donde la utilización de los regímenes informáticos es intensivo, incesante y en invariable desarrollo, y por otra parte los criminales informáticos proceden con más agresión y con factores y herramientas más sofisticados frente a la creciente vulneración de los interesados que al final resultan ser determinadas víctimas de estas malignas manifestaciones.

Figura 1. Procedimientos para el tratamiento de la evidencia

Mercosur. Principios de tratamiento de la evidencia digital.

En la ley penal del Perú no se da cumplimiento con el principio de tipicidad para el castigo o la sancionabilidad del delito de hurto de carácter informática, e igualmente en relación al sabotaje informático y estafa cibernética muy a pesar de contar con evidencias digitales , por lo que urge mayor capacitación a la Policía Nacional del Perú y a los señores Fiscales ; para coger a estos delincuentes que vienen causando grandes perjuicios en las personas y las empresas de diferentes rubros. Urge en nuestra Región Junín implementar una serie de mecanismos para derrotar la ciberdelincuencia y el tráfico de los delitos informáticos, que son un retroceso al avance científico y profesional.

1.2. Delimitación del Problema

1.2.1. Delimitación espacial.

La delimitación espacial del presente estudio constituye el medio geográfico en la que se lleva a cabo la investigación, que viene hacer la ciudad de Huancayo, situada en la Región Junín, bordeada por el anchuroso Rio Mantaro, en el corazón de nuestro país, que comprende varios despachos fiscales y judiciales por lo tanto, su alcance es Regional, es por ello que en la investigación que estamos utilizando información que corresponde a los casos de los delitos informáticos en el proceso penal y sus efectos para los delitos informáticos y la evidencia digital en el proceso peruano del Distrito Judicial de Junín, 2020.

1.2.2. Delimitación social.

La muestra que se ha considerado en la presente investigación nos presenta un nivel socioeconómico perteneciente al nivel medio y medio alto. La sociedad en su conjunto cada vez tiene más dificultades; para encontrar la verdadera justicia social, debido a ello urge analizar y combatir los delitos informáticos y la evidencia digital en el proceso peruano del Distrito Judicial de Junín, 2020. La población de la Región Junín comprende todos los estratos y a ellos va orientado nuestra investigación.

1.2.3. Delimitación conceptual.

Se abordará el tema teniendo en cuenta el punto principal en toda indagación de tipo histórico, mediante el cual se concreta en las informaciones a examinar, pero, la presente investigación no es de particularidad histórica, por lo que las informaciones que en su progreso o avance de acopia y examina conciernen a orígenes con una vejez no superior a 5 años, consiguiendo de manera justificada usar en el progreso de fuentes crecidamente arcaicas de acuerdo a su importancia de su comprendido con el inconveniente de estudio que se refiere a los delitos informáticos y la evidencia digital en el proceso peruano del Distrito Judicial de Junín, 2020

1.3. Formulación del Problema

1.3.1. Problema general.

¿Cuál es la relación que se da entre los delitos informáticos y la evidencia digital en el proceso peruano del Distrito Judicial de Junín, 2020?

1.3.2. Problemas específicos.

1.- ¿Cuál es la relación que se da entre los delitos informáticos y el valor probatorio en el proceso peruano del Distrito Judicial de Junín, 2020?

2.- ¿Cuál es la relación que se da entre los delitos informáticos y los alcances de la regulación en el proceso peruano del Distrito Judicial de Junín, 2020?

3.- ¿Cuál es la relación que se da entre los delitos informáticos y la información digital en el proceso peruano del Distrito Judicial de Junín, 2020?

1.4. Justificación de la investigación

Esta investigación parte de una preocupación constante pues se observa que en el país se hace uso indiscriminado de medios electrónicos para cometer delitos en agravio de los

menores y población vulnerable. Muchas veces se usan estos medios para no solo comunicar e informar sino también para cometer delitos o inducir a error.

Son cada vez más las personas que hacen uso de medios informáticos. Casi todos la usan y le dan múltiples funciones. Creemos también que esta investigación será de interés práctico para los operadores de justicia: jueces, fiscales, abogados, policías y público en general. Por tanto, está asegurada la justificación de esta investigación.

1.4.1. Justificación social.

El presente estudio posee una válida importancia, también de hallar una justificación en la experiencia, se ha probado, actualmente por intermedio de prácticas minuciosas, que se consigue observar una mala conducción de las convenidas motivaciones en las diferentes y variadas resoluciones de tipo o de carácter judicial como manifiestamente se halló en indiscutibles jurisprudencias basados en la relación que se da entre el tratamiento jurídico penal de los delitos informáticos y la evidencia digital en el Distrito Judicial de Junín, 2020. Según Ramos (2011). La investigación debe ser favorable en la práctica y primordial en lo teórico que ayude determinar una dificultad común o que pueda concebir una nueva conjetura. La justificación permitirá crear de manera sólida lo importante y lo relevante de dicha investigación (p. 126).

1.4.2. Justificación teórica.

La jerarquía del trato de este problema que existe dentro de la función de carácter o de tipo jurisdiccional y en los diferentes organismos donde se dispone justicia. La presente investigación se justifica teóricamente toda vez que se analizaron y describieron diversidad de teorías referidas a los delitos informáticos y la evidencia digital. Asimismo, en relación a los medios informáticos como las evidencias digitales, respeto de sus usos, impactos e

implicancias sociales, comunicacionales y jurídicas. Por tanto, la teoría respaldará nuestra investigación dándole sustento y argumento.

1.4.3. Justificación metodológica.

Este estudio se halla metodológicamente justificada, porque dentro del estudio se requerirá la utilización de las herramientas que siguen: Cuestionarios que se emplearan a los juzgadores, expertos en asuntos penales en el Distrito Judicial de Junín ,y teniendo con consideración la Matriz de consistencia de donde se derivaron las preguntas o ítems y que al final sirvió para recopilar datos al ser examinados; para tener respuestas exactas nos poseemos valernos del Programa Excel e inmediatamente se examinaran los datos en el SPSS-25 efecto de la aplicabilidad del cuestionario en que se indagó saber actos de la realidad estudiada. Asimismo, (Santos, 2013) señala que la evidencia digital es "cualquier información, que sujeta a una intervención humana u otra semejante, ha sido extraída de un medio informático" (p. 22).

Al respecto se puede señalar entonces que los delitos informáticos y evidencia digital son todo aquel dato o información que se haya extraído de un medio informático, sea por participación humana u otros instrumentos análogos. En nuestra investigación se realiza mediante enfoque cualitativo, aquí desarrollaremos un análisis exhaustivo de las fuentes documentales. Asimismo, realizaremos entrevistas a los expertos en la materia y encuestas a los sujetos implicados en la problemática. Esta investigación seguirá además una trayectoria metodológica que nos permitirá asegurar la rigurosidad académica y científica propia de una investigación a nivel de Tesis de investigación científica profesional.

1.4.4. Justificación constitucional.

La justificación Constitucional responde directamente al trabajo de nuestra investigación, que tiene el amparo de nuestra Carta Magna, debido a la constante imposición de la medida procesal más gravosa en los delitos informáticos y evidencia digital, y su consecuencia inmediata es la afectación de todo el tratamiento penal de acuerdo a la comisión del delito cometido por el ciudadano, garantizado en nuestro texto Constitucional de 1993.

1.5. Objetivos

1.5.1. Objetivo general.

Determinar la relación entre los delitos informáticos y la evidencia digital en el proceso peruano del Distrito Judicial de Junín, 2020.

1.5.2. Objetivos específicos.

1. Determinar la relación entre los delitos informáticos y el valor probatorio en el proceso peruano del Distrito Judicial de Junín, 2020.

2. Determinar la relación entre los delitos informáticos y los alcances de la regulación en el proceso peruano del Distrito Judicial de Junín, 2020.

3. Determinar la relación entre los delitos informáticos y la información digital en el proceso peruano del Distrito Judicial de Junín, 2020.

Capitulo II

Marco Teórico

2.1. Antecedentes

2.1.1. Antecedentes internacionales.

Rincón (2015) en su investigación en la ciudad de Madrid-España titulada: El delito en la cibersociedad y la justicia penal internacional. Para optar el título de doctorado, en la Universidad Complutense de Madrid; expone su conclusión: Los ciberdelitos no son sabidos por la Corte Penal de tipo do de carácter Internacional de manera accesoria, y contrariamente a lo manifestado, por ser delitos de tipo o de característica Universal, es esta instancia de nivel mundial que tiene los requerimientos para avanzar su persecución, siendo este organismo de nivel internacional quien haga su investigación, realice el juzgamiento y castigue, a partir que se haya tenido conocimiento de su hecho, donde la meta o la finalidad es la aplicabilidad del IUS PUNIENDI, ya no de un determinado país, sino de carácter o de tipo universal. (491p.).

En la investigación el autor se refiere que los ciberdelitos, conocidos como delitos universales deben ser perseguidos y castigados por la Corte Penal Internacional, coincidimos con la conclusión arribada en el sentido que estos Delitos informáticos deben ser sancionados de manera muy severa y contundente, publicándose a los autores a nivel mundial.

Abdulai (2016) realizó la investigación titulada: Determinantes del miedo a la victimización del crimen de cibernética, un estudio del fraude a la tarjeta de crédito entre estudiantes de la Universidad de Saskatchewan". Tesis que se sustentó en el departamento de sociología de la Universidad de Saskatchewan para optar el grado de magister en artes, siendo el objetivo estudiar el temor a la victimización por delito cibernético hecho entre los alumnos de la Universidad de Saskatchewan. Conclusión: Los descubrimientos de la investigación mencionan que la práctica anterior de victimización y las conductas de usanza de Internet se encuentran relacionados de modo positivo con el miedo de los alumnos y su peligro de volverse en víctimas de fraude con tarjeta crediticia.

Wang (2016) según la tesis titulada Estudio comparativo de la ciberdelincuencia en Derecho Penal: China, Estados Unidos, Inglaterra, Singapur y el Consejo de Europa", que sustentó en la Universidad Erasmo de Rotterdam para optar el Grado de Doctor, cuyo objetivo de estudio fue hacer un estudio comparativo de la ciberdelincuencia de los países China, Estados Unidos, Inglaterra, Singapur y el Consejo de Europa. entre sus terminaciones marca que China posee un régimen de regulación de escalas de carácter compuestos en malas operaciones cibernéticas, con instrumentales primordiales y sus dos rectificaciones. No obstante, ambos de las 2 correcciones han acrecentado el alcance de los delitos de tipo o de característica informática. La Corrección (VII) se informó el 2009 para envolver la grieta que se alzó junto con la progresiva popularidad de las computadoras de tipo personal. Posteriormente a estos cambios, se determinó la guía o dirección de 2 puntos. Este punto de vista u orientación realiza una clara diferenciación entre el delito informático de carácter o de tipo genuino y los delitos acostumbrados otorgados por computadoras. Indica que en los Estados Unidos de Norte América.

En los delitos relacionados a la piratería los estudiosos de las leyes prefieren una apariencia y resguardan la computadora de una manera segura; y, en otros delitos como el tráfico de dispositivos, se fundamentan en la conceptualización de datos e informaciones. Partiendo de estas 2 consideraciones, el gentío puede hallar la ley de los EE.UU. sobre la ciberdelincuencia que se tramitan en la experiencia judicial. El país de Inglaterra elige por meter innovadoras o modernos dispositivos que se proceda con las legítimas ciberdelincuencias y se fundamentan en sus leyes penales que existen que tratan de los delitos acostumbrados entregados por computadoras. Discurre que Singapur ha sido dinámico en la divulgación y reforma de su legislación relacionados a Abusos Informáticos. El punto de vista o la orientación que se dio es considerable por las duplicaciones o reproducciones en el interior de los dispositivos legales.

Se asimiló de la Ley Inglesa de manera inicial sobre el mal uso de ordenadores y metió los delitos de piratería que en la actualidad están en contra de la seguridad de las fichas o archivos.

Asimismo, en el mismo período, se tomó los dispositivos normativos semejantes del país de Canadá y metió los delitos de piratería, el cual se concentra en la cabida de proceso y almacenaje del ordenador o de la computadora, como la usanza de los servicios de tipo o de carácter informático no autorizado. En conclusión, ultima que el progreso de modernas técnicas de las informaciones y dispositivos virtuales ofreciendo modernas encrucijadas para los delitos. El primero, proporciona crímenes acostumbrados como el llamado o denominado fraude, y el segundo, crea innovadores delitos como la piratería. Los delitos acostumbrados prestados por ordenadores y los nuevos delitos creados por ordenadores son denominados en la actualidad como cibercrimen.

Nuestra coincidencia con el autor del trabajo de investigación en nuestro medio el ciberdelincuente es muy sagaz lo que busca es desestabilizar los programas y sistemas informáticos de las personas y las empresas, igual aquí en el Perú existen muchos integrantes del cibercrimen, el gran problema es que no estamos preparados; para afrontar a estos delincuentes, nuestro Código Penal es insuficiente; para castigar con rigor a estos delincuentes, urge modificar nuestras leyes para castigar y destruir a estas bandas organizadas.

Alanezi (2015) en su investigación titulada Las percepciones de fraude en línea y el impacto sobre las contramedidas para el control del fraude en línea en las instituciones financieras de Arabia Saudí". Tesis que sustentó en la facultad de diseño de ingeniería y ciencias físicas, Departamento de Ciencias de la Computación de la Universidad Brunel de London, para optar el grado de doctor en filosofía, el objetivo de investigación fue inspeccionar las contramedidas usadas por las entidades de tipo financiero en Arabia Saudita y la influencia de las contramedidas de manera personal y agrupada en el examen y preventivas del fraude en línea en Arabia Saudita. Indica que los individuos son dependientes de Internet; la probabilidad de ser trasgredido por los hackers y embaucadores está ascendiendo, fundamentalmente en las adquisiciones en línea y la banca se llevan a consideración mediante ordenadores individuales o dispositivos de tipo móvil. Su importancia se ha visto que en las zonas donde hay una gran escala de adopción de la comercialización electrónica. Por ello, las argumentaciones es que las medidas tomadas no son suficientes o no han logrado confrontar con eficiencia todas las dificultades a raíz de la situación organizacional y climática de la nación. El estudio fue de orientación cualitativa, tecnológica de entrevista a versados, la población de investigación estuvo formada por 12 magnas instituciones bancarias de Arabia Saudita, circunscribiendo financieras y otras entidades que facilitan servicios bancarios. Definitivamente, el estudioso finiquita que la expansión de la comercialización electrónica y las diligencias en línea son atendidas por

Arabia Saudita con el sostén activo de las financieras, por el preámbulo de servicios tecnológicos de las informaciones para los servicios crediticios.

Pero, este crecimiento de las acciones en línea y utilizando las informaciones financieras asimismo crean congruencias y lagos explotadas por ciertos estafadores en línea, lo que secuela en la merma de más de doscientos 200 millones de dólares el 2010 y 2020. El estudio asemejó un acrecentamiento en la estafa en línea, como consecuencia a la gran unión de financieras.

En nuestro país el Perú, específicamente en nuestra ciudad de Huancayo ocurre lo que está aconteciendo en otras latitudes. El fraude en línea ha sido descrito como una epidemia que se viene extendiendo a la mayoría de las actividades en línea, así como el Covid 19 viene invadiendo todo el mundo, por ello es importante aplicar el tratamiento penal de los delitos informáticos y evidencia digital, causando en nuestro país caos y subdesarrollo en las inversiones financieras y las empresas no desean invertir por el temor de fracasar.

González (2013) en su investigación titulada Delincuencia informática: daños informáticos del artículo 264 del Código Penal y propuesta de Reforma sustentada en la Facultad de Derecho, Departamento de Derecho Penal de la Universidad Complutense de Madrid-España, para optar el grado de doctor, tuvo como objetivo de indagación brindar un enfoque total del crimen informático actualmente, concentrando su examen en el cuadro legal de los delitos de perjuicios informáticos, quienes posteriormente de un examen íntegro de los disímiles delitos informáticos, tipologías y peculiaridades, entre sus primordiales conclusiones indica: Que el crecimiento rápido de la ciberdelincuencia es indiscutible, tratándose de un hecho nuevo cuyas experiencias de carácter delictivo pretende la intervención de los disímiles países, que conjuntamente posee una particularidad inherente al perfeccionamiento técnico; la tecnología adelanta a un compás acelerado, y este arquetipo de

delitos, su visión y su progreso poseen, en refutación con el lento adelanto del Derecho en el trato jurídico de tipo penal de los delitos cibernéticos o informáticos y la prueba virtual. Menciona que la informática posee una propiedad de tipo trasnacional, y que nunca es bastante la regulación de carácter protectora en un país único, no coexiste alejamiento en la regulación eficientemente en los remanentes de países.

De acuerdo a nuestra investigación que venimos realizando el análisis de los delitos informáticos y la evidencia digital ,venimos incrementando nuestros saberes previos en efecto lo desarrollado en otros países enriquece nuestros conocimientos, pero a la vez el Desarrollo de la Tecnología Informática se está convirtiendo en un mal necesario; porque la niñez y juventud requieren de aprender cada vez más acerca de la informática, su control es casi imposible, por el crecimiento vertiginoso demostrado.

Piccirilli (2015) en su investigación titulada Protocolos a aplicar en la forensia informática en el marco de las nuevas tecnologías (Pericia – Forensia y Cibercrimen) que sustentó en la Facultad de Informática de la Universidad Nacional de La Plata-Argentina; para optar el grado de doctor en ciencias informáticas, el objetivo es desarrollar una proposición de carácter metodológico para precisar protocolos a esgrimir en la usanza del foro empleada al tratamiento de la certeza virtual, en el cuadro de las modernas técnicas informáticas. Por ello, el autor ejecuta un examen del experimento desde el secuestro hasta el examen de carácter pericial conveniente, la orientación metodológica usando en el perfeccionamiento de la investigación es analítico, marca que es suficientemente grande la escala de la ciberdelincuencia, y que el invariable avance del delito es la que induce crear modernas intranquilidades.

En la ciudad de Huancayo de acuerdo a los estudios hechos por el autor asimismo se tienen que tener en consideración el moderno ejemplo legal de los peritajes en general y en

específico los peritajes de tipo informático, es ineludible envolver los desatinos de los procesos actuales, por lo que es forzoso referir con una formalidad presente y auténtico para enfrentar los retos técnicos concernientes a las modernas técnicas informáticas. Como indica o menciona el autor del estudio es importante e ineludible establecer un órgano de asesoramiento técnico pericial de tipo informático.

2.1.2. Antecedentes nacionales.

Nuñez (2016) en su tesis Derecho de identidad digital en internet, presentada en la Universidad Nacional Mayor de San Marcos-Perú; para optar el grado de Doctor nos señala: La verificación o comprobación digital es el proceso que, mediante factores seguros y conocidos, consiente fijar una equivalencia con explícitas propiedades a un individuo en concreto, esto es a la demostración de datos que confirman que un sujeto es ciertamente el individuo que usa de internet, de modo indubitablemente. Para interponerse en los 4 grandiosos procedimientos: la gobernabilidad electrónica, la instrucción o educación electrónica, las empresas electrónicas y la comercialización electrónicas precisamos poseer una identificación digital que sea inequívoca, evitando la utilización no adecuada de variadas identidades y la substitución de identidad. Para ello el Derecho de tipo o de carácter Informático debe aprovecharse de modo sistemático y afín. El Estado es el garante de la caracterización de los individuos garantizando la identificación de cada uno de ellos. El derecho de identificación virtual debe ser protegidos por la ley de cada Estado, respetando en internet los derechos de todos los individuos.

En efecto en Huancayo se puede notar que es casi imposible identificar la identidad digital de las personas que hacen uso del internet, falta mucho control y organización; para atrapar a los delincuentes que cometen Ceberdelincuencia, es necesario organizarnos, sistemáticamente.

Parra (2016) en su tesis titulada Proyecto legal para un esquema nacional de Ciber Seguridad. Para optar el Título de Abogado en la Universidad de San Martín de Porres de Lima; concluye: La carencia de proyección en este asunto podría causar que los países sean víctima cada vez altas y malos sucesos, los cuales consiguen ser obviados mediante una labor coordinada y de manera previa, ajustando la técnica al moderno contexto en la que el ciber sitio viene a ser parte de la vida diaria tanto del país como de las poblaciones.

Hemos hallado prueba de agresiones cibernéticos al Estado peruano, materializándose de esta manera el contexto de vulneración en la que nos hallamos, sabiendo, los perjuicios no han sido de gran dimensión, eso no asevera que en el porvenir las agresiones que el Perú recoja logren alcanzar a producir superiores perjuicios. (p. 150)

De acuerdo a nuestra investigación el aporte del autor de la presente investigación efectivamente en nuestra ciudad en general se encuentra desprotegido por el aumento de la ciberdelincuencia, por ello a nivel de todo el mundo urge que nos organicemos y conformemos un solo organismo, se elabore y ejecute un Esquema Nacional de Ciberseguridad; para enfrentar a estos delincuentes que vienen causando enormes desequilibrios, social, económico y político.

Sánchez (2017) en su investigación titulada Adopción de estrategias de ciberseguridad en la protección de la información en la oficina de economía del ejército, San Borja- 2017 sustentada en la Escuela de Posgrado del Instituto Científico Tecnológico del Ejército "General de División Edgardo Mercado Jarrín", para optar el grado académico de magister en ingeniería de sistemas de armas, cuyo objetivo es establecer de qué modo la toma de estrategias de ciberseguridad impacta en la defensa de las informaciones en el departamento de Economía del Ejército teniendo una población de investigación a treinta (30) oficiales, cuarenta (40) técnicos y suboficiales y ciento ochenta (180) empleados civiles, poseyendo una muestra de ciento cincuenta y dos (152) colaboradores, en la que usó como técnica de

investigación la encuesta. El tipo teórico con diseño descriptivo, nivel de estudio descriptivo y explicativo. Se concluye: Que la toma de tácticas de ciberseguridad influye de manera importante en la protección de las informaciones en la Oficina de Economía del Ejército, y asimismo en esta misma unidad castrense no hay planes de defensa contra ciberterrotistas y se colocan en realización y que los puntos de conexión con las que posee el Ejército no son de novísima generación, por lo que no se encuentra totalmente garantizada la protección de la variación de las informaciones.

Alarcón & Barrera (2016) en sus Tesis titulada Uso de internet y delitos informáticos en los estudiantes de primer semestre de la Universidad Pedagógica y Tecnológica de Colombia, Sede Seccional Sogamoso 2016, sustentada en la Escuela de Posgrado de la Universidad Privada Norbert Wiener para optar el grado académico de maestro en informática educativa tuvieron como objetivo es establecer la interrelación de la utilización del internet con los delitos de tipo o de carácter informático en los alumnos de primer semestre de la Universidad de Colombia, Seccional Sogamoso, 2016, para ello se usaron el tipo de estudio básico, de enfoque cuantitativo, nivel correlacional, y el diseño correlacional, cuya muestra de sesenta (60) alumnos. La técnica usada fue la encuesta y su concerniente instrumento con treinta y seis (36) interrogantes. En conclusión, diremos que la utilización del internet que involucra las competencias de información por destreza y factores sociales se interrelacionan con el acto delictivo de carácter informático.

Tenorio & Tuesta (2012) en su tesis titulada Legislación del secreto bancario y su relación con el delito de hurto informático de dinero mediante la violación de claves secretas, Iquitos- 2010, que sustentaron en la Escuela de Posgrado “José Torres Vásquez” de la Universidad Nacional de la Amazonía Peruana, para optar el grado académico de magister en derecho y ciencias penales, cuyo objetivo fue establecer cómo impacta la regla de la ley

del secreto financiero en el acrecentamiento del crimen de hurto de caudales mediante el uso informático esto es violando las claves secretas, en Iquitos el 2010, teniendo como población de investigación a los beneficiarios que fueron burócratas, víctimas, militares, representantes legales, burócratas de INDECOPI, el nivel de estudio fue correlacional, diseño correlacional. Como técnica la encuesta. Entre las transcendentales conclusiones menciona que la ley del secreto financiero peruano, no es conforme con el adelanto técnico y el acrecentamiento del crimen cibernético, también menciona que el secreto financiero es un impedimento en la indagación del delito de hurto de caudales a nivel informático debido a que como todos sabemos el secreto bancario es levantado de modo exclusivo mediante orden judicial en procedimientos concretos, influyendo en la ilegalidad del autor del crimen de hurto informático de caudal, agregando de que en la actualidad no existe ninguna entidad que tenga anotaciones estadísticas de los actos delictivos relacionados con el hurto de caudal a las cuentas de los consumidores de las instituciones bancarias, con el modo de trasgresión de las secretas claves.

En nuestro país y en especial en Huancayo y la Región Junín, según el autor de la investigación coincidimos que es necesario preparar a toda la población con la finalidad de buscar la mayor protección posible del secreto bancario y de las inversiones que requiere proteger sus ahorros de manera muy sistemática; que se logra con educación generalizada y capacitación permanente.

Espinoza (2017) en la tesis titulada Derecho penal informático: deslegitimación del poder punitivo en la sociedad de control, que sustentó en la Facultad de Ciencias Jurídicas y Políticas de la Universidad Nacional del Altiplano-Puno; para optar el título profesional de Abogado, tuvo como objetivo fue precisar el Derecho Penal Informático, usándose la teoría o doctrina jurídica. Siendo los métodos utilizados sintético e inductivo, indica que el Derecho

Penal informático posee por esencia de investigación la legislación penal, así como la seguridad jurídica relacionados a los crímenes informáticos, cuyo fin es bajar el poder de cuidado del poder punible y se determina por ser vengativo, oficial y legal; los delitos informáticos son de carácter inclusive internacional y pluridisciplinarios. El científico pide que se expresen proposiciones de tipo legal de conformidad a los basamentos de carácter internacional de Derechos Humanos sobre cuidado de la comunicación y fundar fiscalías especialistas en técnicas de comunicación y comunicativas.

De conformidad autor del presente estudio nosotros asimismo ultimamos que se deben enunciar una serie de proposiciones legales de conformidad a los fundamentos de carácter internacional de DD.HH. sobre cuidado de las comunicaciones y establecer Fiscalías Especialistas en Tecnologías de Informaciones y Comunicaciones de novísima generación; con el impar propósito de vivir dispuestos contra el cibercrimen.

> Sequeiros (2016) en la tesis titulada Vacíos legales que imposibilitan la sanción de los delitos informáticos en el Nuevo Código Penal Peruano-2015 sustentada en la Facultad de Derecho y Ciencias Políticas de la Universidad de Huánuco; para tener el Título de Abogado, tuvo como meta de investigación establecer qué vacíos legislativas en el NCPP y en sus legislaciones suplementarias no posibilitan el castigo de los delitos informático dentro del Estado peruano el 2015, la muestra estuvo formada por sesenta (60) Fiscales. Tipo básico, de enfoque cualitativa, se esgrimió como técnica la encuesta. Conclusión, como consecuencia de la naturaleza digital de los delitos o crímenes informáticos, estos delitos perseguidos por la justicia penal se logran o consiguen volverse imprecisos al momento de ser tipificados.

El autor de la investigación dentro de sus conclusiones también incide que la naturaleza virtual de los delitos informáticos se vuelve confusos en su tipificación, pero es urgente que se

prepare a la población de la Región Junín, para contrarrestar las malas acciones de los ciberdelincuentes y así evitar que cometan los delitos informáticos contra el patrimonio.

2.2. Bases teóricas

En esta parte de la investigación partiendo de nuestra realidad la Región Junín, específicamente la ciudad de Huancayo, emporio comercial del Estado peruano, se muestran y despliegan ciertas doctrinas o dogmáticas, importantes con relación o en asociación al trato jurídico penal de los crímenes de carácter informático (estafa, fraude), así igualmente en las certidumbres o probanzas virtuales.

Desde el invento de los ordenadores o computadoras y su ulterior implementación de las mallas informáticas, internet y otros regímenes informáticos, el derecho se advirtió necesario a regularizar elementos asociados a la informática no obstante en modo atrasado, en los numerosos contornos y fundamentalmente en el contorno comercial, pero, lo es asimismo la insuficiencia de regulación en el contorno penal porque el comportamiento ahí creadas no son toleradas por la sociedad de esta manera nació el derecho informático y privativamente el derecho penal informático, dada la insuficiencia de castigar comportamientos que perturban bienes jurídicos de tipo penal que son importantes.

Para desenvolver el estudio se necesitan dogmáticas determinadas. Por esto se provendrá a verificar o comprobar ciertos conceptos conexos al argumento de estudio, los que serán esenciales durante el procedimiento del estudio, es por esto que es significativo establecer el perfeccionamiento del cuadro doctrinario o dogmático en el interior del estudio. (Ñaupas, Mejía, Novoa, & Villagómez, 2014) menciona que cuanto más superior es la superioridad de doctrinas o dogmáticas de carácter científico más hacedero será, para el

estudioso, esbozar el cuadro doctrinario del estudio, parte esencial del proyecto de estudio y prontamente la enunciación de las hipótesis. Por ejemplo, no se consigue estudiar sobre el impacto importante de las habilidades pedagógicas en el atributo de la instrucción sin saber de buena tinta la doctrina de manejos pedagógicos y los propios manejos pedagógicas efectuadas en el interior de un tiempo definitivo (p.49). Es decir, el investigador expone su conocimiento de índole teórica y científica en base a las teorías antecedidas. Por ende, se considera que nadie va poder investigar un problema donde no exista una base teórica o se desconozca.

2.2.1. Delitos informáticos.

El avance de las Tecnologías de información y comunicación ha tratado significativas permutaciones a la sociedad, aplaza de manera terrible a la que sabíamos de buena tinta hace quince (15) años detrás. Estas variaciones son metódicas y vertiginosos. Creando poseer enfoques imperecederos de la constante manera de vida. El ser humano se acomoda a las variaciones, arrogarse a estas modernas técnicas y la emplea diariamente, para su usanza en favor de la sociedad, esto es legítimo mientras este trabajo no quebrante los derechos de terceros individuos, es una acción lícita, que puede ser desarrollada sin mayor implicancia.

Lamentablemente contrario a esto el internet y los medios electrónicos son usados como medio delictivo o es objeto de vulneración que puedan afectar y generar perjuicio en la sociedad, este fenómeno debe ser sancionado. A este tipo de comportamientos dañinos se les denomina delitos informáticos, cibercrimen o ciberdelitos.

Según Rayon & Gomez (2014) "Se entiende por Ciberdelito o Cibercrimen" a cualquier tipo de transgresión de carácter punible, donde se implica un aparato informático logre ser acabado para el cometido del delito. (p. 211).

El fenómeno informático ha dado pie a que las organizaciones criminales adquieran estas nuevas tecnologías y lo apliquen para la realización de sus crímenes. Aquí también observamos que el comportamiento del sujeto activo que realiza la acción es de una persona especializada en Tecnologías de la Información, son redes delictivas con alto grado de capacitación. Los cuales tienen constantemente vulnerada la Ciberseguridad.

Para Gerke (2014) "El Ciberdelito y la Ciberseguridad son aspectos que no pueden considerarse separados en un entorno interconectado. Esto queda demostrado en la Resolución de la Asamblea General de las Naciones Unidas de 2010 sobre la Ciberseguridad se aborda el Ciberdelito (p.3). Esto debido a que los Delitos informáticos tiene una connotación mundial, visto que el Ciberespacio no tiene una jurisdicción establecida y el uso de estas Tecnologías se ha globalizado, es decir se utiliza la misma tecnología tanto en el Perú como en China, el acceso y la transferencia de información es igual en todas las partes del Planeta.

En la actualidad estamos frente a un desafío enorme para combatir al delito informático, el problema de su persecución está centrada en llegar a obtener la identificación correcta de los autores eso incluyendo la ausencia de una cooperación eficaz. Por otro lado, para muchos autores el Cibercrimen es más rentable que el tráfico de drogas, moviendo millones de dólares anuales. Quinteros (2014). Manifiesta que la jurisdicción respecto a los Delitos informáticos en el ciberespacio es "planetario", por ende, la ubicación territorial de los autores y de proveedores de servicios son muchos. Por ende, enfoca que la problemática central de los Delitos informáticos no está en la ausencia de tipificación, ni jurisdicción sino en la determinación de un tribunal que pueda juzgar estos delitos (2014, p.186).

El Dr. Edwar Domínguez Fernández en su conferencia “cibernética y delitos informáticos” realizado el 23 de mayo del presente año en el Poder Judicial del Perú, denomino a los Delitos Informáticos como aquellas conductas que se dirigen a chasquear los

procedimientos de conectores de seguridad, esto es penetraciones a ordenadores o métodos de datas con la utilización ilegal una clave de accessibilidad, comportamientos de carácter típico que exclusivamente consiguen ser realizados mediante la técnica nueva o la tecnología moderna", siendo esta denominación la más cercana a la realidad en nuestro país.

2.2.1.1. La clasificación de los delitos informáticos. Consideramos que puede ser utilizado cómo medio o como objeto material. Zegarra (2015) menciona que como medio se encuentran las conductas criminales que se valen de las computadores e internet, como método o medio de la comisión del ilícito (p.111). Cabe explicar que la clasificación de uso como instrumento es para llegar a realizar los actos delictivos, siendo en muchos casos los delitos convencionales los que finalmente desean realizarse. También explica Zegarra (2015) que como objeto real se encuadran los comportamientos delictuales que van encaminadas contra los ordenadores, esto significa, contrariamente a la informática. Por ello varios autores tienen algunas actitudes sobre la codificación de las contravenciones o crímenes informáticos. (Gil, 2007)

Los Delitos de tipo o de carácter Informático como herramienta clasifican a inseparables comportamiento delictuales que usan un conjunto de técnicas de comunicación e informaciones. Para la materialización del delito, como modelo en la adulteración de documentaciones vía informatizada (trabajos, tarjetas de crédito, talones de recibos o cheques), o en la variabilidad de los referidos pasivos y activos en el contexto de la contabilidad de la organización empresarial. Como asimismo en el bosquejo y fingimiento de delitos de tipo convencional (estafa, asesinato, fraudes financieros, violación a menores de edad) O lectura, robo y copia de informaciones de carácter confidencial, transformación de datos tanto en el ingreso como en la escapatoria de informaciones. Asimismo, en el beneficio no debido de un código para ingresar un sistema, ingreso de instrucción no apropiada que logren perjudicar al sistema, cambio referente al destino de chicas cuantías de caudal hacia

una cuenta simulada. Usanza no acreditada de Programaciones de cómputo. Variación de marcha de sistemas mediante la utilización ilegal de virus de tipo o de carácter informático. Ingreso de instrucciones que inciten obstáculos en la razón endógena de los programas. Obtener informaciones residuales prensada en papel prontamente de la realización de labores. Accesibilidad a zonas informatizadas no acreditada.

Porque los delitos de carácter informático como finalidad marcan los comportamientos delictuales que van encaminadas contra los ordenadores o programas como existencia de tipo físico.

Esto significa, en un modelo de programación educacional que causan bloqueo general al sistema. Exclusión de la base de datos de la organización empresarial. Variación en los asalariados de un negocio. Pérdida de programas por diferentes métodos. Perjuicio o menoscabo a la memoria. Deterioro de los focos neurálgicos computados.

De conformidad a los anteriormente manifestados que el bien jurídico que se tutela es la honestidad técnica, la seguridad de los medios que compongan el régimen de tipo o de carácter informático. Gracias a la codificación hemos sistematizado ciertos comportamientos que logren ser apreciadas como Delitos de tipo informático.

2.2.1.2. Tipicidad de los delitos informáticos. Para López (2013) la tipicidad es aquella cualidad atribuida a la conducta que se adecua al tipo penal. (p.53). Es decir, esta conducta nos indica que el hecho está inmerso en la ley penal, siendo la descripción que la contiene. Distinguiendo por un lado el tipo objetivo que está guiada a la actividad, como la tipología subjetiva guiada al dolo. Con lo planteado el estudioso de leyes aparte de efectuar un diagnóstico objetivo de la conducta de carácter punible, argumentando y fundamentando la particularidad ilícita que consiga poseer.

La tipicidad de los delitos informáticos busca establecer el tipo penal para delitos desarrollados con el fenómeno de las tecnologías informáticas, la cual ha generado una nueva forma de criminalidad.

2.2.1.3. Tipicidad objetiva de los delitos informáticos. La tipicidad de carácter objetiva indaga establecer de manera exacta la lesión elaborada a un bien jurídico, entonces debe ser estimada como la diligencia de explícito sujeto y cuando este impacto es solo fruto de la escueta causa.

Ejecutamos un examen de la ley y hallamos que la tipicidad objetiva de los denominados crímenes informáticos está establecida por innegables particularidades como es el objeto del crimen o del delito, como sujetos intervinientes, la acción típica, el re causalidad, la imputabilidad material u objetiva y los factores descriptivos legales en correspondencia a este tipo de Delitos.

De acuerdo a Hurtado (2005). El objeto del delito es la cosa o el individuo encima de la cual cae la actividad del delito (p.413). En lo concerniente a delitos de tipo o de carácter informático poseemos delitos contra sistemas y datos de carácter informático, infracciones informáticas contra independencia sexual, crímenes informáticos contra la propiedad o el patrimonio y contravenciones informáticos frente a la fe pública.

Según Hurtado (2005). La acción típica es el componente fundamental del semblante objetivo del tipo legal radica en un suceso elegido por el verbo primordial del diagnóstico legal (p.413). Esto significa, es la operación que es explicada con el verbo superior en la normatividad vigente.

En lo concerniente a delitos de tipo o de carácter informático contra la autonomía sexual, sus verbos superiores es que mediante el internet instituye relación con una persona

menor de edad. Aquí solamente la mínima intencionalidad de conectarse ya es castigada. Sobre los crimines o trasgresiones contra el secreto a la intimidad o a la comunicación la acción típica se concreta o se plasma en el caso de que de modo deliberado e ilegal intercepta datos de tipo o de carácter informático en trasmisiones no gubernamentales.

El verbo director en los denominados delitos de característica informática sería el que de manera deliberada e ilegalmente bosquejada mete, trastorna, borra, elimina y copia datos informáticos en menoscabo de otros. De la misma manera los delitos contra la fe pública de tipo informático la acción típica es por intermedio de técnicas de la información suplantando la identificación de un individuo o una persona jurídica.

Para Hurtado (2005). El nexo de causalidad es originado como una cualidad de arquetipo jurídico y social (p.421). Donde se pesquisa la ligazón entre el acto delincuencial y el autor del acto delictuoso. Por esto es importante que haya una correspondencia entre secuela y acción. En los crímenes o delitos de tipo informático establecer el vínculo causal está subordinada a la prueba virtual, el cual es la herramienta con el que se logra ubicar al sujeto activo en el acto delincuencial.

Según Hurtado (2005) la Imputación objetiva es la consecuencia al autor del acto delictuoso es establecida en el cuadro del tipo legal (p.421). Sea castigado al sujeto activo por la acción de carácter delictivo. En los delitos de carácter o de tipo informático las penalidades fluctúan entre 1 a 8 años.

Para Hurtado (2005) los factores legales y descriptivos son autónomos uno del otro, estando los aspectos o factores descriptivos las definiciones tomados del léxico habitual que están referido a establecido actos que deben ser materia de comprobación por el Juzgador. Por otro lado, los factores legales están referido a aquellos elementos que solamente logren ser establecidos mediante una evaluación de valor (p.411). En lo que se refiere a los crímenes o a

los actos delincuencias de carácter informático se posee el establecimiento correcto del verbo superior o directos para comprender los factores descriptivos de estos actos delincuenciales que son especiales.

2.2.1.4. Sujetos de los delitos informáticos. Tenemos que considerar como elemento a todo aquel que busca ser parte de un todo. En nuestro caso quienes están implicados en el hecho delictivo. Donde tenemos al sujeto activo y a sujeto pasivo.

Para (Gil, 2007) el sujeto activo a la persona que comete ciberdelito con unas características específicas que no representa al delincuente común o clásico. Visto que estos tienen las habilidades para manejar los sistemas informáticos y usualmente por la posición de índole laboral en la que se pueda encontrar, se sitúan en zonas estratégicas para la facilidad en el acceso de información delicada, o bien son hábiles en el uso de sistemas informatizados. Por ende, no se trata del delincuente común, que puede ser fácilmente identificado, estos trabajan tras una cadena de números y su capacidad de comprensión es binaria. Tiene un alto grado de nivel de aptitudes que en la actualidad aun genera una seria de controversias en cuanto a la ética y al acceso a la educación sobre estos conocimientos proponiendo la limitación de los mismos.

Entre ellos tenemos a los denominados Hackers, que en muchos casos pueden ser los denominados hackers éticos que son contratados por empresas para que vulneren e ingresen a sus sistemas y medir su grado de error para posteriori mejorar, en cambio los Crackers son generalmente personas que se introducen a sistemas informáticos remotos con la intención de destruir datos alterar el sistema, etc.

Por otro lado, tenemos al sujeto pasivo que está constituido por la víctima del delito, siendo el que genera una conducta sea de acción u omisión en referencia al sujeto activo, y se incrementa en los casos de delitos informáticos. De todas maneras, gracias a este elemento

podemos llegar a conocer los variados ilícitos que pueden cometer los delincuentes informáticos, siendo en muchas veces descubiertos casuísticamente debido al desconocimiento del modus operandi.

2.2.1.5. Delincuente informático. Considerado como el autor del ciberdelito, en muchas ocasiones el sujeto activo en la realización del delito. Giménez (2011) considera que los delincuentes informáticos, usualmente son personas de confianza, es decir suelen ser empleados que tienen acceso al sistema informático. Según las estadísticas, más del 90% de los delitos son cometidos por los usuarios del sistema y los otros por técnicos informáticos (p.104).

Dándonos a comprender que, según el fenómeno, el comportamiento de los delincuentes informáticos, son personas que acceden muy fácilmente a estos sistemas, saben sus deficiencias y debilidades. Conocen perfectamente como romper la seguridad y bajar la información necesaria o destruirla.

2.2.1.6. Tipicidad subjetiva de los delitos informáticos. La tipicidad subjetiva es todo aquello que es interrelacionada con la culpabilidad y el dolo. Según Hurtado (2005) Componía el universo interno del autor para ser usadas para observar el delito. (p.447). Por ello es concluyente como elemento para conocer si es una operación típica o diferente. En los delitos de tipo o de carácter informático es ineludible establecer la intencionalidad o el modo en la que se hizo este acto de carácter delictivo para estar al tanto si ajusta en el tipo penal, visto que hay actos delincuenciales de mera diligencia y delitos de secuela. Pero por modelo referido al art. 5 de la Ley de delitos informáticos posee una predisposición endógena trascendental ya que personifica un componente subjetivo diferente al dolo, ya que describe un propósito específico del agente.

Villavicencio (2014) dice que un acto delincuencial de resultado cortado, debido a que el agente acosa un resultado ulterior el cual es conseguir prueba pornográfica o algún acto de carácter sexual (p.49). Es la intencionalidad de aproximación ya estimado delito siendo el sujeto pasivo uno que congregue una sucesión de contextos, por modelo ser persona menor de edad.

2.2.1.7 Delitos informáticos. El adelanto de las TIC's ha conseguido significativas variaciones a la sociedad, prorroga a la que sabíamos hace quince (15) años detrás. Estas variaciones son metódicos y vertiginosos. Creando poseer visiones arregladas de la manera de vida de modo constante. El ser humano dentro de nuestra realidad es adaptable a las variaciones, arroga estas modernas técnicas y la emplea diariamente, para su usanza en favor de la sociedad en su conjunto, esto es legítimo en tanto esta operación no quebrante los derechos de los ajenos individuos, es una acción lícita, que puede ser desarrollada sin mayor implicancia.

Lamentablemente contrario a esto el internet y los medios electrónicos son usados como medio delictivo o es objeto de vulneración que puedan afectar y generar perjuicio en la sociedad, este fenómeno debe ser sancionado. A este tipo de comportamientos dañinos se les denomina delitos informáticos, cibercrimen o ciberdelitos.

Según Rayon & Gomez (2014) ciberdelito o cibercrimen cualquier tipo o caracterítica de infracciones punibles, en el que se implica un aparato informático consiga ser utilizado para la actuación del delito (p.211).

El fenómeno informático ha dado pie a que las organizaciones criminales adquieran estas nuevas tecnologías y lo apliquen para la realización de sus crímenes. Aquí también observamos que el comportamiento del sujeto activo que realiza la acción es de una persona especializada en tecnologías de la información, son redes delictivas con alto grado de capacitación. Los cuales tienen constantemente vulnerada la ciberseguridad.

Para Gerke (2014) "el ciberdelito y la ciberseguridad son aspectos que no pueden considerarse separados en un entorno interconectado. Esto queda demostrado en la resolución de la Asamblea General de las Naciones Unidas de 2010 sobre la Ciberseguridad se aborda el Ciberdelito"(p.3). Esto debido a que los delitos informáticos tiene una connotación mundial, visto que el ciberespacio no tiene una jurisdicción establecida y el uso de estas tecnologías se ha globalizado, es decir se utiliza la misma tecnología tanto en perú como en china, el acceso y la transferencia de información es igual en todas las partes del planeta.

En la actualidad estamos frente a un desafío enorme para combatir al Delito lnformatico, el problema de su persecución está centrada en llegar a obtener la identificación correcta de los autores eso incluyendo la ausencia de una cooperación eficaz. Por otro lado para muchos autores el cibercrimen es más rentable que el tráfico de drogas, moviendo millones de dólares anuales. Quinteros (2014) manifiesta que la jurisdicción respecto a los Delitos informáticos en el ciberespacio es planetario, por ende la ubicación territorial de los autores y de proveedores de servicios son muchos. Por ende enfoca que la problemática central de los Delitos informáticos no está en la ausencia de tipificación, ni jurisdicción sino en la determinación de un tribunal que pueda juzgar estos delitos.

El Dr. Edwar Domínguez Fernández en su Conferencia Cibernética y Delitos Informáticos realizado el 23 de Mayo del presente año en el Poder Judicial del Perú, denomino a los Delitos Informáticos como aquellas conductas que se dirigen a las personas.

Así se posee en el contorno nacional el CP, la ley de delitos de carácter o de tipo informático y sus modificaciones, asimismo, a nivel universal se posee a las leyes de los demás Estados, y en específico al ajuste de cibercriminalidad, impar concierto de trascendencia mundial, ajustable a las naciones que firmaron, pero, como dicho Acuerdo es

de 2001, se debe considerar el comprendido y ser sometidos a efectos de actualización de conformidad al contexto real de las naciones actualmente.

2.2.1.8. Uso de la información en el internet. La introducción de innovadores técnicas comunicativas y de la información variaron el modelaje de los regímenes de todo el universo en cuanto a la conducción y accesibilidad de las comunicaciones e informaciones, habiendo un enérgico impacto en el contorno escolar, en el procedimiento de unificación de los recursos técnicos y la visión de las Web 2.0 que concibieron viable el tránsito de las escenas en la internet donde se mostraron disímiles formas de la accesibilidad a la información de disímiles grados o escalas como páginas Web de carácter comercial, bibliotecas digitales, para el estudio y el aporte al discernimiento, pero en el instituto se vio una pared coligada a los contextos, prácticos y fes del mando de las informaciones.

Con el invento del internet en otras diligencias el año 1969, se edificó una malla que ha reconocido combinar la comunicación y la técnica, los ordenadores ya vivían, pero la utilización de manera exclusiva para trabajos que proporcionaran o suministrarán la labor del hombre (Aguilar & Said, 2010)

La utilización del internet a través del tiempo ascendió de modo grandioso a nivel de todo el planeta, volviéndose en un instrumento de gran jerarquía, proporcionada de caracteres que han facilitado el avance de las técnicas. (Sánchez, 2014).

De acuerdo a (Fullan, 1999, citado en Kozma, 2003, p. 129), se describe a estos contextos como un “reto al trasladar una invención es responder en un nuevo contexto las situaciones que crearon la probable innovación, no la modernización propia”, lo que se vuelve en cómo es viable que estos desconocidos escenarios sean arrogados en las conductas humanas en este asunto los alumnos.

La conceptualización de la utilización del internet, solitariamente no posee sentido, pero en el caso donde se ve la interrelación con las consecuencias de la labor obtiene excelencia, al respecto Anderson (2008) describe a las experiencias con TIC que manifiestan ser seguras ya sea en la instrucción de cursos o en el progreso de modernas destrezas concernientes con la urgencia de Internet y las peticiones de la sociedad del discernimiento, denominadas frecuentemente competitividades siglo XXI (p.6).

La accesibilidad de las informaciones y la utilización que esta reiterada en producción y aprendizaje, involucra un punto de vista en el control de las informaciones, UNESCO (2008) denominado "la alfabetización virtual" para instruir a los alumnos y pobladores en conjunto para la usanza de las nuevas tecnologías y ayudar el perfeccionamiento social, mejorando la producción económica y la cuestión educativa.

La utilización de las diferentes tecnologías y el beneficio del progreso del pensar de manera autónoma y creativo el alumno poseerá que ser competente de solucionar dificultades con confianza y gestionar su oportuno amaestramiento a lo largo de la existencia (OCDE, 2001).

Claro está que todo esto coadyuva un grupo de competitividades informacionales que otorgan en las labores, educatividad comunal y la vida social, circunscribiendo habilidades de administración de información y la cabida de ejecutar juicios sobre la importancia y la confiabilidad al indagar en el campo de Internet (ibídem, p.15).

Para ultimar es significativo que en el contorno escolar la usanza del internet y se irradien en las acciones tanto de profesores como de alumnos, contexto que deberá realizarse reuniendo las competitividades informacionales que le proporcionarán al alumno la cabida y las instrumentales importantes para la dirección de las informaciones si se arrogara metodologías para acrecentar el adeudo, el comportamiento ético, por lo tanto variará los

efectos de carácter nocivo de la usanza no apropiada del internet y reducir los peligros a los que se muestran los alumnos en los centros universitarios y en el cuadro jurídico de la ley de Colombia cuando se trata de imitación, estafa.

SITES (2006) menciona que “la alineación didáctica del pedagogo al utilizar las TIC en su instrucción es céntrico para tener excelentes consecuencias en cláusulas de habilidades de las informaciones”, (p.7). Por ello es básico suministrar al alumno las suficientes sapiencias y desplegar sus habilidades al esgrimir los recursos técnicos. La eficiencia y la eficacia se alcanza cuando este contexto o esta realidad facilita accesibilidad a una clase excelente esbozada y la conformidad de instruirse de modos desemejantes. (Chapman & Malhck, 2004)

Los tratadistas Osborne & Hennessy (2003) mencionan que el “docente efectúa un punto de vista crítico para utilizar el TIC con resultados transformadores relacionados a la instrucción de las sabidurías”. Mediante capacitaciones sobre el escogimiento de informaciones, examen y comentario y productividad de una moderna sapiencia creado de las informaciones a la que tuvieron accesibilidad por intermedio del internet.

Suscitar la utilización de las TICS en el salón de clases, se entiende ser un manejo complicado adentro de la insuficiencia de desplegar destrezas informáticas y el afianzamiento de un área privativa de amaestramiento y la unificación de la técnica como sustento para conseguir metas curriculares.

El “Consorcio de Habilidades Indispensables para el Siglo XXl” y su pensamiento de jerarquizar estas destrezas en:

Habilidades de comunicabilidad e informaciones: Alfabetismo en diferentes medios y destrezas de comunicación. Destrezas de idea y de solucionabilidad de dificultades: Idea de

tipo crítico y tendencia sistémica, identificación, enunciación y solucionabilidad de dificultades, la creación intelectual.

Destrezas personales y de independencia: Destrezas personales y de ayuda e Independencia.

2.2.1.9 El uso del Internet y las competencias informacionales. Por ello el perfeccionamiento de competencias de caracteres o de tipos informacionales son importantes para la administración de la información y la usanza de fuentes que proporcionen la indagación y recobro de informaciones, se compone en un dispositivo de modo o manera indefectible para conservarse renovado y ser competidor en la sociedad en que actualmente vivimos.

Según el planteamiento de Alvarado (2009) en el esclarecimiento de competencias de carácter informacional en 4 modos planteadas a conocer: (a) potencializante, son las ideas del sujeto sobre el discernimiento y la manera de alcanzar a saber; (b) virtualizante, verifica el motivo que mueve al sujeto a proceder y que se declaran en los argumentos para ejecutar y persistir en un trabajo; (c) actualizante, es la sapiencia del sujeto sobre la indagación de informaciones. y; (d) realizante, se enuncia cómo comunica la producción que realiza desde esta, (p.7). La sabiduría de la información guía sus actividades hacia el aprendizaje y enseñanza en información delimitada y exacta, de modo que la valoración de los aprendizajes se concentra en las sapiencias adquiridas.” (Montiel-Overall, 2007).

La competitividad informacional es una experiencia con dimensión didáctica y social; y el énfasis se halla centrado en la interrelación que existe entre su perfeccionamiento y la alineación de un sujeto de carácter o de tipo social que tenga la capacidad de ocupar con conciencia, la multiplicidad y complicación de factores formativas que median la accesibilidad a la información equivalente. (González y Barbosa, 2013, p.109).

Tejada y Tobón (2006). A la competencia, son las mañas, cualidades, capacidades, que se necesitan para la utilización de la información de manera creativa, moral y fructífera.

Ferreira & Dudziak (2004). Extienden las dimensiones de la acometida de las competencias informacionales, subraya la categoría de la alfabetización virtual en este procedimiento, y el perfeccionamiento de los procedimientos de carácter o de tipo cognitivo relacionado, mencionan la importancia de conservar el establecimiento de enlaces entre las destrezas, las sapiencias y los valores edificados por la persona o el individuo en el procedimiento de formarse competente (p.14).

De tal modo que las destrezas para la usanza del internet pretenden de un excelente perfeccionamiento o de las competencias informacionales en los colegios, es esencial instruir de modo premeditado y metódico, esgrimiendo tácticamente las modernas tecnologías, de tal manera que se direccione las informaciones, y apoyar a que la información se transfigure en sapiencia (Becerril & Badia, 2013).

Según Markless y Streatfield, (2016). Las competencias por habilidades Son:

Competencia 1. Mostrarse conforme la insuficiencia de información: Mostrarse de acuerdo la insuficiencia de información es conocer precisar de un modo exacto y claro qué información se requiere y cuál es el fin de la indagación. Implica la sapiencia previa, qué se sabe sobre del asunto o si, contrariamente, es la inicial vez que se oye.

Competencia 2. Delimitar la información: es conocer verificar las excelentes fuentes según la insuficiencia de información, edificar un conjunto de frases clave usando una táctica de indagación sistemática.

Competencia 3. Organizar la información: es establecer y catalogar la información limitada, para elegir la más oportuna para el estudio. Es constituir y proporcionar un determinado sentido a la información recobrada.

Competencia 4. Evaluar la información: Valorar la investigación y sus fuentes de manera crítica es establecer esta información y poseer la calificación para apreciarlo según su novedad, realidad y oportunidad, al similar que la fuente en el que viene. (Association of College & Research Libraries (ACRL), 2016).

Competencia 5. Usar la información: Quiere decir apropiarse lo que se ha asimilado; para crear moderno discernimiento, y emplear de manera crítica para la solución de dificultades.

Competencia 6. Compartir la información: es informar de manera moral y legal, mediante una constante diversidad de conformaciones; mencionando e indicando en forma conveniente; reformando la información para desemejantes designios.

Tal situación o contexto de relaciones interviene como central de referencia de las maneras de apropiarse de la información que poseen sitio mediante, la accesibilidad, valorar y forjar usanza de esta, y que dicen los argumentos formativos en los que estuvieron edificadas (p. 651).

En el procedimiento del amaestramiento el sujeto cataliza varios conocimientos y por intermedio de estos saberes consiguen transformar las conveniencias de descubrir el planeta y asimismo de variar ideas, desde la óptica la usanza ética de las informaciones es tremendamente significativo ya que la persona maneja la información de conformidad a su razón ética con relación a lo científico, es así que Martín & Birke (2004). Quienes conceptualizan la moral científica como una descendencia de la ética empleada que investiga las dificultades y las derivaciones de la mala ética de tipo o de carácter científico.

El acrecentamiento de actos inciertos con el manejo de la información es parte de las competencias informacionales y de acuerdo a Brazuelo & Gallego (2014). La imitación de documentaciones como acción de tipo o de carácter intencional posee 3 dimensiones: valores particulares, retribuciones de autor, y retribuciones individuales y colectivos. (p. 97)

Sobre los comportamientos no éticas con la información Canto & Benois (2009), como indagación ejecutada en la Universidad de Yucatán, concluye que los comportamientos no ética de alumnos son: imitación, carencia de espíritu para laborar en grupo, presentar antivalores, reproducir o formar trampa, mostrar inconvenientes morales en su interrelación con otras dificultades éticos con los educadores, ser independiente, dificultades éticos asociados con la carrera profesional, carencia de principios; y dificultades éticos asociados con la indagación. (ps. 207-223).

Lo que indica que los valores se han transformado de modo impresionante, siendo perjudiciales para la instrucción y la sociedad en su conjunto, así se hace reseña a que es significativo meditar las implicancias a escala institucional. (Martín & Birke, 2004).

Sujeto activo, según Garrido (1992). Es aquel que efectúa totalmente o una porción de la acción detallada por un tipo de carácter penal, estos individuos que realizan los delitos Informáticos tienen algunas particularidades que no muestran el común denominador de los malhechores, o sea son delincuentes hábiles en la conducción de regímenes informáticos y que por contextos inciden en delitos varias veces por analfabetismo.

De acuerdo a Hernández (1997). Referente al sujeto pasivo menciona que es el individuo titular del bien jurídico que la ley resguarda y donde recae la acción típica del sujeto activo (p. 22)

López, López, & Jerónimo (2017). Mencionaron que al equivalente que viven una gran cuantía de delitos de carácter o tipo informático, asimismo coexisten una extensa cantidad de criminales informáticos, dentro de este campo se le reconoce a los versados en seguridad informática con el vocablo de hacker, ósea el individuo que utiliza su destreza para conseguir accesibilidad virtual o informática sin que esta persona sea autorizado a los registros informáticos, pero debemos tomar en consideración que existe una codificación de los hackers, la originaria es el hacker con una prenda blanca y el segundo es el hacker prenda negra.

Pero, si se recurre a los versados informáticos (Aggarwal, Arora, Ghai, & Poonam (2014) hallamos una diversidad de tipos de hackers, así tenemos:

- Script Lidies.

Son los denominados aspirantes piratas a ser hacker.

- Los estafadores (Scammers).

Estos hackers remiten los correos electrónicos falsificados para las agraviadas como recompensas de lotería.

- Grupos de hackers (Hacker Groups).

Estos hackers son concertados por los organismos estatales para situar a experimento la seguridad y manipular los casos relacionados directamente con el fraude.

- Los suplantadores de identidad (Phishers).

Se requiere información íntima mediante Internet de modo engañoso con la finalidad de tener de modo fraudulento dígitos o cifras de tarjetas de crédito, señales u otros datos particulares.

Grupos comerciales, políticas y religiosas.

Este tipo de hackers no se interesan por los beneficios bancarios, sino están dedicado al avance del software malintencionado para aspectos políticos. Así tenemos como un ejemplo el gusano *Stuxnet* que acometió el programa de tipo o de carácter atómico de la nación de Irán de sus infraestructuras nucleares.

- Insiders.

Estos atacadores son apreciados como los de mayor peligrosidad, ya que habitan en el interior de la organización. Ellos poseen el discernimiento de todos los pormenores de una organización y embisten cómodamente la seguridad de la organización empresarial y crean y descomponen el sistema.

- Amenaza persistente avanzada (APT) Agentes (Advanced Persistent Threat *(*APT) Agents)

Este conjunto de hackers se encuentra responsabilizados de agresiones tremendamente concretas hechos por conjuntos financiados por Estados muy organizados.

- Hackers sombrero blanco (White Hat Hackers).

Se refiere a los hackers éticos que se centralizan para obtener de los métodos de TI. El vocablo hacker de sombrero blanco se esgrime de manera común para referir a los hackers que frecuentan de penetrar en los sistemas con la finalidad de apoyar los que ostentan la propiedad del sistema, creándoles fallas dentro de la seguridad.

- Hackers sombrero negro (Black Hat Hackers).

Es un individuo que complica la seguridad de un método informático sin tener la anuencia del dueño.

- Hackers de sombrero gris (Grey Hat Hackers).

Está referido a un hacker versado que a veces procede de manera legal.

Sobre el examen del tipo penal de delitos de carácter informático, puntualizamos:

A. Acerca de la conducta típica. Es la vulnerabilidad de la seguridad de los métodos informáticos para el beneficio no debido, ya sea despojando bienes, valoraciones y datos.

B. Sujeto activos. Denominados delitos de cuello blanco, porque el sujeto activo tiene que tener sapiencias técnicas de carácter informático avanzadas, entonces se deduce que es casi improbable que un individuo corriente pueda realizar o materializar este delito, si poseer sapiencias bastantes de cómo marchan los sistemas informáticos.

C. Sujeto pasivo. Son cualquier persona natural, o persona jurídica como financieras, bancos, cajas de ahorro que usan métodos automatizados de información, ordinariamente acoplados o unidos a otros dispositivos o regímenes exteriores. (Alcívar, Domenech y Ortiz, 2015, p. 46).

D. Bien jurídico protegido. Mayer (2017) el bien jurídico protegido en los crímenes de carácter informático es la información, es la comprendida en un régimen de trato automatizado de la propia, secuela difícil conciliar con un esclarecimiento del interés privilegiado que bosqueje al libre perfeccionamiento del individuo en un Estado de carácter demócrata de derecho (p. 240).

E. Tipicidad subjetiva. Los delitos informáticos, por su ambiente y la escala de sapiencia que pretende, son crímenes puramente dolosos, pero, asimismo se podría materializar por culpabilidad, donde no poseía ninguna intencionalidad de la realización del ilícito penal, pero, quebranta el bien jurídico protegido de manera penal.

F. Móvil o motivo de los delincuentes informáticos. Las estimulaciones que consiga estimular actos delincuenciales a los cibercriminales son heterogéneas.

G. Delitos informáticos. Citando a Aggarwal, Arora, Ghai, & Poonam (2014). Logramos marcar que la piratería de tipo o de carácter informático es el beneficio no debido del software mediante la reproducción ilegal de programas y repartición de los bienes predestinados al pase al legítimo. (p. 49).

Los delitos de tipo o de carácter informático constituyente de estudio son: delitos de sabotaje, estafa. Fraude, hurto.

- Hurto informático.

La incautación de software y datos: aquí el sujeto tiene accesibilidad a un ordenador ajeno o a la reunión de otro beneficiario, donde retira registros informáticos, con la realización del copiado, para inmediatamente almacenar ese comprendido en un soporte propio. (Alcívar, Domenech, & Ortiz, 2015).

- Hurtos sistemáticos.

Es hurto sistemático es sustraer continuamente el patrimonio de un individuo por medio de regímenes informáticos, como es el hecho de las cuentas financieras o crediticias, donde el malhechor, al tener las claves de aseguramiento de las tarjetas crediticias saca el dinero que se hallan en dicha tarjeta, trasladando a otra cuenta.

Hurto de valores.

En la época informática como la actúa no solo los caudales representado por el dinero pueden ser la meta de hurto informático, sino asimismo otros bienes, en su mayor parte, valores virtuales de importancia patrimonial, debido a que con el progreso de la técnica se está encaminando a una fase de cero papeles, porque los títulos valores son factibles de ser objeto de hurto informático.

G. Fraude informático. Es la accesibilidad de modo indebido a los registros y datos con valor patrimonial quitando las medidas de aseguramiento de métodos, mallas y medios electromagnéticos con la finalidad de beneficiarse de manera indebida de los productos del hecho de carácter fraudulento.

Vásquez, Regalado & Guadron (2017). Demarcan que el fraude de tipo o de carácter informático es el daño o menoscabo patrimonial que se crea a otro individuo mediante el manejo de datos informáticos o la interrupción en el trabajo de un sistema informático, cuyo fin es la tenencia ilegal de un provecho económico. (p. 65).

El fraude informático, de conformidad al art. 8 del Convenio de Budapest sanciona penalmente las acciones ilegales que crean perjuicio patrimonial al individuo utilizando borrados, alteraciones o eliminación de datos informáticos; o se interfiere la buena funcionabilidad del sistema informático, donde el sujeto activo intercede con la intencionalidad de carácter doloso la obtención de manera ilegal un provecho económico.

H. Delitos informáticos ligados a los medios de pago electrónico. Los adelantos del conjunto de técnicas informáticas y las comunicaciones, así como el incremento de las sistematizaciones comerciales en Internet tienden a propiciar el brotamiento de modernas

comportamiento de carácter fraudulento concernientes con la utilización de instrumentales de desembolso electrónico. (Rico, 2013).

I. Fraude al sistema. Por esclarecimiento, se refiere que en el delito denominado fraude el sujeto activo del mencionado delito, a discrepancia de la estafa informática, miente a las herramientas de seguridad de los sistemas de tipo o de carácter informático.

J. Fraude en los datos. En el fraude en los datos, el malhechor informático lo que efectúa o ejecuta es la alteración de los archivos o los datos de las técnicas informáticas para aprovecharse económicamente, así tenemos como ejemplo, la accesibilidad a una plataforma de comercialización en línea, dejando de lado las medidas de aseguramiento del sistema, con el fin de cambiar los datos como el importe, el costo, etc.

j. Estafa informática. Es un comportamiento de carácter delictivo que radica en la utilización de los medios informáticos con la finalidad de mentir a la víctima y quitarle su patrimonio y el beneficio no debido del sujeto activo de dicha propiedad.

k. Estafa a través de instrumentos de pago. No obstante, la estafa informática se halla rectamente interrelacionada con el asunto de los medios electrónicos de desembolso, con la meta o la finalidad de lucrarse económicamente con un traspaso no consentido de un activo de tipo o de carácter patrimonial, y asimismo se han mostrado inconvenientes para cuadrar las operaciones de desembolso de tipo o de carácter fraudulento elaboradas mediante Internet o manejo informático. (Rico, 2013).

Wall (2015). Indica que algunas estadísticas exponen de manera clara que el Internet es cada vez crecidamente usado por los delincuentes que estafan para sustraer ilegalmente grandiosas cuantías de caudales o dinero de las agraviadas, o por los hackers para tener información y obstaculizar los procedimientos de organizaciones empresariales de carácter privado y empresas estatales. (p. 76).

M. Modalidades de estafa phreaking. Es el método más viejo en el interior de los nombrados o llamados ciberdelitos, radica en meterse en las redes de telecomunicaciones para ejecutar o efectual llamadas de carácter telefónico a largo recorrido esgrimiendo la cuenta que no le pertenece (ajena). (Alcívar, Domenech y Ortiz, 2015, p. 46).

N. Phishing. En el *phishing*, consiste en la captación de carácter ilícito de datos se materializa este hecho ilegal mediante el envío intensivo de correos de carácter electrónico que aparentan la identificación de una entidad bancaria con el objetivo de requerir a los que reciben los datos de sus concernientes tarjetas, fundamentando varios motivos (fomento de bienes, intervención en concursos, dificultades de seguridad). (Rico, 2013).

Es un modo de fraude de tipo o de carácter informático esbozada con la meta o con el fin sustraerle de modo ilegal su patrimonio o de robarle la identificación al sujeto pasivo. El delito radica o reside en tener información relacionado a cifras de tarjetas crediticias, señales, informaciones de cuentas bancarias por medio de astucias. (Imbaquingo, *et. al*, 2016, p. 140).

Ñ. Pharming. La tecnología usada en el *pharming* asimismo envía a los interesados a páginas Web que son definitivamente falsos, instituidas en forma análoga a las de las instituciones financieras con el fin de realizar captaciones los datos de los consumidores. En estos casos, el proceso no se acarrea con el transporte intensivo de correos electrónicos; la accesibilidad de manera indebida se ocasiona por una vulneración en el *Domain Name System* o en el de los aparatos de los consumidores, que consiente al bandido redirigir el nombre de potestad de la institución a una página Web que aparentemente es igual. (Rico, 2013).

O. Sabotaje informático. Bashir y Khalique (2016). Cree que el sabotaje es la utilización no acreditado de infraestructuras informáticas, modificación o pérdida de

información, sabotaje registro de datos y el bandolerismo en contra de un régimen informático. Los ordenadores deben ser protegidos de sabotajes para obviar cualquier inconveniecia (, p. 16).

También, Alcívar, Domenech & Ortiz (2015). Indican que el sabotaje de tipo o de carácter informático Involucra que el "delincuente" recobre o busque destruir el foco de cómputos almacenados en las computadoras. Se muestra como conductas más usuales y de más gravedad en el contorno político. (p. 45).

El vocablo sabotaje informático se concibe como las prontitudes encaminadas a producir menoscabos en el software de un sistema informático (Herrera, 2018)

El sabotaje informático; reside o radica en borrar, eliminar o cambiar sin autorización datos de los ordenadores con la intencionalidad de entorpecer la función normal del sistema, que se sabe de manera común como el virus de carácter o de tipo informático. (Villavicencio, 2014).

P. Destrucción de datos. El sabotaje informático posee una peculiaridad, es que la materialización de este delito involucra la pérdida, variación, que se haga al sistema, software no permitiendo de esa manera maniobrar con las idénticas potencialidades, creando de esa manera, grandiosas mermas en la agraviada.

Q. Alteración de datos. Asimismo, el sabotaje de tipo o de carácter informático, también, involucra el proceso ilegal de alteración de los datos de los sistemas con el fin de crear perjuicios de carácter económico en la agraviada.

R. Medidas de prevención. Debe haber un proceso de bloqueo de la cuenta financiera si se esgrime la tarjeta crediticia en un sitio donde no te hayas, pero, sino está arraigándose

la transaccionabilidad en un sitio donde no se encuentra o no se halla el celular o el teléfono del dueño de la tarjeta.

Se debe comprobar que la página web, sea verdadero, esto, comprobando el dominio, las medidas de aseguramiento y otros índices.

Debe comprobar la mesura, certificaciones y toda información pertinente a la autenticidad de los diferentes ofrecimientos que se observa en las redes, plataformas de comercialización electrónica ignorados y en caso de ser sabidos comprobar o confirmar que no se encuentre clonada, y preferentemente digitar directa y manualmente la ruta.

2.2.2. Evidencia digital-concepto.

Al respecto Santos (2013) citando a Casey define que la evidencia digital es "todo aquel dato que pueda establecer que un delito se haya ejecutado o que la misma puede también enlazar entre el crimen y su víctima, el autor del delito, los partícipes, cómplices, etc. (p. 22).

Sobre este punto se puede inferir que la evidencia digital es todo aquel dato que nos proporciona toda la información necesaria, así como también aquel que nos establece cuando un crimen sea ejecutada o consumado y la relación que hubiera con éste, con el autor del delito, sus cómplices y los partícipes, entre otros. Es desde luego, que la evidencia digital se conciba en el campo del derecho penal como aquel que recolecta o almacena datos sobre lo ocurrido en un contexto determinado.

Asimismo, Santos (2013). Citando al Manual de directrices para la dirección de pruebas refieren que la evidencia digital es "cualquier información, que sujeta a una intervención humana u otra semejante, ha sido extraída de un medio informático" (p. 22). Al respecto se puede señalar entonces que la evidencia digital es todo aquel dato o información

que se haya extraído de un medio informático, sea por participación humana u otros instrumentos análogos.

Bajo esos criterios citados se puede señalar que las evidencias digitales son aquellas informaciones o datos extraídos de soportes informáticos por el ser humano u otro análogo para su tratamiento o revisión correspondiente. Cabe, asimismo señalar que el tratamiento de los datos del sistema informativo se sustenta en la búsqueda de la verdad, lo cual desde luego es un reto muy importante para aclarar y consolidar un acto u hecho como cierta.

Asimismo, se ha sostenido que la evidencia digital es todo aquel dato que ha sido registrada, almacenada, creada y mantenida en aparatos o instrumentos electrónicos o sistemas computarizados y que las mismas pueden contener diferentes formas, tales como imágenes, audios, voces, textos entre otros aspectos que pueden ser utilizadas como evidencias en procesos en la que se discutan determinados casos que se requieran de ella.

En palabras más sencillas, la evidencia digital busca de alguna manera darle valor legal a la información encriptado en ella y ser admitida en el proceso previamente que ella haya sido sometida de un estudio o investigación por parte de expertos científicos, forenses o peritos especialistas a corroborar su autenticidad.

2.2.2.1. Características de las evidencias digitales. Citamos algunas características más importantes referido a las evidencias digitales, entre ellas están:

A. Volatil. se describe especialmente, a que una porción de la información se halla en conectores de almacenaje transitoria y que la mayor parte del software presentes son bosquejados con un croquis multipropósito, produciendo la reescritura invariable de los conectores de almacenaje de carácter temporal, conjuntamente al apagar el ordenador se extravía toda la información. (Santos, 2013).

Por su estructura, programación y comprendido está capacitado para alterar fácilmente y de modo poco predecible; esto involucra variaciones en su designación, pormenores y datos que consiguieron haber habido instrumentales en la materialización de un acto de carácter delictual. (Escobar, 2017).

B. Duplicable. Esta particularidad presume que la prueba virtual consigue ser reproducida o copiada de modo exacto y se consigue obtener un duplicado para ser analizada como si fuese el propio original. Esto frecuentemente se realiza para no manipular los originales y obviar el peligro de perjudicarlos (Santos, 2013, p. 23)

Es apto de reproducirse de modo o de manera similar que el registro original, lo que entorpece u obstaculiza varias veces particularizar de manera objetiva su inicio; ya que, no obstante, esta persista acumulada por modelo un instrumento virtual sujeto a certidumbre en un conector USB, requiere de un conector con capacidad para el procesamiento de texto lo que involucra que su inicio es ignorado y su autor desconocido (Escobar, 2017, p.32)

C. Borrable. Se señala que es borrable porque la información o dato contenido en el sistema computarizado o cualquiera que fuese similar a ella, esta puede ser de manera perfecta eliminada por quienes manipulan el sistema o la información. De modo tal que la información o dato siempre estarán sujetas o susceptibles de ser anuladas o suprimidas.

D. Anónimo. Es anónima en el sentido de que la información o datos almacenados no reporta autor o autores de manera determinada y especifica. Así pues, las evidencias digitales serán siempre anónimas por cuanto las páginas, redes, documentos electrónicos entre otros no nos proporcionarán la autoría de la misma.

Realizar una identificación a la persona que ha cometido un delito informático por modelo enreda una complicada red de sapiencias técnicas y uso de la razón informática ya que

la prueba digital en su manera originaria, esto significa, datos digitales consigue sufrir designaciones de tipo ilimitado por lo que no esencialmente cualesquiera características de su comprendido describen con plena seguridad al autor de dichas informaciones; por lo que al instante de su cogida debe ser considerado desconocida ya que secuela en cláusulas sencillas improbable establecer la autoría a escueta investigación de una certeza digital (Escobar, 2017, pp. 31-32).

E. Remplazable. Esta característica se refiere que la información o datos digitales pueden ser sustituidos por otros datos o informaciones al sistema computadorizado o electrónicos. En ese sentido el remplazo de los datos y en general de toda la información contenida en ella puede ser susceptible de sufrir la situación de otros datos que no sea la misma.

G. Alterable y manipulable. Esta característica hace referencia básicamente a que las evidencias digítales pueden ser perfectamente alterables y manipulados por el hombre. Así pues, dichas evidencias estarán sujetas a ser cambadas o trastocadas respecto a su estado originalidad, sus características esenciales, entre otros aspectos similares y de la misma pudiendo ser también perfectamente cambiadas, trabajadas, alteradas ya sea con la mano y mediante el uso de instrumentos.

H. De la admisibilidad de la evidencia digital.

Para que una evidencia digital tenga un valor legal y que esta sea plenamente aceptada por la comunidad científica, forense o a nivel del peritaje donde deben de cumplirse ciertos aspectos. Así, señalamos los criterios de admisibilidad de las evidencias digitales las mismas que se clasifican en lo siguiente:

I. Autenticidad. Insinúa enseñar a los justiciables que la certidumbre ha sido formada e inscrita en los espacios interrelacionados con el caso, especialmente en el suceso del probable

ilícito o sitios instituidos en la actividad de levantamiento de seguridad (Macuchapi, 2014, p. 34)

A contraste de los medios no virtuales, en los virtuales se exhibe un sistema volátil y alta cabida de manejo. Por esta lógica es significativo una aclaración que es indefectible comprobar la legitimidad de los ensayos mostrados en medios virtuales antípodas a los no virtuales (Zuccardi y Gutiérrez, 2006, p. 10).

Bajo esos criterios señalados por los autores podemos señalar que la autenticidad devendrá a ser autentica siempre y cuando cumpla con ciertos parámetros como demostrar de manera exacta los hechos ocurridos deben haber sido generadas y registradas en el lugar que se hay efectuado los sucesos o evento delictual.

Del mismo modo también hacer constar que la evidencia digital tiene que establecer que los hechos que reflejan en los instrumentos digitales se hayan efectuado en la realidad, esto es, corresponder o pertenecer a la realidad y descartase reflejos o modificaciones que se pudieran haber podido realizar al respecto. Así pues, con la autenticidad se busca la originalidad de los datos y la información encriptado en un sistema computarizada o electrónica.

J. Confiabilidad. Este término nos indica si, de modo o de manera efectiva, los factores o aspectos demostrativos contribuidos comienzan de fuentes que son verosímiles y comprobables y que mantienen factores de los abogados o del Ministerio Público en el procedimiento que se persigue (Macuchapi, 2014)

Se menciona de manera seria y responsable que los registros de acontecimientos de seguridad son confidenciales y certeros si proceden de fuentes que son verosímiles y fidedignos. Para experimentar esto, se debe poseer con una construcción de automatización en

excelente función, la cual explique que los que crea posee un modo o una manera confiable de ser reconocidos, recogidos, acumulados y comprobados. (Zuccardi y Gutiérrez, 2006).

En ese sentido, la confiabilidad de las evidencias digitales se sustenta en el hecho de que ella precisamente no ha sido trastocada y que la misma se encontraba en perfectas condiciones de funcionamiento o que al menos estaba funcionando correctamente al momento que la información o dato contenida haya sido recibida, almacenada y generada para las pruebas correspondientes.

Así pues, este criterio nos señala que efectivamente para que la evidencia sea admitida tiene que provenir de fuentes debidamente creíble y verificable, pero para determinar que ella sea creíble o verificable es necesario que precisamente pasen a pruebas que determinen que realmente la fuente proporcionada está en correcto funcionamiento y desde luego identificar la credibilidad o al menos generar que tiene forma de ser confiable.

K. Suficiencia de las pruebas. Es la presentación de toda la prueba o certeza necesaria para avanzar el caso, esta particularidad, al similar que las preliminares, es elemento crítico de triunfo en las indagaciones en procedimientos judiciales. Con periodicidad o asiduidad la carencia de evidencias o carencia de factores o aspectos de carácter probatorio produce la demora o finalización de procedimiento (Macuchapi, 2014, p. 35)

Este es punto muy controvertido en el sentido de interrogarnos ¿hasta qué punto la prueba o la información es confiable? Desde que la información proporcionada este completa o basta que ello sea tan evidente o suficiente para determinar que precisamente la evidencia digital es suficiente en la medida que ello otorgue información o corrobore el hecho, o en todo caso dependiendo de la satisfacción que nos pueda proporcionar la información para poder inferir que ella es veraz.

Así pues, la suficiencia de la prueba supone que la evidencia digital puesta a prueba efectivamente cumpla con los parámetros suficientes que ella contiene, esto es, no debe de carecer de datos trascendentales que contrastados con el hecho delictivo no concuerden o que la información no son las adecuadas para corroborar o analizar el evento o suceso que se quiere esclarecer.

L. Evidencia digital. En la actualidad es estimada como una innovadora o moderna fuente probatoria o de certeza. Y debido a que no es usada exclusivamente para delito de tipo o de carácter informático, sino asimismo para la agudeza en delitos de carácter convencional.

Para Gercke (2014) la categoría de la prueba virtual es importante para los delitos de carácter informático ya que circunscribe 2 etapas, la primera que se tiene que aplicar a la designada tecnología forense informática, referido al examen de tipo sistemático sobre los aparatos TI de ese modo hallar la prueba virtual. Coexistiendo como la segunda etapa la dación y muestra de la certidumbre examinada y aprendida en los juzgados, tomando de modo serio y responsable que está emparentada a algunos procesos que es importante emplear, verificado que la averiguación virtual solamente es perceptible visualizando y recurriendo a TI (p. 253). Es decir que para que esta evidencia pueda ser observada para su comprensión debe ser exteriorizada tanto en papel impreso físico o en imágenes o videos.

De esta manera pueda ser considerada en los juzgados.

De conformidad del tratadista Ballesteros (2014) la evidencia electrónica es apreciada o estimada como cualquier tipo informático conseguido solamente que viene de un medio virtual o digital, que es esgrimido para aprobar la seguridad de un acto o de una acción. (p.225), desgraciadamente esta herramienta es muy ignorado en el contorno de carácter judicial especialmente por juzgadores, representantes del Ministerio Público y generalmente por expertos del Derecho. Asimismo, no hay una regulación sobre el asunto de modo exacto,

contienen constantemente refutaciones de modo que crean una discrepancia de discernimientos para la admisión de la propia como evidencia o certeza en los tribunales.

M.Metodología de recolección de evidencia digital. La metodología de recolección de evidencia digital compone un conjunto de pasos para la obtención dela evidencia digital a través de protocolos científicos que permitan darle la validez y confiabilidad a la evidencia, de esta manera sea fehaciente en el proceso penal. Debemos considerar que guiarnos por protocolo de recolección de evidencias digitales correcto, permite disminuir las probabilidades de que estas se alteren o destruyan, a pesar de esto, se debe considerar que se respeten las normas vigentes en el país sobre protocolos utilizados siendo considerada a la evidencia en un proceso penal y declarada admisible.

Esta metodología debe tener tres ápices básicos que son las consideraciones previas antes de proceder a la recolección de evidencia digital, la cuáles serán desde los softwares especializados, los laboratorios, el recurso humano, entre otros. Por otro la manejar un proceso de recolección de evidencia digital y finalmente un proceso de almacenamiento y custodia de la evidencia digital.

En lo concerniente a las consideraciones para la Recolección de Evidencias Digitales, tenemos según Salas (2012) los siguientes:

Primero. Una relación de Principios Básicos:

Incorporarse a los estándares y políticas referentes a la seguridad que se debe tener en el lugar para la correcta manipulación del incidente.

Realizar una captura de pantalla sobre el sistema con la mayor exactitud.

Priorizar la toma de notas que contengan la mayor cantidad de detalles, como las fechas, horas, tipo de evidencia, etc. Estas deberán ser impresas firmadas y finalmente fechadas.

Considerar si existiera una diferencia sobre el reloj del sistema y el Tiempo Universal Coordinado.

Tener todo listo ante la probabilidad de volver a testificar (incluso años posteriores), donde necesitara la mayor cantidad de información sobre el peritaje. Por ende, las notas lo más detalladas son fundamentales.

No tener demasiados cambios en el proceso de recolección de la evidencia. Es decir, limitarse únicamente a cambios externos, más no internos como actualización de archivos digitales o cambios en los tiempos para accesar a los directorios.

Sellar todas las vías de acceso externo, que tuviera la información, de esta manera limitar posibles copias o modificaciones no autorizadas.

Nos vamos encontrar en disyuntivas entre recolectar o analizar la evidencia digital, se recomienda primero recolectar de manera correcta para su posterior análisis.

Es necesario probar los procedimientos para asegurarnos su viabilidad y el manejo de los mismos en una crisis. Lo que se busca es automatizar los procedimientos, sin olvidar la instrumentalización, por un tema de celeridad. Siendo metódico.

Cada dispositivo electrónico tiene un método de recolección de evidencia diferente, pero de seguir los lineamientos establecidos dentro del procedimiento de recolección. En muchos casos la velocidad será determinante cuando la carga de evidencia a analizar es

considerable, por lo que será necesario distribuir el trabajo en diferentes equipos y poder reunir pruebas a la vez.

Por otro lado, existen casos donde la colección de evidencia de un sistema en particular debe ser llevada paso a paso, para no perder ni alterar la información.

Otro punto importante es ir avanzado con la recolección de evidencias digitales según la volatilidad que tenga el dispositivo entre uno y otro.

Por todo lo antecedido, es necesario realizar una copia de prueba y obtener el Hass, que es copia a nivel de bits del sistema. Esto ayudara en el análisis forense, utilizando su copia de prueba a nivel bits, visto que si se aplica en el dispositivo principal este alteraría los tiempos de acceso del archivo.

Esta busca priorizar el orden de las evidencias según las susceptibilidades de los dispositivos de ser volátiles, por ende, será más urgente iniciar con los equipos que tengan mayor volatilidad y terminar con los menos volátiles.

El Código Penal Peruano específica en su Título IV "Delitos contra la Libertad", se debe considerar algunos puntos como es respetar la privacidad de las personas, como también si alguna información obtenida para la investigación va causar algún perjuicio no deberá ser publicada sin consentimiento de la persona interesada o por mandato judicial. También es importante la cooperación de las empresas nacionales y el gobierno para poder continuar con el procedimiento correspondiente sobre la recolección de evidencia digital sobre el incidente

Este ápice establece los requisitos que debe tener la evidencia para ser sujeta a una evaluación y posteriormente ser admitida como prueba en un proceso legal. La evidencia debe ser Admisible, es decir necesita tener y cumplir ciertos requisitos antes de ser

llevado ante el proceso penal, también debe ser Auténtica, de esta manera poder demostrar el nexo causal con las pruebas materiales sobre el incidente. También de estar Completa, es decir la misma narra todo lo acontecido y no solo de manera parcial, por último, debe ser fiable y creíble, la primera no se debe tener duda alguna de la forma en que la evidencia fue recolectada y luego la manera en que fue analizada, la segunda busca que esta llegue a ser comprensible y creíble para los jueces.

Después de todo lo antecedido se requerirá una serie de recursos para efectuar el estudio de las evidencias digitales.

a) Factor Humano: Constituida por un equipo de profesionales que son expertos en recolección y análisis de evidencias digitales.

b) Factor Material: Constituida por los instrumentos preparados para el fin del análisis forense, donde este debe ser una red aislada. También es importante contar con Anotaciones de Campo, Fichas o plantillas de recolección de información, cámara digital, guantes, fundas protectoras, equipos informáticos especializados y software apropiado.

En lo referente a proceso de recolección de evidencia digital tenemos primero la Transparencia, que son aquellos métodos que son utilizados en la recolección de evidencias visto que esta tiene que ser transparente y reproducible. Y por otro lado tener pasos determinados para cumplir con el procedimiento de recolección y de esta manera armar una lista de aquellos sistemas que estén vinculados con el incidente y de aquellos que se recogerán las pruebas. Aquí se considera los siguientes pasos:

- Determinar que es o no una evidencia, caso contrario no proceder con la recolección.

- Manejar el orden sobre la volatilidad que tenga cada sistema.
- Desaparecer las salidas externas.
- Anotar la hora del reloj del sistema.
- Consultar que objetos recolectados pueden ser finalmente probatorios, esto es a medida que avanza la investigación.
- Registrar cada paso realizado.
- Registrar a todas personas involucradas.

Finalmente, lo referido a los procedimientos sobre almacenamiento de las evidencias digitales tendremos a Registro y Codificación donde aquella evidencia que ha sido recolectada tendrá que ser registrada y posteriormente codificada, donde esta última guarda relación con el sitio donde suscitaron los hechos, registrada por fecha, lugar, caso al que pertenece.

Luego tendremos un Registro Fotográfico y Audiovisual donde se considerara lo siguiente:

Retratar, el aparato sin desarmar (sinfuncionamiento con la cifra de de serie).

Retratar, el aparato sin desarmar (con cifras de serie de hardware).

Retratar, la disposición del aparato por adentro.

Retratar el disco duro original y las reproducciones (2) unidas, pasa confirmar la coexistencia de las reproducciones y originales cedidos al conservado.

Por último y transcendental tener una correcta Cadena de Custodia, siendo una serie de procedimientos que están orientados a la preservación de la evidencia digital. Siendo los siguientes:

- Primero la recolección e identificación de la evidencia digital.
- Realizar el análisis de la evidencia digital.
- Proceder al correcto almacenamiento de la evidencia digital.
- Tener la evidencia digital en perfecto estado. Proceder a la preservación.
- Cumplir los protocolos para realizar el transporte de la evidencia.
- Realizar la presentación en el juzgado.
- Proceder a regresarlo al propietario. Es necesario en tener en cuenta los siguientes puntos en lo referente a la cadena de custodia:
- Que la manipulación de las evidencias sea mínima y el estudio de esta, sea por la menor cantidad de agentes.
- Tener en reserva la identidad de las personas que están implicadas desde la obtención hasta la presentación de la evidencia en el juzgado.
- Es de entera responsabilidad que la evidencia digital sea inmutable a pesar de los traspasos entre agentes.
- Llevar el registro de los tiempos, estos deben ser firmados por agentes, en cada uno de los intercambios entre estos sobre la evidencia en cada momento.

- Todos los procedimientos descritos aunados al método científico tecnológico podrán lograr el objetivo de que la evidencia digital sea admitida, creíble y fehaciente dentro del proceso penal.

La metodología de análisis de evidencia digital busca a través de un método científico analizar la evidencia digital, como también producirla y presentarla en el proceso penal. Esta debe tener análisis exhaustivo, sea cual sea el tipo de evidencia digital. Aquí veremos análisis de los datos de la red, análisis de los datos de host, análisis de los medios de almacenamiento. Consideremos que lo que se va analizar son las denominadas armas no convencionales - TIC, las cuales son invisibles y especiales, aquí la informática forense a la criminalística cibernética juega un papel muy importante.

Este análisis de los indicios binarios tiene el análisis lógico y tiene el análisis físico. En este punto se tienen varios conflictos visto que la tecnologías son inconstantes sin coincidencia de aparatos y adjuntos, los regímenes de archivos habita en memoria volatil-ram, los aparatos 3g4g y 4.Sg consienten clonación de aparato o dispositivo, es hacedero de adquirir- obtener equipos de diferentes propietarios, pese a que hay un adelanto en los especialistas no hay auténtica verificación del consumidor existente, hay insuficiencia en las actividades para establecer el vínculo real del aparato celular y malhechor. Todo lo antecedido genera limitaciones y problemáticas para un correcto análisis forense.

En lo correspondiente a un correo se analiza de la siguiente manera una orientación del correo posee 2 partes: La fracción de beneficiario y la parte de dominio. Aquí poseemos ver claramente que el beneficiario de manera normal no está inscrito y los Dominios sí. Por ello, el correo electrónico brinda la probabilidad de circunscribir complementos que consiguen ser registros, bases de datos, audio, etc.

Finalmente procede realizar el informe donde se recopila y organiza los datos de las evidencias digitales para que sea presentada en el Juicio y finalmente admitida. Para ello debe cumplir una serie de requisitos que deben estar plasmados en el Informe. Primero de ser admisible, para ello se empleó una metodología adecuada tanto de recolección como de análisis. Segundo, demostrar su autenticidad, por ello es importante el calco espejo-bit a bit y rúbricas de aseguramiento. Tercero manipular una total actividad en la escena del acto delincuencial. Cuarto, debe ser honesto donde la acción de peritos, usanza de tecnologías e instrumentales forenses legales. Quinto, el proceso para extraer, fortalecimiento, observación y exposición debe ser descifrable para el receptor, debiendo utilizarse las tecnologías claras de certeza física. Por último debe ser creíble, donde este el título habilitante del perito, experiencia comprobada.

Para desplegar y materializar el presente estudio se necesitan o se requieren dogmáticas o doctrinas determinadas. Por esto se emanará a identificar ciertas conceptualizaciones ligadas al asunto de investigación, es por esto que es significativo establecer el progreso del marco doctrinario o dogmático dentro de un estudio. Para Ñaupas (2009) precisa que el Marco de carácter o de tipo Teórico es el fundamento del estudio del problema de cualidad científica. Igualmente se menciona que es la base teórica de la investigación. (p.25), es decir el investigador expone su conocimiento de índole teórica y científica en base a las teorías antecedidas. Por ende, se considera que nadie va poder investigar un problema donde no exista una base teórica o se desconozca

La evidencia judicial se entiende, según Davis (2002), como "cualquier motivo o razón contribuyó al proceso por los medios y procedimientos aceptados en la ley, para traer al juez la convicción o certidumbre sobre los hechos" (p. 25). Por lo tanto, la prueba está configurada en la ley en la medida en que a través de ella las pretensiones o excepciones

pueden cristalizarse en el proceso judicial, alcanzando así la satisfacción de derechos materiales o sustanciales (Gutiérrez, 1990).

Desde esta perspectiva, es necesario aclarar que el manejo adecuado de la prueba o pruebas por parte del fiscal tiene como objetivo mediático informar al juez de las circunstancias que rodean una acción de trascendencia criminal y como objetivo final, promover la materialización de Justicia, que en el ámbito penal se logra aclarando y sancionando comportamientos que afectan en mayor proporción a las garantías fundamentales, es decir, a la conducta punitiva o con la absolución de ciudadanos contra los que no se ha podido distorsionar la presunción de inocencia (Bedoya, 2008).

No es posible calificar a priori la idoneidad de cada una de estas medidas para facilitar la búsqueda de la verdad (sí, por el contrario, obstaculizarla). Es necesario, en el marco de un sistema jurídico particular, identificarlos y luego proceder a enjuiciarlos. Sin embargo, en este espacio es posible analizar la caracterización básica de estas medidas y luego facilitar su localización en relación con un orden positivo dado (Vivares, 2015).

En España, el derecho de uso de las pruebas tiene también un carácter constitucional, consagrado en el artículo 24 de la norma fundamental y, como lo ha señalado el Tribunal Constitucional, entre otros en la Sentencia desde febrero de 2000, Para proporcionar las pruebas necesarias para establecer los hechos en que se basan sus alegaciones. Esta facultad no prejuzga las facultades de los tribunales ordinarios para examinar la legalidad y pertinencia de las pruebas propuestas. (Pardo, 2006).

Hace reseña a los procesos mundiales admitidos para cogida, protección, examen y noticia de la certeza o prueba digital (Macuchapi, 2014).

Este punto de vista se refiere a que la certidumbre o prueba digital debe desempeñar con los códigos de procesos y normas legislativas del Estado. (Zuccardi y Gutierrez, 2006).

Como podemos inferir este es uno de los requisitos de admisibilidad que establece que para considerarse que es una evidencia, ella debe haber sido recolectada, analizada, reportada en concordancia a las normativas y procedimientos legales establecidos internacionalmente como aceptadas y el cumplimento de las normas del país.

Acerca del Sistema de computación abierta. Este sistema está formado por diversos dispositivos electrónicos, que relacionan entre sí. El Hardware que es la porción que resuelve la información de conformidad a las educaciones tomadas por el Software. (Merchan, 2017)

Ahora, en cuanto a sistemas de computación abierta nos estamos refiriendo a aquellos que están hechos de los llamamientos ordenadores particulares y todos sus lindantes como teclas, maus y monitores, los ordenadores manuales. Hoy estos ordenadores poseen la capacidad de almacenar grandes cantidades de información en sus discos duros, lo que los vuelve en una grandiosa fuente de certeza virtual (Santos, 2013).

El método de comunicación está formado por las mallas de telecomunicaciones, la comunicación no alámbrica. Son asimismo un origen de información y de certidumbre virtual (Santos, 2013)

El sistema convergente de computación. Están constituidos por celulares personales o teléfonos, los asistentes particulares virtuales PDAs, las tarjetas inteligentes y cualquier otro equipo de tipo electrónico que tenga afinidad virtual y que consigue dominar certidumbre digital (Santos, 2013).

En estas épocas es más frecuente que la técnica se ha vuelto en un instrumento para ejecutar delitos. Poner en claro estos delitos nuevos y recoger la evidencia importante para

posteriormente entregarla al poder judicial se ha vuelto en un compromiso de los estudiosos determinados (Gil, 2007).

La usanza de la técnica informática en el estudio de un delito utilizando la computadora, ha generado una moderna especialidad, que es la informática de tipo o de carácter forense, que es un procedimiento de identificación, salvaguardar, examinar y mostrar la realidad digital de un modo legítimamente sensato (Gil, 2007).

La verificación o comprobación de la certeza digital. Según Gil (2007), es lo inicial que se efectúa en el procedimiento forense, se debe poseer en consideración qué prueba está presente investigación, adónde y de qué modo de sebe guardar, es importante precisar qué procedimiento serán usados para realizar su recobro.

Los individuos en varios momentos cavilan que solo los ordenadores particulares son el foco de la forense informática, y realmente se extiende a cualquier conector electrónico que es competente de almacenar informaciones, en celulares o teléfonos móviles. (p. 512).

Conservación de la certidumbre virtual (digital). Es un componente indefectible en el procedimiento forense, y son examinados escrupulosamente en el tribunal, es transcendental que cualquier experimento de los datos electrónicos reservados se materialice lo mínimamente intrusiva probable. (Gil, 2007).

El examen de la certidumbre o prueba digital. Una vez conseguida, importantemente pretende de un procedimiento, precedentemente de que obtenga ser entendida por los individuos. Así tenemos en el hecho o en el caso que se posee el retrato de un duro disco, los datos comprendidos en el interior de la igual pretenden un procedimiento (mutación)para que un individuo los consiga los logre descifrar (Gil, 2007).

La exposición de la certeza o prueba digital. Esto involucra el modo formal en la que se muestra una certeza o prueba, la apreciación del experimentado y la fe de los procedimientos que usó para causar la evidencia porque esto se entregará al tribunal o árbitro. (Gil, 2007).

Fases en la evolución de la prueba judicial. Según Davis Echandía citando a Guasp distingue cinco fases de las pruebas judiciales:

1. La fase étnica, en la que se debería llamarse "primitiva" por ser una expresión poco apropiada (Echandia, 2007).

2. La etapa mística del viejo derecho alemán, primero, y del impacto del derecho canónico pronto, establecida en desconocer y el entusiasmo religioso, en esta etapa se esgrimen o usan metodologías probatorias ilógicos, como los denominados reflexiones de Dios. (Echandia, 2007).

3. La etapa legal, que consideramos más conveniente apreciarla como de costo legal, pues se presentó la prueba a una inexorable tarifa anterior de valoraciones, y si bien fue un adelanto en su período, actualmente no es justificado. (Echandia, 2007).

4. La etapa sensitiva, que vendría a ser un mejoramiento de citarla del íntimo convencimiento moral, que se ocasionó en la revolución de Francia como negación frente al coste legal, en el procedimiento penal, asentada en la imperiosa libertad para apreciar la prueba, sin entorpecimiento a una regla, por tribunales de razón ignaros. (Echandia,2007).

5. La fase científica, es la actualmente está principalmente en los códigos procesales modernos, de valoración de acuerdo con la sana crítica y contando con los juristas calificados (Echandía, 2007).

2.3. Definición Conceptual

a. Adolescente.

Es toda persona considerada como tal dese los doce hasta los 18 años. (CNA, 2000)

b. Concurso ideal de delitos.

Cuando distintas disposiciones son aplicadas al propio hecho se sancionará hasta con el máximo de la pena de mayor gravedad, consiguiendo aumentar esta pena hasta en una cuarta parte de la sanción, sin exceder de ninguna manera de 35 años. (Código Penal, 1991)

c. Concurso real de delitos.

Cuando asistan desemejantes hechos materia de punibilidad que deban discurrir como otros muchos actos delincuenciales autónomos, se añadirán las penas de privación de libertad que fije el magistrado hasta un máximo del duplo de la penalidad del acto delictual más peligroso, en ningún caso haya un exceso de treinta y cinco (35) años. (Código Penal, 1991)

d. Datos informáticos.

Toda imagen de vicisitudes, indagación mencionados de cualquier modo que se preste a procedimiento informático, comprendidos los programas esbozados para que un régimen informático realice una función.

e. Delito.

Actividad dolosa o comportamiento culpable, antijurídico y típico, conjuntamente sujeto a ser punible. (Diccionario Español Jurídico de la RAE, 2016)

f. Difundir.

Propagar o divulgar conocimientos, noticias, actitudes, costumbres, modas, etc. (Diccionario Español Jurídico de la RAE, 2017)

g. Distribuir.

Entregar una mercancía a los vendedores y consumidores. (Diccionario Español Jurídico de la RAE, 2017)

h. Falsedad.

Es la ausencia de posibles verificaciones para lo que se está enjuiciando.

i. Falsificación

Es un acto consistente en la creación o modificación de ciertos documentos, efectos, productos (bienes o servicios), con el fin de hacerlos parecer como verdaderos o para alterar o simular la verdad.

j. Indemne.

Libre o exento de daño. (Diccionario Español Jurídico de la RAE, 2017)

k. Indemnidad sexual.

Derecho a que ningún individuo no soporte interrupción en la alineación de su conveniente vida sexual. Primariamente se destina a los individuos de ambos sexos menores de edad y a individuos incapaces. El quebrantamiento de este derecho crea que conmueva de modo psíquicológico al progreso y consideren buenos trances que en realidad no son. Las personas afectadas poseen como derecho ineludible, que una vez estén mayores, de resolver su conducta sexual. (Dudas legislativas.com, 2018)

l. Informática.

Grupo de sapiencias científicas y tecnológicas que forjan la posibilidad del trato de carácter automático de las informaciones por intermedio de ordenadores. (Diccionario Español Jurídico de la RAE, 2017)

m. Internet.

Red internacional descentrada, desarrollada por la ligadura directa entre computadoras y restantes conectores mediante una formalidad específica de comunicación, el TCP/IP, con el fin de que los consumidores consigan informarse en el "ciberespacio" y tener accesibilidad a grandiosas cuantías de informaciones de todo el planeta. (Diccionario Español Jurídico de la RAE, 2016)

n. Libertad Informática.

Esfera de libertad personal que debe reconocerse a toda persona frente a los abusos de la informática. (Diccionario Español Jurídico de la RAE, 2016)

ñ. Libertad Sexual.

Facultad de la persona de auto determinarse en el ámbito de su sexualidad. (Diccionario Español Jurídico de la RAE, 2016)

o. Niño (a).

Es todo individuo o toda persona desde su nacimiento hasta tener los 12 años. (CNA, 2000)

p. Pornografía.

La pornografía es la filmación, fotografiado y exposición de manera explícita de relaciones sexuales.

q. Propiedad Intelectual.

Es una norma que abarca los derechos de los que crean algo a nivel intelectual. Mediante de dicha normatividad es probable su amparo, organización y resguardo frente a otras personas.

r. Proposición.

Acción y efecto de proponer, es decir, hacer una propuesta. (Diccionario Español Jurídico de la RAE, 2017).

s. Sistema Informático

Todo punto de conexión aislado o grupo de conectores interrelacionados entre sí, cuyo funcionamiento, o la de ciertos de sus factores, será el procedimiento computarizado de datos en cumplimiento de un programa.

t. Tecnología de la Información.

Esta conceptualización abarca todo lo interrelacionado con el aspecto informático, la tecnología de la electrónica y las telecomunicaciones. Los adelantos técnicos como el Internet, la comunicación móvil, los satélites. Han hecho importantes variaciones en el régimen socio económico, impactando en las interrelaciones de carácter social.

2.4. Marco histórico.

La Internet y su influjo en la sociedad en su conjunto de redes a nivel contemporáneo acarreó la denominada “Sociedad de la Información”; En el Internet es personificada por la Red Científica del Perú, entidad que tiene una funcionabilidad de modo independiente, sin ninguna contribución económica de tipo o de carácter foráneo, su meta es el cambio de informaciones y perfeccionamiento o desarrollo de las telecomunicaciones; esta entidad en

pocos años, ha divulgado considerablemente su comprendido. Como Internet tenemos: el TCP/IP (Transfer Control Protocol/Internet Protocol). También consideramos a la World Wide Web (www o web) que consiente que las informaciones de todo tipo de redes conectada a Internet puedan ser delimitada sin interesar su sitio físico. (Barriuso, 2000).

Los sobrenombres de dominio es la dirección de Internet asignada en frases, de tal manera que secuela cómodamente clara para el consumidor de Internet. La funcionabilidad de este régimen de sobrenombres de dominio ("domainnamessystem" DNS) es mediante de bases de datos y sus concernientes direcciones IP. El "domainname" este compuesto de 2 factores uno populares "yahoo", "terra" y otro apropiables a "com", "edu", "gob". (Barriuso, 2000).

Los dominios se catalogan en: dominio de escala preferente ("Top LevelDomains" o TLD) y dominios de 2do, 3cer o 4to grado. Los TLD de carácter o de tipo comercial, "org" para formaciones, etc.), dominios específicos para instituciones o entidades organizacionales que desempeñan con indiscutibles exigencias ("edu" "gov-int") y dominios mundiales ("pe" "es", "ar") siendo el primero Perú, el segundo España y el tercero Argentina. (Lara, 1996).

En equivalente, la informática y Derecho Informático y simplemente Derecho no son indiferentes a este progreso porque en 1962, Philippe Dreyfus usa el vocablo "Informatique" para unir 2 definiciones: "automática" "información", naciendo con ello una nueva carrera profesional, llamada Informáticpor lo que en la actualidad exiten profesionales en la especialidad de informática y que servirán como unametodología en el campo del Derecho (Rondinel, 1995).

Al afin es apropiada la conceptualización esbozada por Perez (1984), quien meciona que el Derecho Informático; estudia el comportamiento automatizado de los orígenes de comprensión jurídica, siendo su meta "la aplicacabilidad de la técnica de las informaciones jurídicas". Pero hay que tener en consideración, la tecnología informática posee implicaciones de carácter jurídico y que se hallaban interrelacionadas a su conveniente ordenación, es así

como brota el Derecho Informático como la disciplina del Derecho que percibe al grupo de normatividades que rigen las modernas técnicas de las comunicaciones y las informaciones son la telemática y la informática.

Según Calderón (2000) en esta realidad la presente Sociedad de Información Jurídica, surgen innovadoras o modernas tecnologías que propician un auténtico cambio de ejemplos, el arcaico modelo del escrito encima del papel se ha transfigurado en ejemplo de las informaciones digitales. Tal ha es el efecto que ha inducido el elemento cibernético en la conducción de las informaciones de nuestra propia sociedad que se ha elegido por designar a nuestra época como la época de la información.

Esto, en el campo jurídico, posee consecuencias suficientemente indiscutibles y que se interrelacionan con la llamada "desmaterialización del Derecho"Trazegnies (1998). El invento de las redes de conexión y el Internet han precipitado dicha no materialización, lo que guarda interna relación con la conveniente naturaleza del ambiente digitalizado, mencionemos, por modelo, el caso de Internet. Debido a que por internet transitan grandiosas cuantías de información digital, por ello en muchos países se le conoce con el nombre de super camino de información, "red de redes", red de cubierta territorial universal. (Rowland, 1998).

Dentro de este contexto real hay varias incriminaciones donde aparecen comportamientos que quebrantan bienes jurídicos no convenidas y a su vez conductas que se ejecutan utilizando medios no convenidas para lacerar bienes jurídicos convencionales. Uno y otros, poseen íntimas relaciones técnicas. Asimismo, podemos mencionar la utilización de manera general de la red Internet son debidas a sus semejantes propiedades, las propias que Christine Mayewski ha explicado de modo comprensible, y son: la habilidad de su usanza, su inferior coste, su celeridad, sus capacidades y la carencia de límite de tipo o de carácter geográfico (Zaffaroni, 1981).

Tal insuficiencia, creada desde inicios de la última década en compañías hondamente informatizadas, se ha reubicado a compañías como de nosotros, los adelantos técnicos o de carácter tecnológico ha habido grandes influjos en el contorno del crimen por ello este moderno modo de operar consiente atraer vacíos en el campo del Derecho Criminal o Penal acostumbrado, permaneciendo desamparados los comprendidos no materiales de la técnica informática. (Cafure de Battistelle, 1995).

Para proporcionar todavía más los objetos, para los que necesitan de grandiosas sapiencias de telemática e informática, se establecieron interfaces más cordiales, establecidas en representaciones de tipo gráfico de la información comprendida en los diferentes computadores, de un modo parecido a un mural. Asimismo, se instauraron programas que proporcionan la accesibilidad a diferentes representaciones, sin insuficiencia de digitar complicadas fórmulas. La inicial noción manifestado es la página web, y el que sigue es el navegador. Haciendo mención que Mosaic es el primer navegador en su género y que fue creado el año 1993.

Sin embargo, pese a lo anteriormente manifestado EE.UU. mediante sus autoridades gubernamentales no facultaba la accesibilidad de carácter universal o mundial a la red Internet, sin embargo, cuando cayó el muro de Berlín y dejando de existir los grandes temores de un conflicto o conflagración nuclear, se liberó la accesibilidad el año 1994. Pero posteriormente o sea durante el año 1995, el incremento de la red es extraordinario, y es como actualmente sabemos y conocemos, cada vez que hacemos uso de la red de internet nos damos cuenta de sus bondades tecnológicas, y que hoy en día se ha vuelto una necesidad indispensable y que seguramente en el futuro no habrá domicilio sin internet.

La revolución de carácter tecnológico que se inició a partir de la segunda medianía del siglo veinte es solamente confrontables, por sus influencias sociales y de carácter económico, a la transformación industrial del siglo diecinueve. Efectivamente, la técnica perfeccionada

después de la Segunda Beligerancia a nivel Mundial consiente dialogar de una “revolución tecnológica” en la que la informática y, fundamentalmente el microchip, es el dispositivo céntrico que proporcionó la creatividad de todos los equipos de usanza frecuente en la existencia cotidiana.

Las variaciones de tipo tecnológico brotaron en el siglo veinte, causando una metamorfosis del tamaño como los realizados por la transformación tecnológica del siglo diecinueve donde se dio un avance o progreso de las técnicas informáticas, en la cual los ordenadores abandonaron la oficina para penetrar los domicilios y comprender casi todas las acciones y labores de carácter humano.

A esto se adhirió el internet que exclusivamente consciente la accesibilidad de carácter antiguo a cualquier método informático, manifestándonos que la idea de Bill Gates (1999) que asevera que:

El futuro acoplado por una auténtica travesía de la información es ya es algo real y material de la cual nos deleitamos, nos favorecemos e inclusive sufrimos. Pero, la tecnología no solamente ha influido de modo favorable en la existencia humana, sino que asimismo ha ocasionado la aparición de modernas maneras de crimen. (pág. 59).

2.5. Marco legal.

2.5.1. Casos más relevantes a nivel mundial.

A. Caso Herbert Zinn.

a) Fue la primera persona que fue sentenciado judicialmente bajo el contexto del delito de Fraude con computadora durante el año 1986

b) Contaba con dieciséis (1 6) años cuando quebrantó o vulneró la accesibilidad a AT&T y los regímenes de la Oficina de Defensa

c) Pérdida de aproximadamente US $174,000 en registros, duplicados de programas.

d) Sentenciado judicialmente a nueve (9) meses de privación de cárcel y a una garantía de US$10,000.

B. Caso David Smith.

a) Delatado de instaurar y realizar la distribución del virus que bloqueó millares de cuentas de correo.

b) Condena con un máximo de 10 años de privación de libertad en un centro penitenciario.

c) Contagio a más de 100,000 computadoras de todo el planeta, circunscribiendo a organizaciones empresariales como Microsoft, Intel, Compaq, gobiernos públicos de EE.UU.

C. Caso Kevin Poulsen.

a) Delatado de robar mandatos de trabajo concernientes con un ejercicio de la fuerza del aire de carácter militar.

b) Enfrenta hasta diez años de encarcelamiento.

c) Popular por su destreza para intervenir el método telefónico de la organización empresarial Pacific Bell.

d) Crackeó todo arquetipo de áreas, pero él se concernía por los contenidos de asuntos de resguardo nacional.

D. Difamación. Este delito se explica en el superior desvalor de la labor por la cabida de propagarse el agravio a una amplia o espaciosa cuantía de individuos mediante “si el delito se ejecuta por medio del texto y los periódicos […]”.

Aquí, se pide que la versión vejatoria se propague encima de un medio de comunicación de tipo o de carácter social, como la TV, los periódicos, la radio. Pero, actualmente las técnicas informativas han incrustado una diversidad de correos electrónicos, Twitter redes sociales, páginas web o blogs que congregan 2 peculiaridades céntricas para trascender las noticias como i) cabida de resistir registros en video o en escritura y II) aforo de propagación inclusive

en una página web o blog, la referencia o acotación tiene la capacidad de ser observado o mirado por una cantidad que no se puede determinar de individuos.

Por este contexto o esta realidad, para obviar vacíos de acciones punibles que perturben el fundamento de legitimidad, porque la prensa son publicaciones de carácter asiduas, comúnmente escritas, donde los medios comunicativos acostumbrados no abarcan los modernos caminos de difusión por ello consideramos que debe haber una reforma de este articulado para circunscribir una fórmula que entienda a los modernos medios técnicos como se concibe el CP de España "cualquier medio de eficiencia similar".

E. Violación de la intimidad (Art. 154 del Código Penal). Se define como la accesibilidad o interrupción, no debida, de elementos de la confianza individual mediante instrumentales o procedimientos tecnológicos que consientan para mirar o ver o registrar actos o retratos. En la perjudicial, el conocimiento de "medio de comunicación social" consigue ser descifrado como he mencionado en la calumnia de carácter agravado, por lo que para circunscribir a todas las conveniencias de comunicación o propagación de informaciones mediante el internet o las redes de carácter social se consiguen utilizar la receta cualquier medio de eficiencia similar.

F. Violación de correspondencia, supresión o extravío indebido de correspondencia y publicación indebida de correspondencia (Arts. 161, 163 y 164 del Código Penal). La primordial limitante para acomodar a estos tipos de carácter penal para agarrotar las expresiones de la transgresión técnica es el objetivo de carácter material. Se circunscribe a la "correspondencia telegráfica", de irrisoria usanza, como la meta sobre el que cae la actividad, esto es, que los hechos de eliminación o perdición solamente consiguen caer en comunicaciones de tipo escrito como mensajes o encargos. Estos actos de carácter delincuencial se conformaron en el período pre internet cuando la comunicación se perpetraban fundamentalmente con papel "u otra de peculiaridad similar" circunscribe el comentario a

quienes que poseen como sustentáculo el papel; el tipo penal resguarda exclusivamente a las cosas palpables. Esto es, debido a que la exegesis excelente a lo expresado por el artículo. 161 "otro de particularidad similar" es asimilar a distintos factores análogos o semejantes el escrito, documento o comunicación telefónica que posean como sustentáculo el papel. Consecuentemente se debe variar este tipo penal para circunscribir en el objeto de tipo o de carácter material a la comunicación interindividuales que se ejecuten por intermedio que use la informática y las TIC.

G. Delito de escucha indebida (Art. 162 del Código Penal). La ley menciona que el objeto de tipo o de carácter material es una "diálogo telefónico o análogo", lo cual se limita a las comunicaciones de onda vocal, pues es referido a las equivalentes comunicaciones entre las que de modo único consiguen ser las difusiones de onda vocal. Consecuentemente, se excluyen ajenas difusiones que se ejecutan con las modernas tecnologías de informaciones.

H. Interferencia de comunicaciones electrónicas (Art. 162-B del Código Penal). Este tipo incrustado en 2015 intenta cobijar la falta o carencia de amparo que poseían las innnovadoras o modernas comunicaciones, por ello, hubiese sido preferible instaurar el objeto material concerniente a las TIC. para circunscribir a los medios actuales o nuevos de comunicación que han sido incrustados por la informática.

I. Delito de turismo sexual comercial infantil y adolescente en el ámbito de turismo (Art. 181-A del Código Penal). Esta reforma circunscribió como medio transmisión al internet para publicar el aprovechamiento sexual especialmente de menores de edad, no obstante, sería provechoso ejecutar una reforma para esgrimir una receta más extensa y circunscribir cualquier modo de comunicación que use los métodos de la información.

J. Delito de publicidad de prostitución sexual infantil (Art. 182-A del Código Penal). Se describe a los garantes, son los editores de los medios de comunicación, sin

embargo, se descarta la web o de otros medios de comunicación de tipo o de carácter electrónica.

K. Exhibición o publicación obscena (Art. 183 del Código Penal) y pornografía infantil (Art. 183-A del Código Penal). La exposición a menores de edad de material relacionado a la pornografía puede ejecutarse "por cualquier medio", incluyendo internet, pero en el hecho de carácter delincuencial como es lo relacionado al delito pornográfico infantil se circunscribe explícitamente la internet.

La Legislación de delitos de tipo o de carácter informático del año 2013 hizo un perfeccionamiento de este comportamiento delincuencial al aumentar los medios de propagación a los compendios que brindan las técnicas de la información, lo cual propone una visión más extensa que la internet. Las TICs están referido a recursos que se desplegaron a partir del ordenador e indiscutiblemente el internet.

L. Delitos contra el patrimonio. Delito de hurto telemático (modalidad agravada comprendida en el Art. 186, segundo párrafo, inc. 3 del CP) La afectación del patrimonio particular son las iniciales expresiones del crimen informático, pero no existía manera de castigar por los delitos acostumbrados que resguardaban este bien jurídico. Los actos delincuenciales de hurto hallaban una restricción en relación a la cosa mueble como cosa de incautación ilegal.

Las cosas idóneas para ser el bien de carácter material en la óptica expresada en el Art. 185 del CP, fundamentalmente en el llamado "hurto telemático" en la entrega electrónica de caudales, son, esencialmente, los caudales comprendidos como dinero electrónico, sin embargo, cuando la ley de tipo penal se refiere considerablemente a la utilización de la telemática, se trata de todo tipo de elemento de carácter informático con importe económico formando parte de la propiedad particular. (ROJAS VARGAS, 2000, P. 284).

El acto de tipo delincuencial denominado hurto telemático marchó de manera perfecta hasta su abolición por la Ley de delitos de carácter o de tipo informático del año 2013. Por ello, partiendo de esta ley, el amparo del patrimonio tuvo protección con el nuevo tipo de estafa informático.

Delito de estafa es un hecho en 3 actos: i) perjuicio patrimonial ii) error iii) engaño. Por ello, no era idóneo para enfrentar la utilización de la tecnología para quedarse con el patrimonio de otra persona. La Ley N.° 30096, anuló el hurto telemático e instituyó el tipo de estafa telemático. Delito de daños La dogmática plantea la interpretación del delito de daños para enfrentar las dificultades del sabotaje informático. Lo realmente importante, nos comunica Gutiérrez Francés es que "se menoscabe algo apreciado económicamente" donde se incluye a los elementos razonables de los regímenes informáticos como objeto de carácter material del delito de daños.

M. Delitos contra los derechos de autor y conexos (Arts. 216, 217 y 219 del Código Penal). La usanza de la informática y la técnica establecen medios lucrativos y eficientes para perturbar el bien jurídico. Al respecto los Arts. 220-A, 220-B y 220-C del CP a las conductas que usan medios técnicos para desactivar los dispositivos de seguridad que se instalan en las obras para, necesariamente, impedir su reproducción ilegal.

N. El tipo penal de atentado a la integridad de sistemas informáticos. Para tal fin, se apela a una exegesis sistemática de la ley penal, la razón deductiva, la ley contrastada y la teoría mundial que avisa o comunica uno de los hechos internacionales mundiales de más importancia actualmente: el cibercrimen. De este modo, revela los vacíos de carácter legislativo y la omisión que esta norma tiene en su comprendido y, conjuntamente, propone la falta de coherencia que hay entre sus factores, y las que existe entre la ley y la normatividad penal habitual.

Desde que Robert Tappan Morris, alumno de veinte y tres años de la Universidad de Cornell de los EE.U., contagiara el do del mes de noviembre del año 1988 con el primer modelo de malware autorreplicable, un gusano informático, que conmovió arduamente el trabajo de aproximadamente seis mil (6, 000) computadores de un integral de sesenta mil (60, 000) del régimen integral de internet de la mencionada nación, comprendido la NASA, transitaron doce años para que en la nación peruana es una de manera tímida, por Ley N.° 27309, la imagen de los actos delincuenciales de tipo informático (Arts. 207-A, 207-B, 207-C y 207-D del CP) y 25 años para que se publique la Ley N.° 30096 relacionados a delitos informáticos. (Diario Gestión, 2016)

Fecha del Documento: febrero 2017-Procedencia del Documento: Perú-Consideración General:

La División de Estadística, ente rector del Sistema Estadístico de la PNP, ha hecho el Almanaque Estadístico PNP 2016, que me condesciende en mostrar, documentaciones que es producto de una labor invariable y simultáneo entre los integrantes de los órganos del Método Estadístico PNP. Posee veinte y seis Capítulos, donde uno de ellos es La DIRINCRI PNP, donde el 2016 ha reportado veinte y dos mil ochocientos ochenta y uno (22,881) denuncias por otros delitos; de los cuales cuatro mil quinientos cuarenta y cuatro (4,544) fueron decididos parecidos al 1.63%. Donde se encuentra la DIVINDAT - División de Investigación de Alta Tecnología. Conclusión del Análisis Documental

En los datos estadísticos arrojados por la División de Estadística de la PNP, sobre denuncias recibidas por Comisión de Delitos Registrados por la Dirincri PNP, según tipo de Delitos en el año 2016, se aprecia que tuvimos 880 denuncias recibidas sobre Delitos Informáticos, divididos en 4 trimestres. El primer trimestre (enero a marzo) con 196 denuncias.

El segundo trimestre (abril a junio) con 193 denuncias. El tercer trimestre (Julio a Setiembre) con 206 denuncias y el último y cuarto trimestre (noviembre a diciembre) con 285 denuncias.

En un segundo Cuadro 3.4 sobre Detenidos según tipo de Delitos y Modalidades en la DIVINDAT - DIRINCRI PNP. Año 2016, se aprecia que solo tuvimos 18 detenidos sobre Delitos Informáticos, divididos en 4 cuatro trimestres. El primer trimestre (enero a marzo) con 5 detenidos. El segundo trimestre (abril a junio) con 1 detenido. El tercer trimestre (Julio a Setiembre) con 6 detenidos y el último y cuarto trimestre (noviembre a diciembre) con 6 detenidos.

Lo que refleja una diferencia abismal entre las denuncias y los detenidos por este tipo de Delitos. Aquí resaltan una vez más las falencias de herramientas especializadas, instrumentalización, personal suficiente y capacitado, operadores jurídicos capacitados, entre otros. Lo cual requiere una especial atención porque este es el centro de la problemática de la investigación en curso.

Exp. Nº3603-2015-85-1501-RP-PE-02

Delito: Delito Informático

Objeto Jurídicamente Protegido: Contra la Indemnidad y Libertad Sexual Normativa: Art. 5 de la Ley de Delitos Informáticos. Propuestas a menores y adolescentes con fines sexuales por medios técnicos.

Problemática Jurídica:

La agraviada de trece (13) años fue antedicha por medio del teléfono celular y Facebook con retratos pornográficos con la intencionalidad de emanar a realizar el acto sexual, porque se

reveló en los diálogos determinantes para evidenciar su intencionalidad. La mamá de la menor insinúa de esto al Ministerio Público y lo cual se provienen la detención al Sujeto activo.

Decisión:

Se solucionó con la Anticipada Terminación de parte del accionado determinado en el Art. 468 del CPP, y se le dio una penalidad de cuatro años y seis meses.

Comentario:

En el universo teorizante se ha creado una discusión referido al examen de esta ley donde mediante tecnologías de la información relaciona con una menor de catorce años para la obtención del material relacionado a la pornografía o para realizar un hecho sexual. Son considerados de la misma manera los que poseen entre catorce y dieciocho años de edad y medie el ardid. Esto significa, se busca la buena exégesis de la propia pues lo que se indaga o se investiga es la comprobación de la tipicidad subjetiva finita del sujeto activo, preferentemente en lo que se refiere “para solicitar". Aquí se condena la intención. Por ende, el caso en mención ha establecido una jurisprudencia fundamental.

Exp. Nº01719-2014-80-1601-JR-PE-06

Delito: Delito Informático

Objeto Jurídicamente Protegido: Contra la Indemnidad y Libertad Sexual Normativa: Art. 5 de la Ley de Delitos Informáticos. Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos.

Problemática Jurídica:

El sujeto pasivo tiene trece (13) años fue contactada a través de Facebook donde se le solicitaron imágenes y se le realizaron proposiciones obscenas. La madre de la menor advierte de esto a la Fiscalía y lo cual se procede a detener al Sujeto activo. Decisión:

La fiscalía solicito la Terminación Anticipada establecido en el Art. 468 del Código Procesal Penal, y se le dio una pena de 4 años y 6 meses.

Comentario:

De la jurisprudencia antecedida se ve un mismo patrón donde el contactar, pero con un fin que está en contra de la indemnidad sexual y libertad sexual es penado, todo esto se configura cuando son realizados a través de medios electrónicos (celular, Tablet, laptop, etc.) o el internet. Sobre este delito a comparación de los otros delitos informáticos establecidos en la ley tiene el 90% de incidencia de ser denunciado y sentenciado.

Exp. Nº0514-2014 (13105-2014)

Delito: Delito Informático

Objeto Jurídicamente Protegido: Contra el Patrimonio

Normativa: Art. 8 de la Ley de Delitos Informáticos. Fraude Informático. Problemática Jurídica:

Una persona mediante phishing, clona la página de un banco. El titular de la tarjeta ingresa a hacer nuevos movimientos, donde se aparece la página clonada.

Decisión:

La Fiscalía solicito la Terminación Anticipada establecido en el Art. 468 del CPP, y se le dio una pena de 3 años, su pena finalmente no fue efectiva.

Comentario:

Sobre este delito, aquí estamos frente a un delito de criminalidad organizada. Pues no solo es una persona la involucrada, sino una red de criminalidad el cual busca realizar fraudes informáticos con herramientas y softwares de alta tecnología. El más conocido en este caso es el denominado phishing, aquí la página del banco es donde para que el titular de la tarjeta y cuenta procede a ingresar el número de tarjeta y su clave y posteriormente la página desaparece, con estos datos procede el sujeto activo a retirar 3,000 soles, haciendo una trasferencia a otra cuenta. La señora se percata del movimiento pues tiene conectada la aceptación a través de su correo electrónico, por lo cual sorprendida se acerca al banco, donde solicita el número de cuenta donde ha sido enviada la transacción, con el cual obtiene el nombre del sujeto activo. Este se defendió argumentando que saco una tarjeta por un favor a una señora y esta le daría 20 soles, por lo que accedió. Pero finalmente al realizar el peritaje correspondiente y el análisis de la evidencia digital se determinó que en su computador tenía varios programas con este fin, es decir tenía una actividad delictiva informática.

Exp. Nº2587-2015

Delito: Delito Informático

Objeto Jurídicamente Protegido: Contra el Patrimonio

Normativa: Art. 8 de la Ley de Delitos Informáticos. Fraude Informático. Problemática Jurídica:

En este caso el Sujeto Activo era conocida del Sujeto Pasivo, donde este por hacerle un favor presta su tarjeta y cede su número de cuenta y contraseña. Catorce meses después esta persona realiza una transacción a la cuenta del sujeto activo. Esta también es advertida

mediante correo electrónico y se apersona al banco, procediendo a realizar la denuncia correspondiente.

Decisión:

La Fiscalía solicito la Terminación Anticipada establecido en et Art. 468 del CPP, y se le dio una pena de 3 años.

Comentario:

En esta jurisprudencia se observa que et proceder a cometer delitos contra el patrimonio a través de medios electrónicos. Tenemos este tipo penal el cual sanciona diversas y variadas conductas sobre el indebido empleo de datos informáticos y la manipulación sobre el funcionamiento del sistema.

La ley de Delitos Informáticos nos presente un bagaje de artículos que han evolucionado et concepto no solamente legislativo sino de Teoría del Delito por tal complejidad en su comprensión en cuanto a sus Tipicidad, tanto Objetiva como Subjetiva. Si bien es cierto nuestro legislador se preocupó por penalizar estas conductas, y la DIVINDAT está tratando de luchar contra este denominado Cibercrimen, se ve una deficiencia en cuanto apoyo interinstitucionales.

Interpretación de la Norma

Fragmento ubicado el Capítulo I de la Ley de Delitos Informáticos Nº 30096 Artículo 1.

La presente Ley tiene por objeto prevenir y sancionar las conductas ilícitas que afectan tos 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 delincuencia.

El presente fragmento nos establece que el objeto y la finalidad de esta ley es combatir los Delitos Informáticos o Delitos Informáticos, el cual nos refuerza la existencia de una normativa que nos avala esta persecución, ya que busca la correcta investigación y llegar al enjuiciamiento que garantice la sanción.

2.6. Derecho comparado.

A. Estados Unidos. El Acta Federal de Abuso Computacional de 1994, que modificó el Acta Fraude y Abuso Computacional de 1986, diferencia el tratamiento a aquellos que de manera temeraria lanzan ataques de virus, de aquellos que lo realizan con la intención de estragos. (Ramírez, 2016, p 23).

Como el autor expresa, el acta de Estados Unidos fue modificada llegando a plantear diversas medidas de sanción para regularizar los virus que contaminen bases de datos, ya que, al destruir, trasmitir o cambiar los sistemas informáticos, estos se consideran como delitos, es por tal motivo que la ley impuesta se semejó al problema dando cabida a una nueva era de ataques tecnológicos.

El Acta define dos niveles para el tratamiento de quienes crean virus, estableciendo para aquellos que intencionalmente causan daño por la trasmisión de ese virus, el castigo de hasta 10 años en prisión más una multa y para aquellos que lo trasmiten, solo de manera imprudencial la sanción consiste de entre una multa y un año en prisión.

Los legisladores estadounidenses, la nueva Ley constituye un acercamiento más responsable al creciente problema de los virus informáticos, específicamente no definiendo a los virus sino describiendo el acto para dar cabida en un futuro a la nueva era de ataques tecnológicos a los sistemas informáticos en cualquier forma en que se realicen. Diferenciando

los niveles de delito, la nueva Ley da lugar a que se contemple que se debe entender como acto delictivo. (Viere, 1994, p. 20).

Para el autor, Estados Unidos es como un país en donde existen con facilidad la irregularidad de los medios informáticos en donde la ley regulada guarda nexo con el problema planteado, en donde cambia la figura del delito por la palabra acto delictivo.

En el Estado de California, en 1992 se llega adoptar la Ley de Privacidad en donde se contemplan los delitos informáticos, pero en menor grado que los delitos guardando relación con la intimidad la cual se constituyen como el objetivo principal de esta Ley. (Ramírez, 2016, p. 23)

Para el autor Ramírez el objeto de la Ley es la protección del individuo con respecto a la base de datos y a los sistemas computarizados ilegales, en donde la protección legal es base para la protección de la intimidad de los individuos, dando bienestar al Estado de California.

B. Colombia. Andrés Velásquez, presidente y fundador de la compañía de Civet Seguridad Informática, expresa que existen dos tipos de Civet, aquellos que llegan a realizar un delito aprovechando de que saben sobre las vulnerabilidades de los sistemas informáticos y aquellos que se encargan de robar información de la empresa o base de datos con el fin de utilizarla para beneficio propio, muy a pesar que no son expertos con la tecnología. (Huerta, 1990, p.19)

El problema más presentado por el autor frente a la comunidad colombiana es la suplantación de identidad, difamación por internet, fraude cibernético, denegación de servicios, fuga de información, entre otros. Ahora bien, estos problemas son consecuencia los hackers tal como lo demuestran los medios de comunicación, pero para la compañía Civet estos problemas llegan a vulnerar la privacidad individual y empresarial.

El Congreso de la Republica de Colombia bajo la Ley 1273 dado el 5 de enero de 2009, llega a sancionar, protegiendo la información y datos de sistemas tecnológicos de información y comunicaciones. (García, 2009, p, 16).

Para el autor esta norma se llegó a convertir como protección de un bien titulado estableciendo una normatividad de conductas delictivas relacionadas a la tecnología a través de medios informáticos, en donde el país de Colombia pasó a ser el pionero a nivel mundial en materia de legislación de delitos informáticos.

Actualmente existe la Ley 1273 en donde estos delitos son castigados con pena de prisión que equivalen a las 48 y 12 meses y multas de hasta 1,000 salarios mínimos legales mensuales vigentes, pero para algunos expertos expresan que mientras existen más creaciones de normas que generen soluciones a problemas, están surgiendo más tecnología para burlarse de ellas.

C. Venezuela. Aquellas conductas que son sancionadas por el derecho haciendo un mal uso del medio informático, existe una ley en Venezuela que se encarga a pasos agigantados de la regulación de un área tecnológica en donde las actividades sin ser ilícitas presentan una plaga a la sociedad. (Pérez, 1996, p. 41).

Para el autor en Venezuela hay leyes que se encargan de regular el ambiente tecnológico sin embargo hay algunos que a pesar de que no sean ilícitos estos presentan consecuencias a la sociedad entre ellas tenemos: Acceso Indebido, sabotaje o daño a sistemas, Espionaje informático, falsificación de documentos, manejo fraudulento de tarjetas inteligentes o instrumentos análogos, difusión o exhibición de material pornográfico, apropiación de propiedad intelectual, etc. Estas actividades antes mencionadas llegan o no estar tipificadas como delitos, sin embargo, hace un gran daño a la sociedad.

D. Panamá. Teniendo como imagen España acerca de la penalidad por usurpar la identidad o lesionarla, la Policía Nacional se preocupó por reforzar el tema denunciado el uso incorrecto de las redes sociales, autores como el abogado Jorge Torregrosa (2004). Indica que los delitos informáticos se encuentran tipificados en el Código Penal, imponiendo en el Código sanciones que llevan a la prisión aproximadamente seis años, esta conducta se encargará de la regulación de los delitos informáticos. (p, 29).

Como bien expresa el abogado la legislación de Panamá verso mucho en casos de España, en donde los delitos se encuentran tipificados de acuerdo al Código Penal, esta Ley tiene que determinar la responsabilidad de los imputados como también identificar los daños cibernéticos.

Las normas establecidas y adoptadas mediante la ley 26 del 2008, la Ley 5 de 2009, la Ley 68 de 2009 y la Ley 14 del 2010 Título VIII Delitos contra la Seguridad Jurídica de los medios electrónicos Capítulo I Delitos contra la seguridad Informática que va desde el artículo 289 hasta el artículo 291. (Cavara, 1993, p. 15).

E. Ecuador. Se inició a través de los primeros tipos penales informáticos en el año 2002 en donde surgió el proyecto para la creación de la Ley de comercio electrónico, los cuales posteriormente fueron incluidos en el Código Penal, esto se pensó luego de que pasará los primeros ataques en el año 2001 fuera de la página del Municipio de Quito, tomando como referencia el primer delito que se cometido en el año 1996, cometido por EMETEL. (Núñez, 1998, p. 26).

Para el autor Ecuador dio inicio de la proyección de medios informáticos cuando en este surgió ataques en Quito, dándose la creación de la Ley de comercio electrónico, actualmente ejerciéndolo como un procedimiento técnico en donde participan expertos en la

materia, teniendo como ayuda alguna asistencia penal internacional para recabar la información respectiva.

La Ley 67, publicada el 17 de abril del 2002, tiene un avance muy importante en el sentido de incluir figuras penales que castiguen los ilícitos informáticos, con lo cual junto al Código Penal integran normas creadas para la sociedad de la información. (Abellán, 2010, p.20)

Dentro de estas normas promulgadas en la Ley 67 para posteriormente ser trascritas al Código Penal, constan los siguientes ilícitos informáticos:

Art 57 LCEFEMD: Infracciones informáticas. - son aquellas que tienen carácter administrativas y se encuentran tipificadas en el Código Penal, en la presente Ley.

Art. 58 LCEFEMD, Con. Art 202.1 CP: Contra la Información Protegida. - aquella persona que quiere acceder o vulnerar información y también la seguridad de dicha información será reprimida con prisión de seis meses a un año y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica.

Esta Ley permite establecer lineamientos jurídicos a través de las normas, incluidas el comercio electrónico en donde se encarga de cuidar los principios de confidencialidad y la reserva de los mensajes de datos, sin llegar a violar los principios de intuición electrónica.

F. México. En el Código Penal Federal de México, dedica un capítulo del noveno título de su segundo libro" accesibilidad ilegal a sistemas informáticos", en donde se instituye la defensa de las comunicaciones. (Téllez, 2004, p. 29).

Como dice el autor se necesita de manejos que apoyen a efectuar una sana interrelación entre las diferentes personas con la tecnología, consiguiendo a la investigación y acosando delitos, congregándolos en una idéntica Ley Federal.

Capitulo III.

Hipótesis y Variables

3.1. Hipótesis

3.1.1. Hipótesis General.

Existe una relación directa y significativa entre los delitos informáticos y la evidencia digital en el proceso peruano del Distrito Judicial de Junín, 2020.

3.1.2. Hipótesis Específica(s).

1.- Existe una relación directa y significativa entre los delitos informáticos y el valor probatorio en el proceso peruano del Distrito Judicial de Junín, 2020.

2.- Existe una relación directa y significativa entre los delitos informáticos y los alcances de la regulación en el proceso peruano del Distrito Judicial de Junín, 2020.

3.- Existe una relación directa y significativa entre los delitos informáticos y la Información digital en el proceso peruano del Distrito Judicial de Junín, 2020.

3.2 Variables.

3.2.1. Variable Independiente: Delitos informáticos.

El avance de las TIC's ha traído importantes cambios a la sociedad, difiere terriblemente a la que conocíamos hace 15 años atrás. Estos cambios son sistemáticos y rápidos. Generando tener visiones renovadas del modo de vida constantemente. El hombre como ser que se adapta a los cambios, asume estas nuevas tecnologías y la aplica en su día a día, para su

uso en beneficio de la sociedad, esto es válido mientras esta acción no vulnere los derechos de las otras personas, es una acción lícita, que puede ser desarrollada sin mayor implicancia.

Lamentablemente contrario a esto el internet y los medios electrónicos son usados como medio delictivo o es objeto de vulneración que puedan afectar y generar perjuicio en la sociedad, este fenómeno debe ser sancionado. A este tipo de comportamientos dañinos se les denomina Delitos informáticos, Cibercrimen o Ciberdelitos.

DIMENSIONES	**INDICADORES**
1.1.Hurto informático	1.1.1. Denuncia el hurto sistemático de tus cuentas.
	1.1.2. Analiza la legislación peruana por delitos informáticos.
	1.1.3. Conoce la regulación y sanción del hurto informático.
	1.1.4. Promueve la sanción con rigor el hurto informático.
1.2.Fraude informático	1.2.1. Estamos expuestos a ser víctimas de fraude informático.
	1.2.2. Sanción con rigor el fraude informático.
	1.2.3. Analiza que el daño causa un fraude informático.
	1.2.3. Analiza que el daño causa un fraude informático.
1.3.Estafa informática	1.3.1. Genera confianza Comprar y contratar servicios de internet.
	1.3.2.identifica la tipicidad para sancionar la estafa
	1.3.3. Conoce la regulación específica de estafa informática.
	1.3.4. Destruir la red es cometer estafa informática.
1.4.Sabotaje informático	1.4.1. Identifica el principio de tipicidad en el sabotaje informático.
	1.4.2. Aplica la regulación específica del sabotaje informático.
	1.4.3. Conoce la prevención de los delitos informáticos contra el patrimonio.
	1.4.4.Previene que se cometa el sabotaje informático

3.2.2. Variable dependiente: Evidencia digital.

Al respecto Santos (2013). Citando a Casey define que la evidencia digital es "todo aquel dato que pueda establecer que un delito se haya ejecutado o que la misma puede también enlazar entre el crimen y su víctima, el autor del delito, los partícipes, cómplices, etc. (p. 22).

Sobre este punto se puede inferir que la evidencia digital es todo aquel dato que nos proporciona toda la información necesaria, así como también aquel que nos establece cuando un crimen sea ejecutada o consumado y la relación que hubiera con éste, con el autor del delito, sus cómplices y los partícipes, entre otros. Es desde luego, que la evidencia digital se conciba en el campo del derecho penal como aquel que recolecta o almacena datos sobre lo ocurrido en un contexto determinado.

DIMENSIONES	INDICADORES
2.1. Valor probatoria	2.1.1. Reconoce que la evidencia digital es de gran valor.
	2.1.2. Analiza la información jurídica como valor probatorio.
	2.1.3. Teniendo la evidencia digital se puede probar el delito.
	2.1.4. Reconoce el valor probatorio de la informática.
2.2. Alcances de la regulación	2.2.1. Identifica la determinación del daño de manera regular.
	2.2.2. Regula la investigación de la evidencia digital.
	2.2.3. Preparar los alcances en la regulación de la evidencia digital
	2.2.3. Preparar los alcances en la regulación de la evidencia digital
2.3. Informed digital	2.3.1. Reconoce que debe actualizar la información digital.
	2.3.2. Actualizar la información digital para mejores efectos.
	2.3.3. Reconoce que el Estado debe proporcionar facilidades en apoyo a la justicia.
	2.3.4. Identifica la importancia de la información digital.

3.3. Operationalization de Variables.

VARIABLE	DEFINICIÓN CONCEPTUAL	DIMENSIONES	INDICADORES	ESCALA
Variable Independiente **DELITOS INFORMATICOS**	Los primeros antecedentes del delito informático fueron realizados a partir de estudios empíricos llevados en los años 70, desarrollados con base en investigación científica de la rama de la criminológica (División de Investigación y Desarrollo del Consejo Nacional de la Prevención del Delito, 1981), donde se detectó el primer caso de delito informático denominado el caso de Draper Jhon, en Septiembre de 1970, o también como el del Captain Curnch, donde se tenía que descubrir un obsequio y lo que hacía era duplica perfectamente la frecuencia del tono 2600 hz de una línea de WATS permitiéndole hacer llamadas telefónicas gratis y la gran víctima era AT & T. Unos de los primeros temas a definir es el contenido del injusto del denominado "delito informático", pues se trata de un término muy usado para definir conductas en las cuales se constata el uso de la informática o	1.1. Hurto informático 1.2. Fraude informático 1.3. Estafa informática	1.1.1. Denuncia el hurto sistemático de tus cuentas. 1.1.2. Analiza la legislación peruana por delitos informáticos. 1.1.3. Conoce la regulación y sanción del hurto informático. 1.1.4. Promueve la sanción con rigor el hurto informático. 1.2.1. Estamos expuestos a ser víctimas de fraude informático. 1.2.2. Sanción con rigor el fraude informático. 1.2.3. Analiza que el daño causa un fraude informático. 1.2.4. Reconoce las estrategias para prevenir la sanción. 1.3.1. Genera confianza Comprar y contratar servicios de internet. 1.3.2. Identifica la Tipicidad para sancionar la estafa informática.	O R D I N A L

		1.4. Sabotaje informático.	1.3.3. Conoce la regulación específica de estafa informática. 1.3.4. Destruir la red es cometer estafa informática. 1.4.1. Identifica el principio de tipicidad en el sabotaje informático. 1.4.2. Aplica la regulación específica del sabotaje informático. 1.4.3. Conoce la prevención de los delitos informáticos contra el patrimonio. 1.4.4. Previene que se cometa el sabotaje informático...	
Variable Independiente **LA EVIDENCIA DIGITAL**	Al respecto Santos (2013) citando a Casey define que la evidencia digital es "todo aquel dato que pueda establecer que un delito se haya ejecutado o que la misma puede también enlazar entre el crimen y su víctima, el autor del delito, los partícipes, cómplices, etc. (p. 22). Sobre este punto se puede inferir que la evidencia digital es todo aquel dato que nos proporciona toda la información necesaria, así como también aquel que nos establece cuando un crimen sea ejecutada o consumado y la relación que hubiera con éste, con el autor del delito, sus cómplices y los partícipes, entre otros. Es desde luego, que la evidencia digital se conciba en el campo del derecho penal como aquel que recolecta o almacena datos sobre lo ocurrido en un contexto determinado.	2.1. Valor probatorio 2.2. Alcances de la regulación.	2.1.1. Reconoce que la evidencia digital es de gran valor. 2.1.2. Analiza la información jurídica como valor probatorio. 2.1.3. Teniendo la evidencia digital se puede probar el delito. 2.1.4. Reconoce el valor probatorio de la informática. 2.2.1. Identifica la determinación del daño de manera regular. 2.2.2. Regula la investigación de la evidencia digital. 2.2.3. Preparar los alcances en la regulación de la evidencia digital 2.2.4. Se debe regular la celeridad de la evidencia digital	O R D I N A L

		2.3.Informacion digital	2.3.1. Reconoce que debe actualizar la información digital. 2.3.2. Actualizar la información digital para mejores efectos. 2.3.3. Reconoce que el Estado debe proporcionar facilidades en apoyo a la justicia. 2.3.4. Identifica la importancia de la información digital.	

Capitulo IV.

Metodología

4.1. Método de Investigación

4.1.1. Método General.

El Método esgrimido o usado en el actual estudio es el Método Científico que tiene cuatro partes la primera consiste en la formulación del problema, seguido por el planteamiento de la hipótesis, para luego contrastar estas hipótesis, y finalmente se ponen las conclusiones que vendrían a ser las nuevas teorías o las teorías ampliadas o agregadas. (Valderrama, 2002)

Un proceso para revelar los contextos en que se muestran acontecimientos determinados, diferenciado corrientemente por ser tentativo, demostrable, de lógica rigurosa y observación práctica. (Tamayo, 2000)

4.1.2. Método Específico.

Los métodos específicos utilizado en la presente investigación serán; la observación y la experimentación, se interesan por identificar las cualidades y características del hecho y al mismo tiempo manipular las variables. Considerándose a la observación y medición. (Bernal , 2010)

4.2. Tipo de Investigación

El tipo es teórica o básica.

De conformidad a Behar (2008) el estudio es básica o teórica se precisa como: estudio doctrinario, teórico. Se especifica porque se inicia de un cuadro dogmático y persiste en él; el fin reside en formular modernas teorías o cambiar las que existen, en aumentar las sapiencias científicas, pero sin verificarlos.

Poco se inquieta de la aplicabilidad los descubrimientos, por considerar que ello incumbe a otro individuo y no al estudio. Pero, la insuficiencia de diligencia contigua, este modo de indagación pesquisa el adelanto científico y su jerarquía reside en que muestra extensas generalidades y escalas de abstracción con miras a declaraciones dudosas de posible aplicabilidad ulterior. La indagación esencial es un procedimiento formal y metódico de coordinación el método de carácter o de tipo científico de análisis y generalidad con las etapas razonadas e inductivas del raciocinio.

4.3. Nivel de la Investigación.

El estudio por el nivel de investigación en nuestra investigación es: Explorativa, Descriptiva y Correlacional, Según (Hernández, Fernández, & Baptista, 2014) Busca especificar propiedades y características importantes de cualquier fenómeno que se analice. Pretende establecer las causas de los sucesos o fenómenos que se estudian, El nivel de investigación es descriptivo para indagar detallar las características significativos de individuos, conjuntos de personas y colectividades.

4.4. Diseño de la Investigación

El diseño metodológico por la naturaleza del estudió es el no experimental; ya que trata de una investigación donde no hacemos variar intencionalmente las variables independientes según (Hernández, Fernández, & Baptista, 2014)

Y es de tipo Correlacional simple ya que en la presente investigación recopilaremos datos en un momento único según (Hernández, Fernández, & Baptista, 2014)

Esquema del diseño de investigación: X -M- Y

Dónde:

X1: Observación de la variable independiente: Delitos informáticos.

M: Muestra

Y1: Observación de la variable dependiente: La evidencia digital.

r: Relación de causalidad de las variables

4.5. Población y Muestra

4.5.1. Población.

Para Hernández, Fernández, & Baptista, (2014) "una población es el conjunto de todos los casos que concuerdan con una serie de especificaciones". Para la presente investigación "Delitos informáticos y la evidencia digital en el proceso peruano del Distrito judicial de Junin,2020". La población es un conjunto de individuos de la misma clase, limitada por el estudio.

4.5.2. Muestra.

Para el autor Kinnear et al, (1993). El muestreo de carácter estadístico o probabilístico es que la muestra se halla mediante la utilización de la estadística de una población determinada, y este universo es elegido por el investigador.

Criterios de selección de muestra

Estos criterios de inclusión y de exclusión son los siguientes

Criterios de inclusión

La Policía Nacional del Perú, el Fiscal, los Jueces y Operadores de Justicia del Poder Judicial de Junín.

Criterios de exclusión

La muestra es no probabilística, el tipo de muestreo fue por conveniencia, según Carrasco (2005). Considera el investigador selecciona sobre la base de su propio criterio las unidades de análisis, por tanto, consideraremos 40 operadores de derecho para que respondan los cuestionarios acerca de los delitos informáticos y la evidencia digital, de acuerdo a la siguiente tabla:

Operadores de derecho

Policía Nacional del Perú…… 10

Jueces…….10

Operadores de justicia……...10

Abogados……..10

Total……..40

4.6. Técnicas e Instrumentos de recolección de datos.

4.6.1 Técnicas.

Son aquellas que viabilizan hallar la solución a algunos conflictos. Estas son escogidas según el asunto temático que se está estudiando, el fin que se acosa y la razón. Así poseemos:

La revisión documental

Apoyó a examinar los recursos como textos y manuales y ello admitió ejecutar el cuadro doctrinario, así como realizar el estudio de investigaciones parecidas.

Análisis de las normas nacionales

Esta técnica nos consentirá examinar las subsiguientes normas:

-La Carta Magna.

-El CP.

-El NCPP.

-Los antecedentes obligatios o vinculantes

-Se utilizará como técnica la ficha de observación y la encuesta

4.6.2. Instrumentos.

Entre las técnicas tenemos:

Ficha

Se usan fichas de resúmenes. Y fichas de observación.

Cuestionario

Conjunto de interrogaciones formuladas de modo escrita a personas con particularidades específicas, sobre una cuestión en concreto (Bernal, 2010). Hecho en base de una sucesión de preguntas cerradas en relación a las dimensiones y variables, que se aplican a los operadores del Ministerio Público y Abogados.

Confiabilidad.

De acuerdo a Rosas & Zúñiga (2010) la confiabilidad debe ser superior a 0,75 para ser considerada fiable. (Ver Anexo 06-A)

Para la variable 1: Delitos informáticos. Para una prueba con 16 ítems, y 15 cuestionarios.

Estadísticas de fiabilidad
Alfa de Cronbach ,799
N de elementos 16

En el cuadro se puede observar que alfa de cronbach es 0,799, es así que es mayor a 0,75; por tanto, el instrumento es confiable.

Para la variable 2: Evidencia digital. Para una prueba con 12 ítems, y 15 cuestionarios.

Estadísticas de fiabilidad
Alfa de Cronbach ,762
N de elementos 12

En el cuadro se puede observar que alfa de cronbach es 0,762, es así que es mayor a 0,75; por tanto, el instrumento es confiable.

Validez. El instrumento ha sido validado por el Juicio de experto de acuerdo al (VerAnexo 6)

4.7. Técnicas de procesamiento y análisis de datos

Aplicabilidad del Instrumento: Se prorratearon las entrevistas a cada empleado que admitió participar y que anticipadamente firmó la anuencia. Se proporcionaron instrucciones para reconocer las interrogaciones abiertas. Examen de las informaciones: Para el examen de las interrogaciones abiertas, a partir de la leída de las entrevistas, las contestaciones con particularidades análogas se fraccionaron en desiguales categorías.

La información derivada en las entrevistas fue analizada de modo personal por medio de una sábana de datos elaborada en Excel de Microsoft Office, para proporcionar y aligerar el cruce de variables y la edificación de tablas y gráficas.

Para el examen de los datos se esgrimirán cuadros y figuras estadísticas. Para ello se utilizarán los subsiguientes softwares; SPSS - 25, Excel - 2016, que consintieran condenar datos emanados con las instrumentales de recolección de datos.

a) Estadística descriptiva.

Fabricar matriz de puntos que conciernen a las variables y dimensiones de investigación.

Hacer tablas para hallar las frecuencias, con el Programa Excel.

Preparar figuras estadísticas Excel, admitiendo que de modo natural se consigan ver las peculiaridades de las variables de investigación; utilizando asimismo gráficos de barras.

b) Estadística inferencial.

Para obtener y procesamiento de las derivaciones de la verificación de hipótesis, se usó el SPSS V 25. y Rho de Spearman.

Se ejecuta la Prueba de Kolmogorov – Smirnov- Shapirto Wilk con un nivel de significancia al 5%, para hallar la normalidad.

4.8. Aspectos éticos de la investigación

Se asevera la identificación de las personas que ayudaron en la cogida de datos, poseyendo pautas morales y deontológicas, como lo anónimo y la confidencia. Esto significa la imposibilidad de publicar los datos obtenidos para finalidades que diferentes del estudio.

Toda la información recolectada a través de la Ficha de Observación será tratada netamente para hallar los resultados de la presente investigación, sin divulgar los datos para ningún otro fin, manteniendo así la confidencialidad.

Capítulo V

Resultados

5.1. Descripción de resultados.

5.1.1. Resultados de la Variable 1: Delitos Informáticos.

Acerca de la aplicación de la legislación en los Delitos Informáticos en el Proceso Peruano del Distrito Judicial de Junín, 2020.

A. Resultados de delitos informáticos.

Tabla 1. Delitos Informáticos

	Frecuencia	Porcentaje
MUY POCO	0	0.0%
POCO	8	20.0%
MEDIANAMENTE SUFICIENTE	25	62.5%
SUFICIENTE	7	17.5%
SOBRESALIENTE	0	0.0%
Total	40	100.0%

Fuente. En base al cuestionario de delitos informáticos

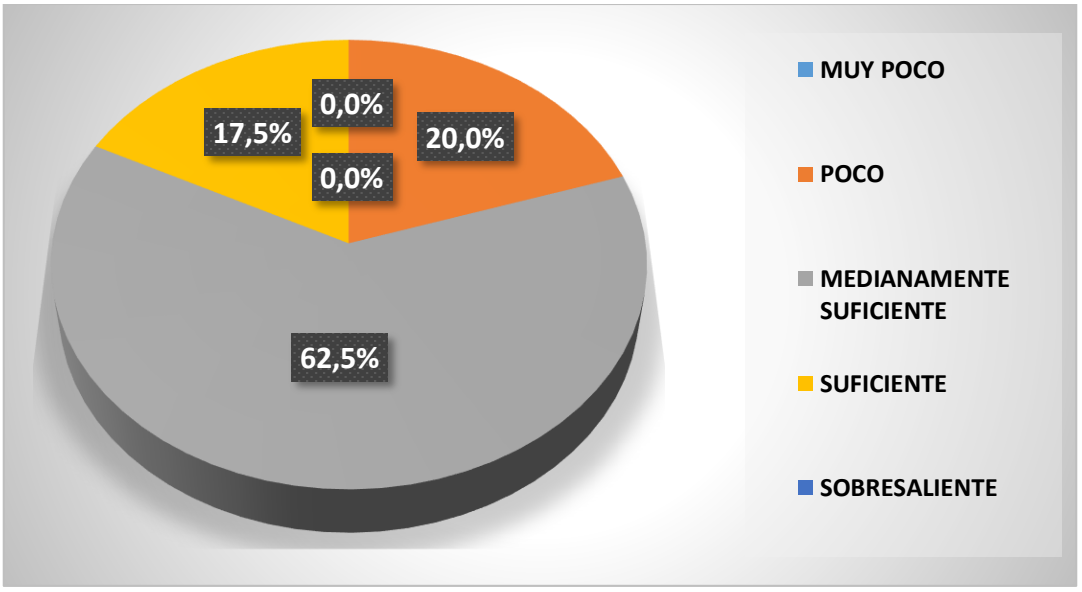


Figura 2. Delitos Informáticos

Interpretación:

Como podemos observar en la tabla 1 y figura 2, el nivel de delitos informáticos es muy poco 0.0%, poco 20.0% medianamente suficiente 62.5%, suficiente 17.5%, sobresaliente 0.0%

Por lo tanto, la mayoría de los operadores de derecho, consideran que el nivel en que se aplica la legislación para los delitos informáticos en el proceso peruano del distrito judicial de Junín, 2020, es medianamente suficiente (62.5%).

B. Resultados de hurto informático.

Tabla 2. Hurto Informático

	Frecuencia	Porcentaje
MUY POCO	5	12.5%
POCO	21	52.5%
MEDIANAMENTE SUFICIENTE	12	30.0%
SUFICIENTE	1	2.5%
SOBRESALIENTE	1	2.5%
Total	40	100.0%

Fuente. En base al cuestionario de delitos informáticos

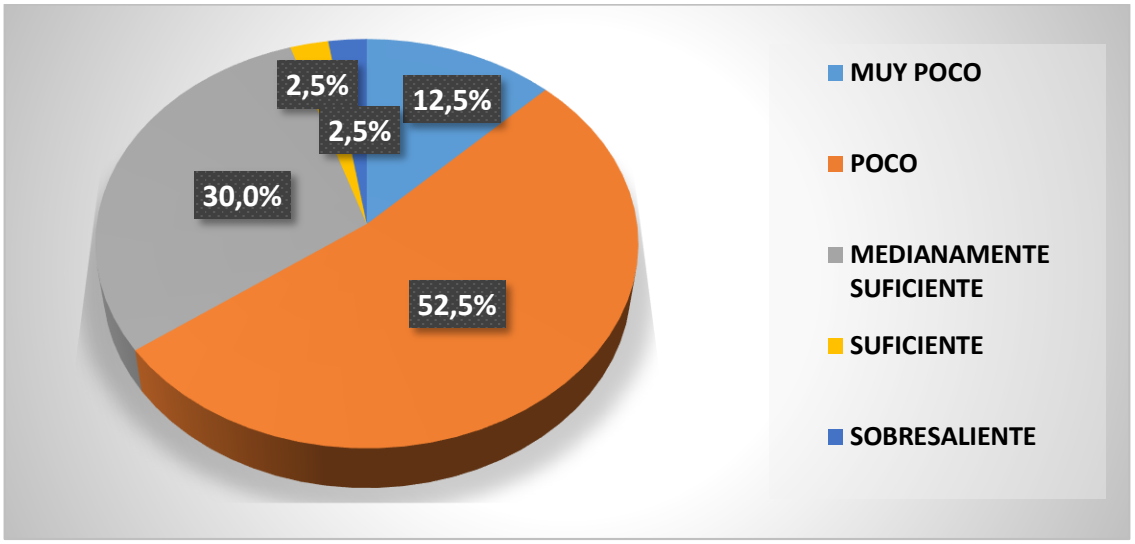


Figura 3. Hurto Informático

Interpretación:

Como podemos observar en la tabla 2 y figura 3, el nivel de hurto informático es muy poco 12.5%, poco 52.5% medianamente suficiente 30.0% suficiente 2.5% sobresaliente 2.5%

Por lo tanto, la mayoría de los operadores de derecho, consideran que el nivel en que se aplica la legislación para el hurto informático en el proceso peruano del distrito judicial de Junín, 2020, es poco (52.5%).

C. Resultados de fraude informático.

Tabla 3. Fraude Informático

	Frecuencia	Porcentaje
MUY POCO	1	2.5%
POCO	4	10.0%
MEDIANAMENTE SUFICIENTE	17	42.5%
SUFICIENTE	16	40.0%
SOBRESALIENTE	2	5.0%
Total	40	100.0%

Fuente. En base al cuestionario de delitos informáticos

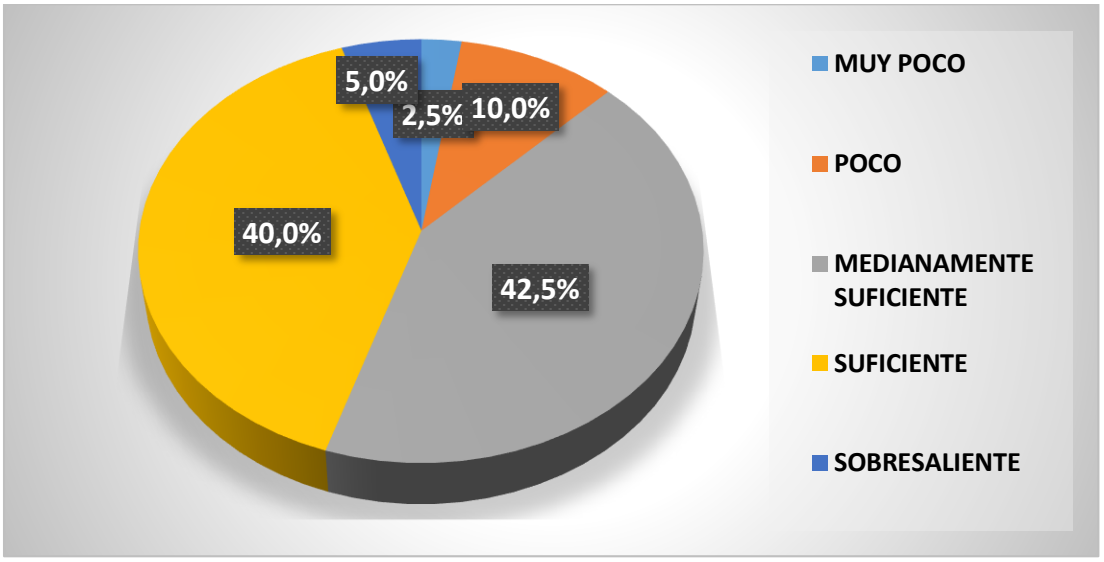


Figura 4. Fraude Informático

Interpretación:

Como podemos observar en la tabla 3 y figura 4, el nivel de fraude informático es muy poco 2.5%, poco 10.0%, medianamente suficiente 42.5%, suficiente 40.0%, sobresaliente 5.0%.

Por lo tanto, la mayoría de los operadores de derecho, consideran que el nivel en que se aplica la legislación en el fraude informático en el proceso peruano del distrito judicial de Junín, 2020 es medianamente suficiente (42.5%)

D. Resultados de estafa informática.

Tabla 4. Estafa Informática

	Frecuencia	Porcentaje
MUY POCO	3	7.5%
POCO	11	27.5%
MEDIANAMENTE SUFICIENTE	19	47.5%
SUFICIENTE	5	12.5%
SOBRESALIENTE	2	5.0%
Total	40	100.0%

Fuente. En base al cuestionario de delitos informáticos

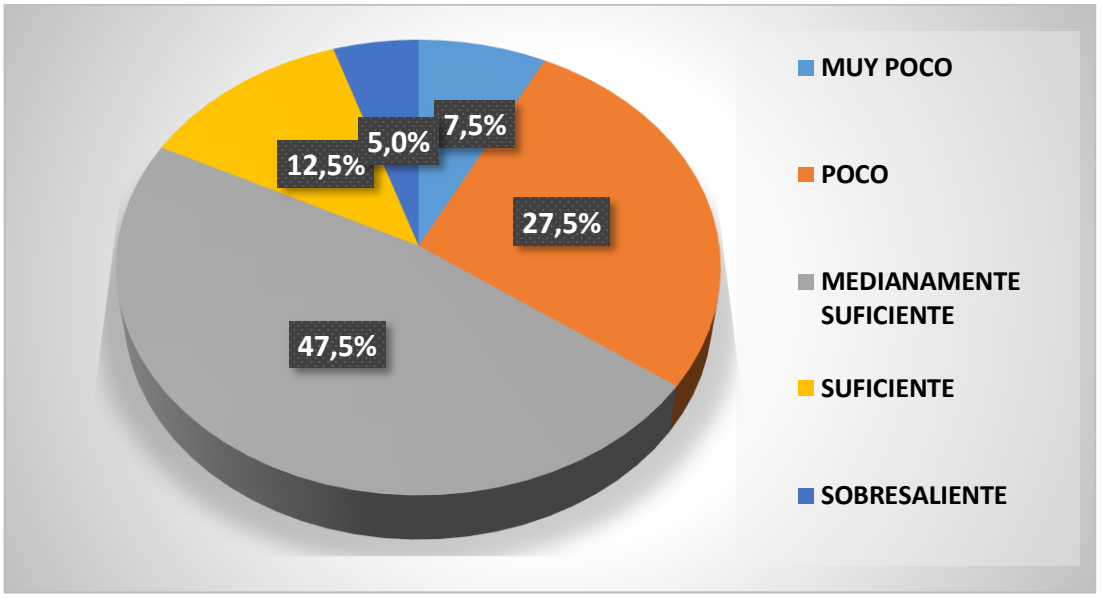


Figura 5. Estafa Informática

Interpretación:

Como podemos observar en la tabla 4 y figura 5, el nivel de estafa informática es muy poco 7.5%, poco 27.5%, medianamente suficiente 47.5%, suficiente 12.5%, sobresaliente 5.0%.

Por lo tanto, la mayoría de los operadores de derecho, consideran que consideran que el nivel en que se aplica la legislación en la estafa informática en el proceso peruano del distrito judicial de Junín, 2020 es medianamente suficiente (47.5%)

E. Resultados de sabotaje informático.

Tabla 5. Sabotaje Informático

	Frecuencia	Porcentaje
MUY POCA	0	0.0%
POCA	7	17.5%
MEDIANAMENTE SUFICIENTE	22	55.0%
SUFICIENTE	6	15.0%
SOBRESALIENTE	5	12.5%
Total	40	100.0%

Fuente. En base al cuestionario de delitos informáticos

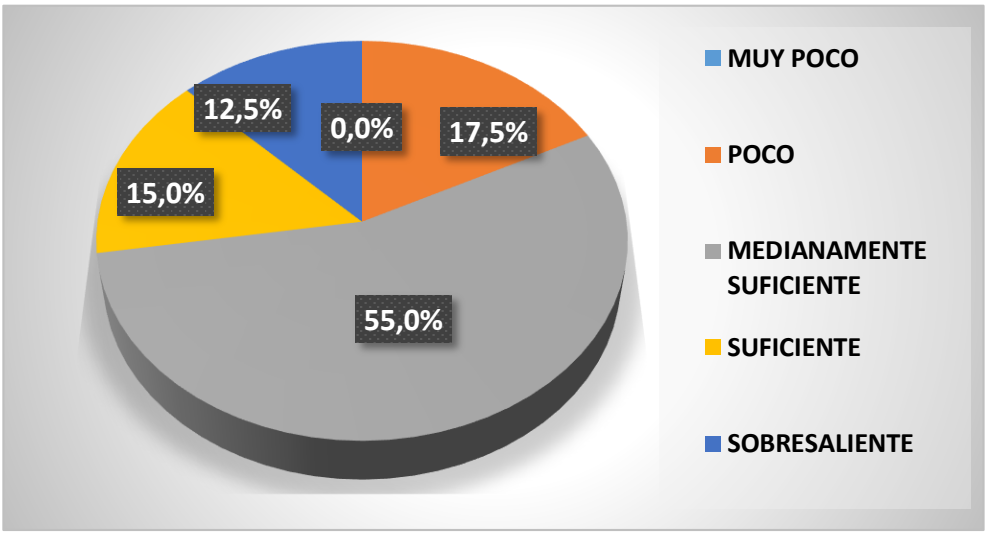


Figura 6. Sabotaje Informático

Interpretación:

Como podemos observar en la tabla 5 y figura 6, el nivel de Sabotaje Informático es muy poco 0.0%, poco 17.5%, medianamente suficiente 55.0%, suficiente 15.0%, sobresaliente 12.5%.

Por lo tanto, la mayoría de los operadores de derecho, consideran que el nivel en que se aplica la legislación en el sabotaje informático en el proceso peruano del distrito judicial de Junín, 2020 es medianamente suficiente (55.0%)

5.1.2. Resultados de la Variable 2: Evidencia Digital.

A. Resultados de evidencia digital.

Tabla 6. Evidencia Digital

	Frecuencia	Porcentaje
MUY BAJO	0	0.0%
BAJO	1	2.5%
MEDIO	4	10.0%
ALTO	19	47.5%
MUY ALTO	16	40.0%
Total	40	100.0%

Fuente. En base al cuestionario de Evidencia Digital

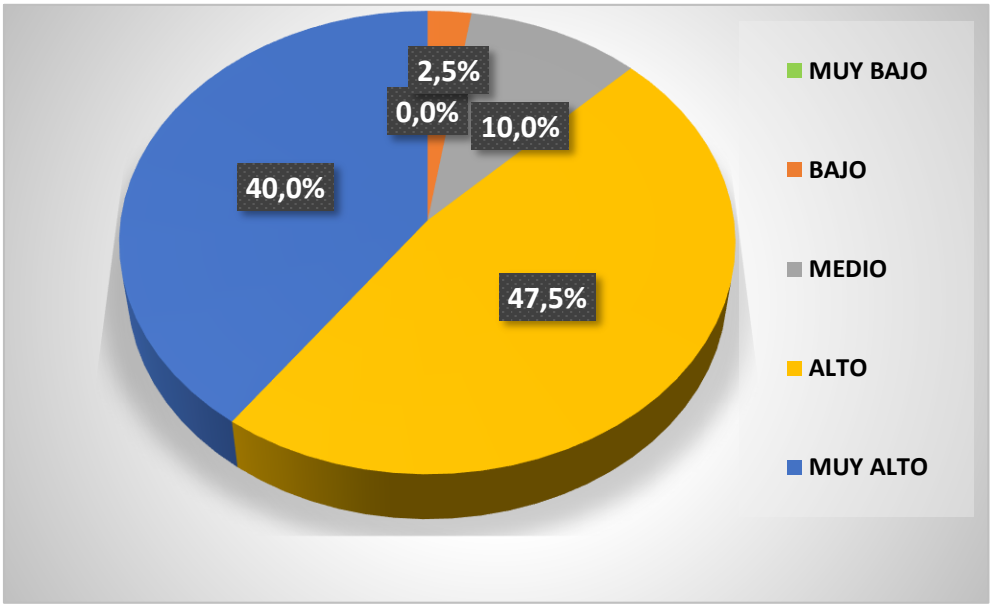


Figura 7. Evidencia Digital

Interpretación:

Como podemos observar en la tabla 6 y figura 7, el nivel de evidencia digital es muy bajo 0.0%, bajo 2.5% medio 10.0% alto 47.5% muy alto 40.0%

Por lo tanto, la mayoría de los operadores de derecho, consideran que el nivel de evidencia digital en el proceso peruano del distrito judicial de Junín, 2020 es muy alto (40.0%).

B. Resultados de valor probatorio.

Tabla 7. Valor Probatorio

	Frecuencia	Porcentaje
MUY BAJO	1	2.5%
BAJO	0	0.0%
MEDIO	8	20.0%
ALTO	24	60.0%
MUY ALTO	7	17.5%
Total	40	100.0%

Fuente. En base al cuestionario de Evidencia Digital

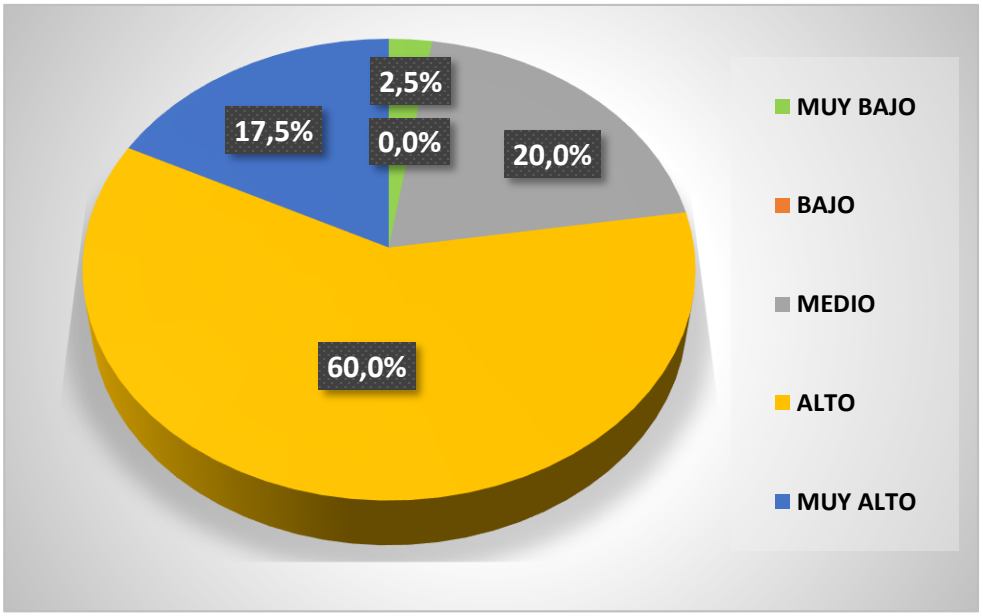


Figura 8. Valor Probatorio

Interpretación:

Como podemos observar en la tabla 7 y figura 8, el nivel de valor probatorio es muy bajo 2.5%, bajo 0.0% medio 20.0% alto 60.0% muy alto 17.5%

Por lo tanto, la mayoría de los operadores de derecho, consideran que el nivel de valor probatorio en el proceso peruano del distrito judicial de Junín, 2020 es alto (60.0%)

C. Resultados de alcances de regulación.

Tabla 8. Alcances de Regulación

	Frecuencia	Porcentaje
MUY BAJO	0	0.0%
BAJO	1	2.5%
MEDIO	10	25.0%
ALTO	15	37.5%
MUY ALTO	14	35.0%
Total	40	100.0%

Área del gráfico

Fuente. En base al cuestionario de Evidencia Digital

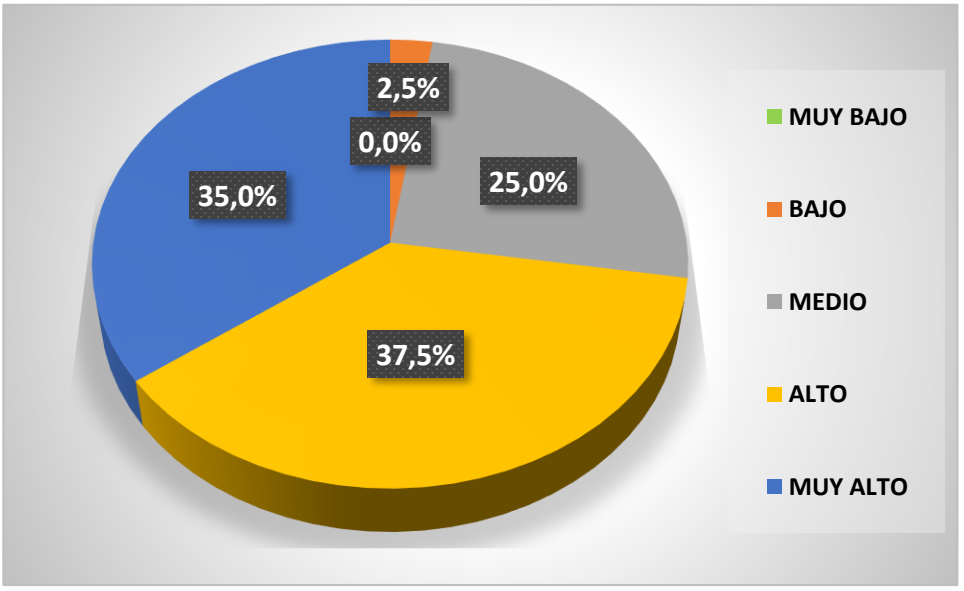


Figura 9. Alcances de Regulación

Interpretación:

Como podemos observar en la tabla 8 y figura 9, el nivel de alcances de regulación es muy bajo 0.0%, bajo 2.5%, medio 25.0%, alto 37.5%, muy alto 35.0%.

Por lo tanto, la mayoría de los operadores de derecho, consideran que el nivel de alcances de regulación en el proceso peruano del distrito judicial de Junín, 2020 es alto (37.5%)

D. resultados de información digital.

Tabla 9. Información Digital

¤	Frecuencia¤	Porcentaje¤
MUY·BAJO¤	1¤	2.5%¤
BAJO¤	1¤	2.5%¤
MEDIO¤	11¤	27.5%¤
ALTO¤	13¤	32.5%¤
MUY·ALTO¤	14¤	35.0%¤
Total¤	40¤	100.0%¤

Fuente. En base al cuestionario de Evidencia Digital

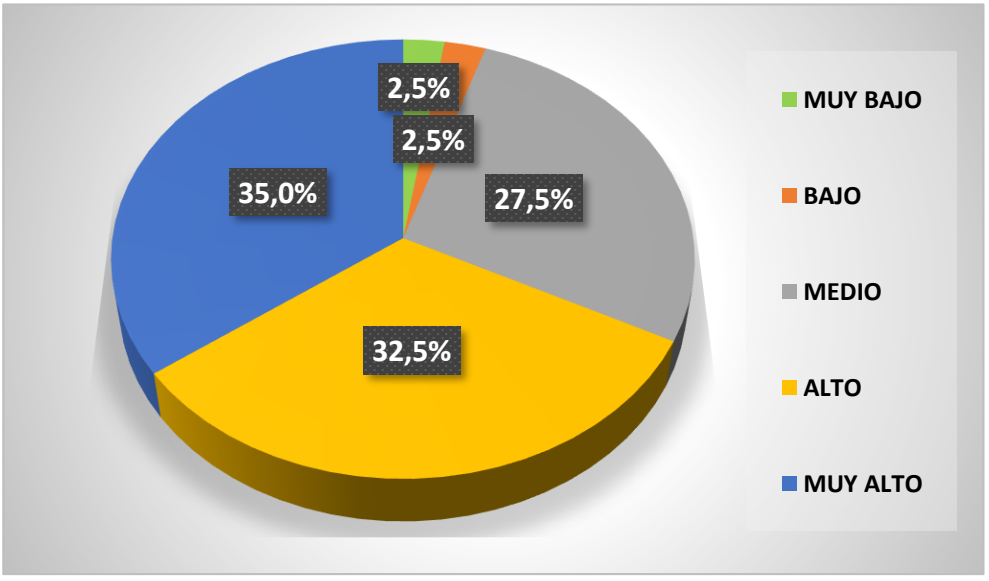


Figura 10. Información Digital

Interpretación:

Como podemos observar en la tabla 9 y figura 10, el nivel de información digital es muy bajo 2.5%, bajo 2.5% medio 27.5% alto 32.5% muy alto 35.0%

Por lo tanto, la mayoría de los operadores de derecho, consideran que el nivel de información digital en el proceso peruano del distrito judicial de Junín, 2020 es muy alto (35.0%).

5.2. Constrastación de hipótesis

5.2.1. Hipótesis general.

Existe una relación directa y significativa entre los delitos informáticos y la evidencia digital en el proceso peruano del Distrito Judicial de Junín, 2020.

Formulación de H_0 y H_1:

H_0: No existe una relación directa y significativa entre los delitos informáticos y la evidencia digital en el proceso peruano del Distrito Judicial de Junín, 2020.

H_1: Si existe una relación directa y significativa entre los delitos informáticos y la evidencia digital en el proceso peruano del Distrito Judicial de Junín, 2020.

Determinación de la significancia y la prueba estadística:

Se utiliza una significancia del 5% (α=0,05). Se hace uso de la prueba no paramétrica **rho de Spearman**, por ser la muestra menor a 50.

Regla de decisión:

Se acepta H_1 si el p-valor ≤ 0,050

Se acepta H_0 si el p-valor > 0,050

Tabla 10. Correlaciones entre Delitos Informáticos y Evidencia Digital

			DELITOS INFORMÁTICOS	EVIDENCIA DIGITAL
Rho de Spearman	DELITOS INFORMÁTICOS	Coeficiente de correlación	1,000	-,010
		Sig. (bilateral)	.	,952
		N	40	40
	EVIDENCIA DIGITAL	Coeficiente de correlación	-,010	1,000
		Sig. (bilateral)	,952	.
		N	40	40

Fuente: Elaboración propia

Interpretación: Se puede observar que el valor de r = - 0,010 entre Delitos Informáticos y Evidencia Digital, lo que indica una Correlación inversa débil (Ver Anexo 06-A) y la significancia (p=0,952>0.05) lo cual evidencia que la relación no es significativa.

Decisión Estadística:

Se acepta la hipótesis nula que dice: No existe una relación directa y significativa entre los delitos informáticos y la evidencia digital en el proceso peruano del Distrito Judicial de Junín, 2020. (p=0,952>0.05)

5.2.1. Hipótesis específica 1.

Existe una relación directa y significativa entre los delitos informáticos y el valor probatorio en el proceso peruano del Distrito Judicial de Junín, 2020.

Formulación de H_0 y H_1:

H_0: No existe una relación directa y significativa entre los delitos informáticos y el valor probatorio en el proceso peruano del Distrito Judicial de Junín, 2020.

H_1: Si existe una relación directa y significativa entre los delitos informáticos y el valor probatorio en el proceso peruano del Distrito Judicial de Junín, 2020

Determinación de la significancia y la prueba estadística:

Se utiliza una significancia del 5% (α=0,05). Se hace uso de la prueba no paramétrica **rho de Spearman**, por ser la muestra menor a 50.

Regla de decisión:

Se acepta H_1 si el p-valor ≤ 0,050

Se acepta H_0 si el p-valor > 0,050

- *Tabla 11. Correlaciones entre Delitos Informáticos y Valor Probatorio*

			DELITOS INFORMÁTICOS	VALOR PROBATORIO
Rho de Spearman	DELITOS INFORMÁTICOS	Coeficiente de correlación	1,000	-,078
		Sig. (bilateral)	.	,632
		N	40	40
	VALOR PROBATORIO	Coeficiente de correlación	**-,078**	1,000
		Sig. (bilateral)	**,632**	.
		N	40	40

Fuente: Elaboración propia

Interpretación: Se puede observar que el valor de r = - 0,010 entre Delitos Informáticos y Valor Probatorio, lo que indica una Correlación inversa moderada (Ver Anexo 06-A) y la significancia (p=0,632>0.05) lo cual evidencia que la relación no es significativa.

Decisión Estadística:

Se acepta la hipótesis nula que dice: No existe una relación directa y significativa entre los delitos informáticos y el valor probatorio en el proceso peruano del Distrito Judicial de Junín, 2020. (p=0,632>0.05)

5.2.2. Hipótesis específica 2.

Existe una relación directa y significativa entre los delitos informáticos y los alcances de la regulación en el proceso peruano del Distrito Judicial de Junín, 2020.

Formulación de H_0 y H_1:

H_0: No existe una relación directa y significativa entre los delitos informáticos y los alcances de la regulación en el proceso peruano del Distrito Judicial de Junín, 2020.

H_1: Si existe una relación directa y significativa entre los delitos informáticos y los alcances de la regulación en el proceso peruano del Distrito Judicial de Junín, 2020.

Determinación de la significancia y la prueba estadística:

Se utiliza una significancia del 5% (α=0,05). Se hace uso de la prueba no paramétrica **rho de Spearman**, por ser la muestra menor a 50.

Regla de decisión:

Se acepta H_1 si el p-valor ≤ 0,050

Se acepta H_0 si el p-valor > 0,050

Tabla 12. Correlaciones entre Delitos Informáticos y Alcances de la regulación

			DELITOS INFORMÁTICOS	ALCANCES DE LA REGULACIÓN
Rho de Spearman	DELITOS INFORMÁTICOS	Coeficiente de correlación	1,000	,108
		Sig. (bilateral)	.	,509
		N	40	40
	ALCANCES DE LA REGULACIÓN	Coeficiente de correlación	,108	1,000
		Sig. (bilateral)	,509	.
		N	40	40

Fuente: Elaboración propia

Interpretación: Se puede observar que el valor de r = 0.108 entre Delitos Informáticos y Alcances de la regulación, lo que indica una Correlación directa débil (Ver Anexo 06-A) y la significancia (p=0,509>0.05) lo cual evidencia que la relación no es significativa.

Decisión Estadística:

Se acepta la hipótesis nula que dice: No existe una relación directa y significativa entre los delitos informáticos y los alcances de la regulación en el proceso peruano del Distrito Judicial de Junín, 2020. (p=0,509>0.05)

5.2.3. Hipótesis específica 3.

Existe una relación directa y significativa entre los delitos informáticos y la Información digital en el proceso peruano del Distrito Judicial de Junín, 2020.

Formulación de H_0 y H_1:

H_0: No existe una relación directa y significativa entre los delitos informáticos y la Información digital en el proceso peruano del Distrito Judicial de Junín, 2020.

H_1: Si existe una relación directa y significativa entre los delitos informáticos y la Información digital en el proceso peruano del Distrito Judicial de Junín, 2020.

Determinación de la significancia y la prueba estadística:

Se utiliza una significancia del 5% (α=0,05). Se hace uso de la prueba no paramétrica **rho de Spearman**, por ser la muestra menor a 50.

Regla de decisión:

Se acepta H_1 si el p-valor ≤ 0,050

Se acepta H_0 si el p-valor > 0,050

Tabla 13. Correlaciones entre Delitos Informáticos y Alcances de la regulación

			DELITOS INFORMÁTICOS	INFORMACIÓN DIGITAL
Rho de Spearman	DELITOS INFORMÁTICOS	Coeficiente de correlación	1,000	-,024
		Sig. (bilateral)	.	,884
		N	40	40
	INFORMACIÓN DIGITAL	Coeficiente de correlación	-,024	1,000
		Sig. (bilateral)	,884	.
		N	40	40

Fuente: Elaboración propia

Interpretación: Se puede observar que el valor de r = -0.024 entre Delitos Informáticos y Alcances de la regulación, lo que indica una Correlación inversa débil (Ver Anexo 06-A) y la significancia (p=0,884>0.05) lo cual evidencia que la relación no es significativa.

Decisión Estadística:

Se acepta la hipótesis nula que dice: No existe una relación directa y significativa entre los delitos informáticos y la Información digital en el proceso peruano del Distrito Judicial de Junín, 2020. (p=0,884>0.05)

Discusión de Resultados

Los resultados del objetivo general muestran que No existe una relación directa y significativa entre los delitos informáticos y la evidencia digital en el proceso peruano del Distrito Judicial de Junín, 2020. (p=0,952>0.05). Donde la mayoría de los operadores de derecho, consideran que el nivel en que se aplica la legislación para los delitos informáticos en el proceso peruano del distrito judicial de Junín, 2020 es medianamente suficiente (62.5%). Y la mayoría de los operadores de derecho, consideran que el nivel de evidencia digital en el proceso peruano del distrito judicial de Junín, 2020 es muy alto (40.0%).

En este sentido se tiene investigaciones con resultados similares como la de Sequeiros (2016) donde el autor señala la existencia de vacíos legales que imposibilitan la sanción de los delitos informáticos en el Nuevo Código Penal Peruano, asimismo incide que la naturaleza virtual de los delitos informáticos se vuelve confusos en su tipificación, pero es urgente que se prepare a la población de la Región Junín, para contrarrestar las malas acciones de los ciberdelincuentes y así evitar que cometan los delitos informáticos contra el patrimonio.

Donde la base teórica según La Interpol (2013) caracteriza los delitos de tipo o de carácter informáticos como: Agresiones contra datos de tipo o de carácter informático, Usurpación de la identificación, Repartición de retratos de ataques sexuales a menores de edad, Estafas mediante Internet, Intromisión en servicios bancarios en línea, Propagación de virus, Botnets y el Phishing. Acerca de la evidencia digital Santos (2013) citando a Casey define que la evidencia digital es “todo aquel dato que pueda establecer que un delito se haya ejecutado o que la misma puede también enlazar entre el crimen y su víctima, el autor del delito, los partícipes, cómplices, etc. Es entonces que de acuerdo al problema planteado en la legislación penal peruana no se cumple con el principio de tipicidad para la sanción del delito de hurto informático, sabotaje informático, estafa informática y es bastante genérica y

dentro de fraude informático se pretende comprender todas las modalidades de delitos informáticos muy a pesar de contar con evidencias digitales, lo cual se hace evidente en los resultados donde se observa que las leyes acerca de los delitos informáticos se perciben de acuerdo a la presente investigación como medianamente suficiente (62.5%) y la evidencia digital se ha percibido con un nivel es muy alto (40.0%).

Los resultados del objetivo específico 1 muestran que No existe una relación directa y significativa entre los delitos informáticos y el valor probatorio en el proceso peruano del Distrito Judicial de Junín, 2020. (p=0,632>0.05). Donde la mayoría de los operadores de derecho, consideran que el nivel de valor probatorio en el proceso peruano del distrito judicial de Junín, 2020 es alto (60.0%)

En este sentido, no se cuenta con antecedentes similares acerca del valor probatorio en la presente investigación; y acerca de la base teórica según Santos (2013) señala que la evidencia digital busca de alguna manera darle valor legal a la información encriptada en ella y ser admitida en el proceso previamente que ella haya sido sometida de un estudio o investigación por parte de expertos científicos, forenses o peritos especialistas a corroborar su autenticidad.

Los resultados del objetivo específico 2 muestran que No existe una relación directa y significativa entre los delitos informáticos y los alcances de la regulación en el proceso peruano del Distrito Judicial de Junín, 2020. (p=0,509>0.05). Donde la mayoría de los operadores de derecho, consideran que el nivel de alcances de regulación en el proceso peruano del distrito judicial de Junín, 2020 es alto (37.5%)

En este sentido se tiene investigaciones con resultados similares como la González (2013) afirma que la informática tiene un carácter trasnacional, por lo que nunca es suficiente la regulación protectora en un único Estado, no existe ausencia en la regulación eficiente en

los demás o resto de Estados, puesto que, para la comisión de los delitos informáticos, no se requiere la cercanía física, puede hacerlo tan lejos como el medio de comunicación o el internet tiene alcance.

Donde la base teórica precisa que de la invención de la computadora y su posterior implementación de las redes informáticas, internet y otras sistemas informáticos, el derecho se vio obligado a regular aspectos vinculados a la informática aunque en forma retrasada, en los diversos ámbitos y especialmente en el ámbito comercial, sin embargo, lo es también la necesidad de regular en el ámbito penal debido a que las conductas ahí desarrolladas constituyen intolerables por la sociedad, es así como nace el derecho informático y específicamente el derecho penal informático, dada la necesidad de sancionar conductas que afectan bienes jurídicos penalmente relevantes.

Los resultados del objetivo específico 3 muestran que No existe una relación directa y significativa entre los delitos informáticos y la Información digital en el proceso peruano del Distrito Judicial de Junín, 2020. ($p=0,884>0.05$). Donde la mayoría de los operadores de derecho, consideran que el nivel de evidencia digital en el proceso peruano del distrito judicial de Junín, 2020 es muy alto (40.0%)

En este sentido se tiene investigaciones con resultados similares como la Sánchez (2017), quien concluye que la adopción de estrategias de ciberseguridad incide significativamente en la protección de la información en la oficina de economía del ejército, y entre otras conclusiones señala que en la oficina de economía del ejército no existen planes de protección contra ciberterrortistas y se ponen en ejecución y que los dispositivos con las que cuenta el ejército no son de última generación, por lo que no se garantiza la protección de la alteración de la información.

Donde la base teórica según, precisa el autor Ramírez, el objeto de la Ley es la

protección del individuo con respecto a la base de datos y a los sistemas computarizados ilegales, en donde la protección legal es base para la protección de la intimidad de los individuos.

Conclusiones

1. Se ha determinado que los resultados del objetivo general muestran que No existe una relación directa y significativa entre los delitos informáticos y la evidencia digital en el proceso peruano del Distrito Judicial de Junín, 2020. (p=0,952>0.05). Donde la mayoría de los operadores de derecho, consideran que el nivel en que se aplica la legislación para los delitos informáticos en el proceso peruano del distrito judicial de Junín, 2020 es medianamente suficiente (62.5%). Y la mayoría de los operadores de derecho, consideran que el nivel de evidencia digital en el proceso peruano del distrito judicial de Junín, 2020 es muy alto (40.0%).

2. Se ha determinado que los resultados del objetivo específico 1 muestran que No existe una relación directa y significativa entre los delitos informáticos y el valor probatorio en el proceso peruano del Distrito Judicial de Junín, 2020. (p=0,632>0.05). Donde la mayoría de los operadores de derecho, consideran que el nivel de valor probatorio en el proceso peruano del distrito judicial de Junín, 2020 es alto (60.0%)

3. Se ha determinado que los resultados del objetivo específico 2 muestran que No existe una relación directa y significativa entre los delitos informáticos y los alcances de la regulación en el proceso peruano del Distrito Judicial de Junín, 2020. (p=0,509>0.05). Donde la mayoría de los operadores de derecho, consideran que el nivel de alcances de regulación en el proceso peruano del distrito judicial de Junín, 2020 es alto (37.5%)

4. Se ha determinado que los resultados del objetivo específico 3 muestran que No existe una relación directa y significativa entre los delitos informáticos y la Información digital en el proceso peruano del Distrito Judicial de Junín, 2020. (p=0,884>0.05). Donde la mayoría de los operadores de derecho, consideran que el nivel de evidencia digital en el proceso peruano del distrito judicial de Junín, 2020 es muy alto (40.0%)

Recomendaciones

- 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.
- Los ciudadanos, que están en contacto de las tecnologías de la información y la comunicación, como correos electrónicos, chats, transacciones electrónicas y el uso de las redes sociales, deben precautelar su propia seguridad y limitar el acceso a estas plataformas en lugares públicos.
- 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.
- Si realiza transacciones bancarias en línea, efectué las transacciones bancarias y pagos de servicios desde su hogar por internet, de esa manera evitará exponerse en la calle a los delincuentes.
- Si una persona ha sido víctima de un delito, debe acudir inmediatamente a denunciarlo en las oficinas más cercanas de la Policía Nacional. Recuerde que al denunciar el delito, contribuirá a que la Fiscalía conozca cómo opera la delincuencia y pueda tomar medidas preventivas encaminadas a disminuir la impunidad y criminalidad del país.

Referencias Bibliográficas

Referencias Bibliográficas

Abdulai. (2016). *Determinantes del miedo a la victimización del crimen de cibernética, un estudio del fraude a la tarjeta de crédito entre estudiantes de la Universidad de Saskatchewan".* Tesis que se sustentó en el Departamento de Sociología de la Universidad de Saskatchewan.

Abdulai. (2016). *Determinantes del miedo a la victimización del crimen de cibernética: un estudio del fraude a la tarjeta de crédito / débito entre estudiantes de la Universidad de Saskatchewan.* Para optar el grado de Magister en Artes. Canadá.

Adame, M. (1998). *Derecho en Internet.* . Sevilla, España, Edit. Mergablum. .

Aggarwal, P., Arora, P., Ghai, R., & Poonam. (2014). *Revisión sobre crimen cibernético y seguridad.* Revista Internacional de Investigación en Ingeniería y Ciencias Aplicadas.

Aguilar, D., & Said, E. (2010). *Identidad y subjetividad en las redes sociales virtuales: caso de Facebook.* Red de Revistas Científicas de América Latina, el Caribe, España y Portugal.

Aguilar, D., & Said, E. (2010). *Identidad y Subjetividad en las redes sociales: Caso de Facebook.*

Alanezi. (2015). *Las percepciones de fraude en línea y el impacto sobre las contramedidas para el control del fraude en línea en las instituciones financieras de Arabia Saudí.* Para optar el grado de Doctor en Filosofía Universidad Brunel de London.

Alarcón, & Barrera. (2016). *Uso de internet y delitos informáticos en los estudiantes de Primer Semestre de la Universidad Pedagógica y Tecnológica de Colombia, Sede Seccional*

Sogamoso 2016",. sustentada en la Escuela de Posgrado de la Universidad Privada Norbert Wiener para optar el grado académico de maestro en informática.

Alcívar, C., Domenech, G., & Ortiz, K. (2015). *La seguridad jurídica frente a los delitos informáticos.* . Revista de Investigación Jurídica.

Alvarado. (2009). *Competencia, acción y pensamiento: una mirada a las posibilidades de uso del concepto de competencia en la pedagogía.* Revista Científica «Gereral José Maria Córdoba».

Alvarado. (2009). *Competencia, acción y pensamiento: una mirada a las posibilidades de uso del concepto de competencia en la pedagogía.* Revista Científica Gereral José Maria Córdoba.

Anderson, R. . (2008). *Implications of the information and knowledge society for education. In J.* .

Anderson, R. (2008). *Implications of the information and knowledge society for education. In J. Voogt & G. Knezek (Eds.), International handbook of information technology in primary and secondary education (pp. 5-22).* . New York: Springer.

Becerril, L., & Badia, A. (2013). *La competencia informacional en la educación secundaria. Demanda de aprendizaje y resolución colaborativa de problemas relativos a la información con apoyo de las TIC.* Revista De Educación.

Brazuelo, F., & Gallego, D. (2014). *Estado del Mobile Learning en España.* Educar em Revista, 99-128.

Campbell, C., Swift, C., & Denton, L. (2000). *Cheating goes hi-tech: Online term paper mills.* Journal of Management Education.

Canto, P., & Benois, N. (2009). *Estudio acerca de la ética profesional en estudiantes de posgrado en una universidad pública, en Pedro Canto (coord.),* . Ética en la universidad: conceptos y enfoques, Mérida (Yucatán), Unas Letras Industria Editorial.

Chapman, W., & Malhck, O. (2004). *Adapting Technology for School Improvement: A Local Perspective* . Paris: IIEP.

Chapman, W., & Malhck, O. (2004). *Adapting Technology for School Improvement: A Local Perspective* . *Paris: IIEP-UNESCO.*

CNA. (2000). *Art. I del Título Preliminar.*

Código Penal. (1991). *Artìculo 148 del Código Penal.*

Comas, R., Sureda, A., & Morey. (2011). *La integridad académica entre el alumnado universitario español.* . Estudios pedagógicos (Valdivia).

Diccionario Español Jurídico de la RAE. (2016). *Definición de términos.*

Diccionario Español Jurídico de la RAE. (2017). *Definiciones.*

División de Investigación y Desarrollo del Consejo Nacional de la Prevención del Delito. (1981). *Informática y Delito. Estados Unidos.*

Dudas legislativas.com. (2018). *Definición de Indemnidad Sexual.*

Empírica. (2007). *Digital literacy and ICT skills. Bonn and Brussels: empirica: Gesellschaft für Kommunikations- und Technologieforschung mbH.*

Espinoza. (2017). *Derecho penal informático: deslegitimación del poder punitivo en la sociedad de control", que sustentó en la Facultad de Ciencias Jurídicas y Políticas de la Universidad Nacional del Altiplano.* Para optar el Título Profesional de Abogado.

Ferreira, & Dudziak. (2004). *La alfabetización informal para la ciudadanía en América latina: el punto de vista del usuario final de programas nacionales de información y/o inclusión digital. Memoria; World Library an information.* Congress: 70 th IFLA General Conference and Council. Buenos Aires.

García, C. (2017). *Los delitos de estafas y sus consecuencias a través de las redes sociales.* . Babahoyo Ecuador: Universidad Regional Autónoma de los Andes – UNIANDES.

Garrido, M. (1992). *Nociones Fundamentales de la Teoría del Delito.* Edit. Jurídica de Chile.

Gil, G. (2007). *Derecho informático.* Grupo digital Megabite SAC.

González & Barbosa. (2013). *Delincuencia informática: daños informáticos del artículo 264 del Código Penal y propuesta de Reforma".* Sustentada en la Facultad de Derecho, Departamento de Derecho Penal de la Universidad Complutense de Madrid-España, para optar el Grado de Doctor.

Hernández, F. (1997). *Delitos Informáticos.* Ponencia Jornadas sobre el Marco Legal y Deontológico de la Informática, Mérida.

Herrera, L. (2018). *Eficacia de la ley de delitos informáticos en el Distrito Judicial de Huánuco 2017.* . Huánuco: Universidad de Huánuco.

López, A., López, L., & Jerónimo, G. (2017). *Factores que contribuyen a la prevención de los delitos informáticos en el Estado de Tabasco.* Revista Gênero & Direito.

Martín, A., & Birke, A. (2004). *"Panorama general sobre los principios éticos aplicables a la investigación científica y la educación superior".* México.

Montiel-Overall, P. (2007). *Information Literacy: Toward a Cultural Model.* . Canadian Journal of Information and Library Science. Information Literacy .

Nuñez, J. (2016). *Derecho de Identidad Digital en Internet.* Pesentada en la Universidad Nacional Mayor de San Marcos-Peru para optar el Grado de Doctor.

Ñaupas, H., Mejía, E., Novoa, E., & Villagómez, A. (2014). *Metodología de la investigación.* Tercera edición, Perú.

OCDE. (2001). *Los desafios de las tecnologías de la información en la educación.* . Organización para la Cooperación y Desarrollo Económicos (OCDE) y Ministerio de Educación, Cultura y Deporte. España.

OCDE, 2001 . (n.d.). *Aprender a cambiar tics en las escuelas.*

Osborne, J., & Hennessy, S. (2003). *Literature review in science education and the role of ICT: Promise, problems and future directions.* . Bristol: Futurelab.

Osborne, J., & Hennessy, S. (2003). *Literature review in science education and the role of ICT: Promise, problems and future directions.* . Bristol: Futurelab.

Parra. (2016). *Proyecto legal para un Esquema Nacional de Ciber Seguridad.* Para optar el Título de Abogado, de la Universidad de San Martín de Porres de Lima.

Piccirilli. (2015). *Protocolos a aplicar en la Forensia Informática en el marco de las nuevas tecnologías (Pericia – Forensia y Cibercrimen)" que sustentó en la Facultad de Informática de la Universidad Nacional de La Plata* . Para optar el grado de doctor en Ciencias Informáticas.

Ramos, C. (2011). *Como hacer una tesis de derecho y no envejecer en el intent.* . Lima: Editorial San Marcos.

Rayon, M., & Gomez, J. (2014). *Cibercrimen: particularidades en su investigación y enjuiciamiento.* . Universidad Complutense de Madrid. Madrid - España.

Reusser, C. (2003). *Internet, Conceptos Generales.* Santiago, Chile, Centro de Estudios de Derecho Informático, Universidad de Chile. 2p.

Rincón, J. (2015). *El delito en la cibersociedad y la justicia penal internacional.* Para optar el Título de Doctorado, de la Universidad Complutense de Madrid.

Rincón, J. (2015). *El delito en la cibersociedad y la justicia penal internacional.* Para optar el Título de Doctorado, en la Universidad Complutense de Madrid;.

Rychen, D., & Salganik, H. (2003). *Key Competencias for a Successful Life and a WellFunctioning Society. Hogrefe & Huber.*

Rosas, & Zúñiga. (2010). *Estadística Descriptiva E Inferencial I. Fascículo 3. Correlación y regresión lineales.* . Colegio de Bachilleres.

Sánchez. (2017). *Adopción de estrategias de Ciberseguridad en la protección de la información en la Oficina de Economía del Ejército, San Borja- 2017" sustentada en*

la Escuela de Posgrado del Instituto Científico Tecnológico del Ejército . Para optar el grado académico de Magister.

Santos, J. (2013). *Procedimientos en la investigación, recolección y manejo de la evidencia digital en la escena del crimen.* . Guegueteneango, Guatemala URL.

Sequeiros. (2016). *Vacíos legales que imposibilitan la sanción de los delitos informáticos en el Nuevo Código Penal Peruano-2015" sustentada en la Facultad de Derecho y Ciencias Políticas de la Universidad de Huánuco.* Para optar el Título Profesional de Abogado.

SITES. (2006). *Resultados Nacionales SITES 2006, Second Information Technology and Education Study - SITES 2006.* . Centro de Educación y Tecnología del Ministerio de Educación, Santiago, Chile.

Tamayo, M. (2000). *El proceso de la investigación científica.* Limusa, México.

Tenorio, & Tuesta. (2012). *Legislación del secreto bancario y su relación con el delito de hurto informático de dinero mediante la violación de claves secretas, Iquitos- 2010".* Para optar el Grado Académico de Magister en Derecho y Ciencias Penales.

UNESCO. (2008). *El Desafío mundial de la alfabetización. Perfil de la alfabetización de jóvenes y adultos a mediados del Decenio de las Naciones Unidas de la Alfabetización 2003-2012.* . UNESCO. Recuperado de: http://unesdoc.unesco.org/images/0016/0016.

Vásquez, C., Regalado, J., & Guadron, R. (2017). *Cibercrimen e informática forense: introducción y análisis en El Salvador.* . Revista Tecnológica.

Villavicencio, F. (2014). *Delitos informáticos.* . IUS ET VERITAS, 24(49), 284-304.

Villavicencio, F. (2014). *Delitos Informáticos en La Ley 30096 y La Modificación de la Ley 30071* . Lima – Perú.

Wall, D. (2015). *Crimen desorganizado: hacia un modelo distribuido de la organización del cibercrimen.* La Revista Europea del crimen organizado. Sgocnet.

Wang. (2016). *Estudio comparativo de la ciberdelincuencia en Derecho Penal: China, Estados Unidos, Inglaterra, Singapur y el Consejo de Europa".* Que sustentó en la Universidad Erasmo de Rotterdam para optar el Grado de Doctor,.

Wang. (2016). *Estudio comparativo de la ciberdelincuencia en Derecho Penal: China, Estados Unidos, Inglaterra, Singapur y el Consejo de Europa" que sustentó en la Universidad Erasmo de Rotterdam.* Para optar el grado de Doctor.

Anexos

Anexo 1: Matriz de Consistencia

TÍTULO: LOS DELITOS INFORMÁTICOS Y LA EVIDENCIA DIGITAL EN EL PROCESO PERUANO DEL DISTRITO JUDICIAL DE JUNIN, 2020.

I. PROBLEMA	II. OBJETIVO	III. HIPÓTESIS	IV: VARIABLES Y DIMENSIONES	V. METODOLOGÍA
PROBLEMA GENERAL ¿Cuál es la relación que se da entre los delitos informáticos y la evidencia digital en el proceso peruano del Distrito Judicial de Junín, 2020? **PROBLEMA ESPECÍFICO** 1.- ¿Cuál es la relación que se da entre los delitos informáticos y el valor probatorio en el proceso peruano del Distrito Judicial de Junín, 2020? 2.-¿Cuál es la relación que se da entre los delitos informáticos y los alcances de la regulación en el proceso peruano del Distrito Judicial de Junín, 2020?	**OBJETIVO GENERAL:** Determinar la relación entre los delitos informáticos y la evidencia digital en el proceso peruano del Distrito Judicial de Junín, 2020. **OBJETIVOS ESPECÍFICOS** 1. Determinar la relación entre los delitos informáticos y el valor probatorio en el proceso peruano del Distrito Judicial de Junín, 2020. 2. Determinar la relación entre los delitos informáticos y los alcances de la regulación en el proceso peruano del Distrito Judicial de Junín, 2020. 3. Determinar la relación entre los delitos informáticos y la información digital en el	**HIPÓTESIS GENERAL** Existe una relación directa y significativa entre los delitos informáticos y la evidencia digital en el proceso peruano del Distrito Judicial de Junín, 2020. **HIPÓTESIS ESPECÍFICAS** 1.- Existe una relación directa y significativa entre los delitos informáticos y el valor probatorio en el proceso peruano del Distrito Judicial de Junín, 2020. 2.- Existe una relación directa y significativa entre los delitos informáticos y los alcances de la regulación en el proceso peruano del Distrito Judicial de Junín, 2020. 3**.-** Existe una relación directa y significativa entre los delitos	Variable independiente **DELITOS INFORMATICOS** Dimensiones 1.-Hurto informático. 2.-Fraude informático. 3.-Estafa informática. 4.-Sabotaje informático. Variable dependiente **EVIDENCIA DIGITAL** Dimensiones: 1.-Valor probatorio 2.-Alcances de la regulación. 3.-Informacion digital	• **MÉTODO:** Científico **Métodos particulares** Inductivo Deductivo Analítico Sintético • **TIPO DE INVESTIGACIÓN** Pura o básica • **NIVEL DE INVESTIGACIÓN** Exploratorio-Explicativo-Correlacional • **DISEÑO DE INVESTIGACIÓN** Correlacional Simple • **POBLACIÓN** Nuestra población está conformada por 40 de del distrito judicial de Junín, 2020.

3.- ¿Cuál es la relación que se da entre los delitos informáticos y la información digital en el proceso peruano del Distrito Judicial de Junín, 2020?	proceso peruano del Distrito Judicial de Junín, 2020.	informáticos y la Información digital en el proceso peruano del Distrito Judicial de Junín, 2020.		• **MUESTRA** El muestreo es no probabilística y censal, por lo tanto, se considerará el total de la población, es decir, 40 de del distrito judicial de Junín, 2020. **TECNICAS E INSTRUMENTOS DE RECOLECCIÓN DE DATOS** Encuesta y cuestionario

Anexo 02: Matriz de Operacionalización de Variables

VARIABLE	DEFINICIÓN CONCEPTUAL	DIMENSIONES	INDICADORES	ESCALA
Variable Independiente **DELITOS INFORMATICOS**	Los primeros antecedentes del delito informático fueron realizados a partir de estudios empíricos llevados en los años 70, desarrollados con base en investigación científica de la rama de la criminológica (División de Investigación y Desarrollo del Consejo Nacional de la Prevención del Delito, 1981), donde se detectó el primer caso de delito informático denominado el caso de Draper Jhon, en Septiembre de 1970, o también como el del Captain Curnch, donde se tenía que descubrir un obsequio y lo que hacía era duplica perfectamente la frecuencia del tono 2600 hz de una línea de WATS permitiéndole hacer llamadas telefónicas gratis y la gran víctima era AT & T. Unos de los primeros temas a definir es el contenido del injusto del denominado "delito informático", pues se trata de un término muy usado para definir conductas en las cuales se constata el uso de la informática o	1.1. Hurto informático 1.2. Fraude informático 1.3. Estafa informática	1.1.1. Denuncia el hurto sistemático de tus cuentas. 1.1.2. Analiza la legislación peruana por delitos informáticos. 1.1.3. Conoce la regulación y sanción del hurto informático. 1.1.4. Promueve la sanción con rigor el hurto informático. 1.2.1. Estamos expuestos a ser víctimas de fraude informático. 1.2.2. Sanción con rigor el fraude informático. 1.2.3. Analiza que el daño causa un fraude informático. 1.2.4. Reconoce las estrategias para prevenir la sanción. 1.3.1. Genera confianza Comprar y contratar servicios de internet. 1.3.2. Identifica la Tipicidad para sancionar la estafa informática.	O R D I N A L

		1.4. Sabotaje informático.	1.3.3. Conoce la regulación específica de estafa informática. 1.3.4. Destruir la red es cometer estafa informática. 1.4.1. Identifica el principio de tipicidad en el sabotaje informático. 1.4.2. Aplica la regulación específica del sabotaje informático. 1.4.3. Conoce la prevención de los delitos informáticos contra el patrimonio. 1.4.4. Previene que se cometa el sabotaje informático...	
Variable Independiente **LA EVIDENCIA DIGITAL**	Al respecto Santos (2013) citando a Casey define que la evidencia digital es "todo aquel dato que pueda establecer que un delito se haya ejecutado o que la misma puede también enlazar entre el crimen y su víctima, el autor del delito, los partícipes, cómplices, etc. (p. 22). Sobre este punto se puede inferir que la evidencia digital es todo aquel dato que nos proporciona toda la información necesaria, así como también aquel que nos establece cuando un crimen sea ejecutada o consumado y la relación que hubiera con éste, con el autor del delito, sus cómplices y los partícipes, entre otros. Es desde luego, que la evidencia digital se conciba en el campo del derecho penal como aquel que recolecta o almacena datos sobre lo ocurrido en un contexto determinado.	2.1. Valor probatorio 2.2. Alcances de la regulación.	2.1.1. Reconoce que la evidencia digital es de gran valor. 2.1.2. Analiza la información jurídica como valor probatorio. 2.1.3. Teniendo la evidencia digital se puede probar el delito. 2.1.4. Reconoce el valor probatorio de la informática. 2.2.1. Identifica la determinación del daño de manera regular. 2.2.2. Regula la investigación de la evidencia digital. 2.2.3. Preparar los alcances en la regulación de la evidencia digital 2.2.4. Se debe regular la celeridad de la evidencia digital	ORDINAL

		2.3.Informacion digital	2.3.1. Reconoce que debe actualizar la información digital. 2.3.2. Actualizar la información digital para mejores efectos. 2.3.3. Reconoce que el Estado debe proporcionar facilidades en apoyo a la justicia. 2.3.4. Identifica la importancia de la información digital.	

Anexo 03: Matriz de Operacionalización del instrumento

VARIABLE	DEFINICIÓN CONCEPTUAL	DIMENSIONES	INDICADORES	ITEMS
Variable Independiente **DELITOS INFORMATICOS**	Los primeros antecedentes del delito informático fueron realizados a partir de estudios empíricos llevados en los años 70, desarrollados con base en investigación científica de la rama de la criminológica (División de Investigación y Desarrollo del Consejo Nacional de la Prevención del Delito, 1981), donde se detectó el primer caso de delito informático denominado el caso de Draper Jhon, en Septiembre de 1970, o también como el del Captain Curnch, donde se tenía que descubrir un obsequio y lo que hacía era duplica perfectamente la frecuencia del tono 2600 hz de una línea de WATS permitiéndole hacer llamadas telefónicas gratis y la gran víctima era AT & T. Unos de los primeros temas a definir es el	1.1.Hurto informático 1.2.Fraude informático 1.3.Estafa informática	1.1.1. Denuncia el hurto sistemático de tus cuentas. 1.1.2. Analiza la legislación peruana por delitos informáticos. 1.1.3. Conoce la regulación y sanción del hurto informático. 1.1.4. Promueve la sanción con rigor el hurto informático. 1.2.1. Estamos expuestos a ser víctimas de fraude informático. 1.2.2. Sanción con rigor el fraude informático. 1.2.3. Analiza que el daño causa un fraude informático. 1.2.4. Reconoce las estrategias para prevenir la sanción.	1. ¿Los bancos están dispuestos a denunciar penalmente de hurto sistemático de tus cuentas? 2.- ¿En la legislación peruana está bien legislada el hurto informático? 3.- ¿Está vigente la regulación sobre prevención y sanción del hurto informático? 4.- ¿La ley de delitos informáticos sanciona con rigor el hurto informático? 5.- ¿Las personas y empresas están expuestos a ser víctimas de fraude informático? 6.- ¿La ley de delitos informáticos sanciona con rigor el fraude informático? 7.- ¿Qué daño puede causar un fraude informático? 8.- ¿A la fecha existen estrategias claras para la prevención y sanción de fraude informático? 9.- ¿Te genera confianza comprar y contratar servicios a través de internet?

	contenido del injusto del denominado "delito informático", pues se trata de un término muy usado para definir conductas en las cuales se constata el uso de la informática o nuevas tecnologías que afectan diversos bienes jurídicos.	1.4. Sabotaje informático.	1.3.1. Genera confianza Comprar y contratar servicios de internet. 1.3.2. identifica la Tipicidad para sancionar la estafa informática. 1.3.3. Conoce la regulación específica de estafa informática. 1.3.4. Destruir la red es cometer estafa informática. 1.4.1. Identifica el principio de tipicidad en el sabotaje informático. 1.4.2. Aplica la regulación específica del sabotaje informático. 1.4.3. Conoce la prevención de los delitos informáticos contra el patrimonio. 1.4.4. Previene que se cometa el sabotaje informático.	10- ¿La ley de delitos informáticos cumple con el principio de tipicidad para sancionar la estafa informática? 11- ¿En nuestra legislación existe regulación específica del delito de estafa informática? 12- ¿Cuándo un pirata informático destruye la red comete estafa informática? 13- ¿La ley de delitos informáticos cumple con el principio de tipicidad para sancionar el sabotaje informático? 14- ¿Existe regulación específica del delito de sabotaje informático? 15- ¿Existe prevención de los delitos informáticos contra el patrimonio? 16- ¿Se requiere una reforma legislativa para prevenir y sancionar el sabotaje informático contra el patrimonio
Variable Independiente **LA EVIDENCIA DIGITAL**	Al respecto Santos (2013) citando a Casey define que la evidencia digital es "todo aquel dato que pueda establecer que un delito se haya ejecutado o que la misma puede también	2.1. Valor probatorio	2.1.1. Reconoce que la evidencia digital es de gran valor. 2.1.2. Analiza la información jurídica como valor probatorio.	1.- ¿Está de acuerdo que la evidencia digital tiñe valor probatorio en la investigación? 2.- ¿La Fiscalía cuenta con la evidencia digital que es tecnología informática y jurídica de valor probatorio?

	enlazar entre el crimen y su víctima, el autor del delito, los partícipes, cómplices, etc. (p. 22). Sobre este punto se puede inferir que la evidencia digital es todo aquel dato que nos proporciona toda la información necesaria, así como también aquel que nos establece cuando un crimen sea ejecutada o consumado y la relación que hubiera con éste, con el autor del delito, sus cómplices y los partícipes, entre otros. Es desde luego, que la evidencia digital se conciba en el campo del derecho penal como aquel que recolecta o almacena datos sobre lo ocurrido en un contexto determinado.	2.2. Alcances de la regulación. 2.3.Informacion digital	2.1.3. Teniendo la evidencia digital se puede probar el delito. 2.1.4. Reconoce el valor probatorio de la informática. 2.2.1. Identifica la determinación del daño de manera regular. 2.2.2. Regula la investigación de la evidencia digital. 2.2.3. Preparar los alcances en la regulación de la evidencia digital 2.2.4. Se debe regular la celeridad de la evidencia digital 2.3.1. Reconoce que debe actualizar la información digital. 2.3.2. Actualizar la información digital para mejores efectos. 2.3.3. Reconoce que el Estado debe proporcionar	3.- ¿El valor probatorio de la evidencia digital sirve para el juzgamiento del delito? 4.- ¿El valor probatorio de la evidencia digital representa un gran avance de la informática? 5.- ¿Es de vital importancia la determinación del daño causado por la evidencia digital? 6.- ¿Los alcances de la regulación afecta a la víctima en la investigación de la evidencia digital? 7.- ¿Está de acuerdo que una preparación adecuada favorece en la identificación de la evidencia digital? 8.- ¿Se necesita celeridad para reconocer la evidencia digital? 9.- ¿Es necesario la actualización profesional en la información digital? 10.- ¿Existe ausencia de información tecnológica actualizada para el reconocimiento de la evidencia digital? 11.- ¿Está de acuerdo que el Estado debe brindar facilidades para otorgar información digital a la brevedad posible?

			facilidades en apoyo a la justicia. 2.3.4. Identifica la importancia de la información digital.	12.- ¿Está usted de acuerdo brindar información digital por parte de los operadores de justicia?

Anexo 04: Instrumento de Recolección de datos

UNIVERSIDAD PERUANA LOS ANDES
CUESTIONARIO 1: DELITOS INFORMÁTICOS

El presente instrumento servirá para demostrar mejorar los delitos informáticos y la evidencia digital en el proceso peruano del Distrito Judicial de Junín, 2020 motivo por el cual solicito su colaboración: Tenga en cuenta la tabla siguiente:

Nunca	**1**	Rara vez	**2**	A veces	**3**	A menudo	**4**	Siempre	**5**

N°	DELITOS INFORMATICOS	Nunca	Rara vez	A veces	A menudo	Siempre
	HURTO INFORMATICO					
01	¿Los bancos están dispuestos a denunciar penalmente de hurto sistemático de tus cuentas?	1	2	3	4	5
02	¿En la legislación peruana está bien legislada el hurto informático?	1	2	3	4	5
03	¿Está vigente la regulación sobre prevención y sanción del hurto informático?	1	2	3	4	5
04	¿La ley de delitos informáticos sanciona con rigor el hurto informático?	1	2	3	4	5
	FRAUDE INFORMATICO					
05	¿Las personas y empresas están expuestos a ser víctimas de fraude informático?	1	2	3	4	5
06	¿La ley de delitos informáticos sanciona con rigor el fraude informático?	1	2	3	4	5
07	¿Qué daño puede causar un fraude informático?	1	2	3	4	5
08	¿A la fecha existen estrategias claras para la prevención y sanción de fraude informático?	1	2	3	4	5
	ESTAFA INFORMATICO					
09	¿Te genera confianza comprar y contratar servicios a través de internet?	1	2	3	4	5
10	¿La ley de delitos informáticos cumple con el principio de tipicidad para sancionar la estafa informática?	1	2	3	4	5
11	¿En nuestra legislación existe regulación específica del delito de estafa informática?	1	2	3	4	5
12	¿Cuándo un pirata informático destruye la red comete estafa informática?	1	2	3	4	5
	SABOTAJE INFORMATICO					
13	¿La ley de delitos informáticos cumple con el principio de tipicidad para sancionar el sabotaje informático?	1	2	3	4	5
14	¿Existe regulación específica del delito de sabotaje informático?	1	2	3	4	5
15	¿Existe prevención de los delitos informáticos contra el patrimonio?	1	2	3	4	5
16	¿Se requiere una reforma legislativa para prevenir y sancionar el sabotaje informático contra el patrimonio?	1	2	3	4	5

Fuente Matriz de Variables.

¡Gracias por su colaboración!

UNIVERSIDAD PERUANA LOS ANDES
CUESTIONARIO 2: EVIDENCIA DIGITAL

El presente instrumento servirá para demostrar mejorar los delitos informáticos y la evidencia digital en el proceso peruano del Distrito Judicial de Junín, 2020. Motivo por el cual solicito su colaboración: Tenga en cuenta la tabla siguiente:

Nunca	**1**	Rara vez	**2**	A veces	**3**	A menudo	**4**	Siempre	**5**

N°	**LA EVIDENCIA DIGITAL**	Nunca	Rara vez	A veces	A menudo	Siempre
	VALOR PROBATORIO					
01	¿Está de acuerdo que la evidencia digital tiene valor probatorio en la investigación?	1	2	3	4	5
02	¿La Fiscalía cuenta con la evidencia digital que es tecnología informática y jurídica de valor probatorio?	1	2	3	4	5
03	¿El valor probatorio de la evidencia digital sirve para el juzgamiento del delito?	1	2	3	4	5
04	¿El valor probatorio de la evidencia digital representa un gran avance de la informática?	1	2	3	4	5
	ALCANCES DE REGULACION					
05	¿Es de vital importancia la determinación del daño causado por la evidencia digital?	1	2	3	4	5
06	¿Los alcances de la regulación afecta a la víctima en la investigación de la evidencia digital?	1	2	3	4	5
07	¿Está de acuerdo que una preparación adecuada favorece en la identificación de la evidencia digital?	1	2	3	4	5
08	¿Se necesita celeridad para reconocer la evidencia digital?	1	2	3	4	5
	INFORMACION DIGITAL					
09	¿Es necesario la actualización profesional en la información digital?	1	2	3	4	5
10	¿Existe ausencia de información tecnológica actualizada para el reconocimiento de la evidencia digital?	1	2	3	4	5
11	¿Está de acuerdo que el Estado debe brindar facilidades para otorgar información digital a la brevedad posible?	1	2	3	4	5
12	¿Está usted de acuerdo brindar información digital por parte de los operadores de justicia?	1	2	3	4	5

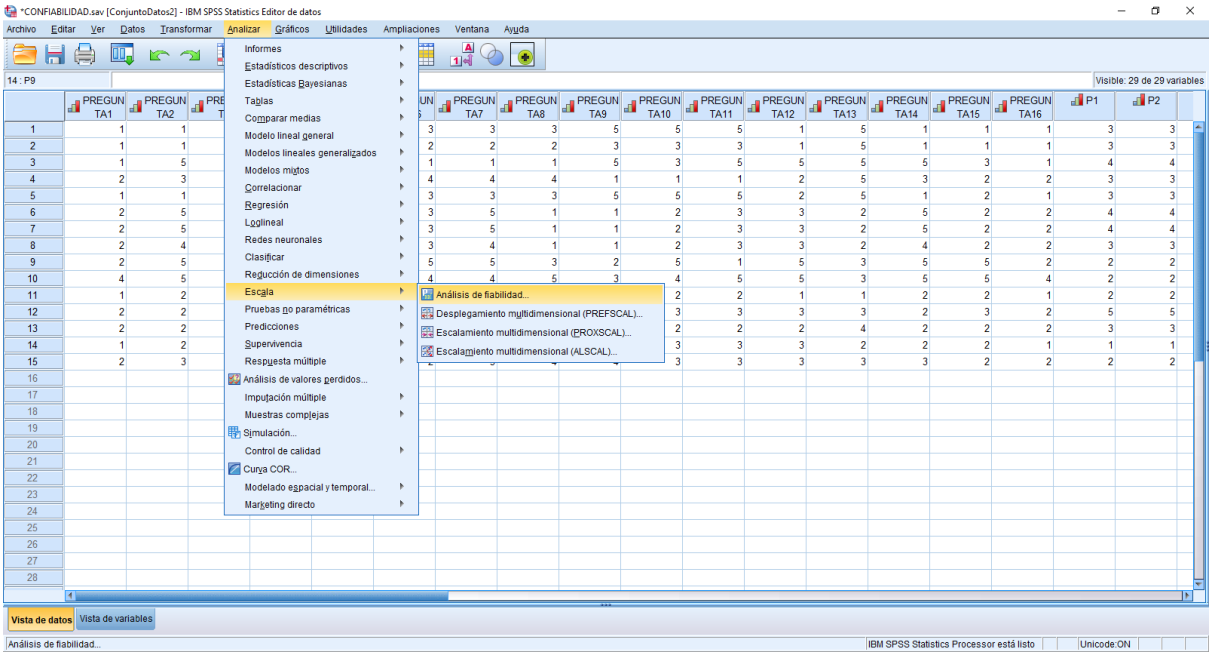
Fuente Matriz de Variables.

¡Gracias por su colaboración!

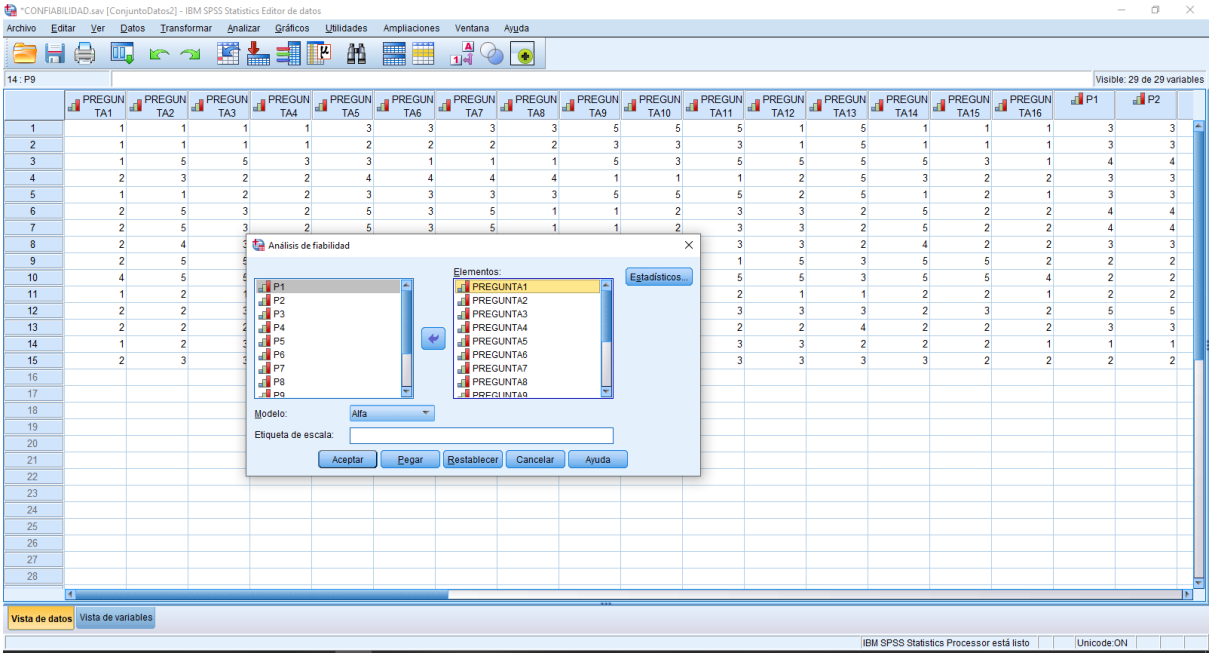
Anexo 05: Confiabilidad y validez del instrumento

Para el instrumento de la Variable 1: Delitos Informáticos

PASO 1



PASO 2



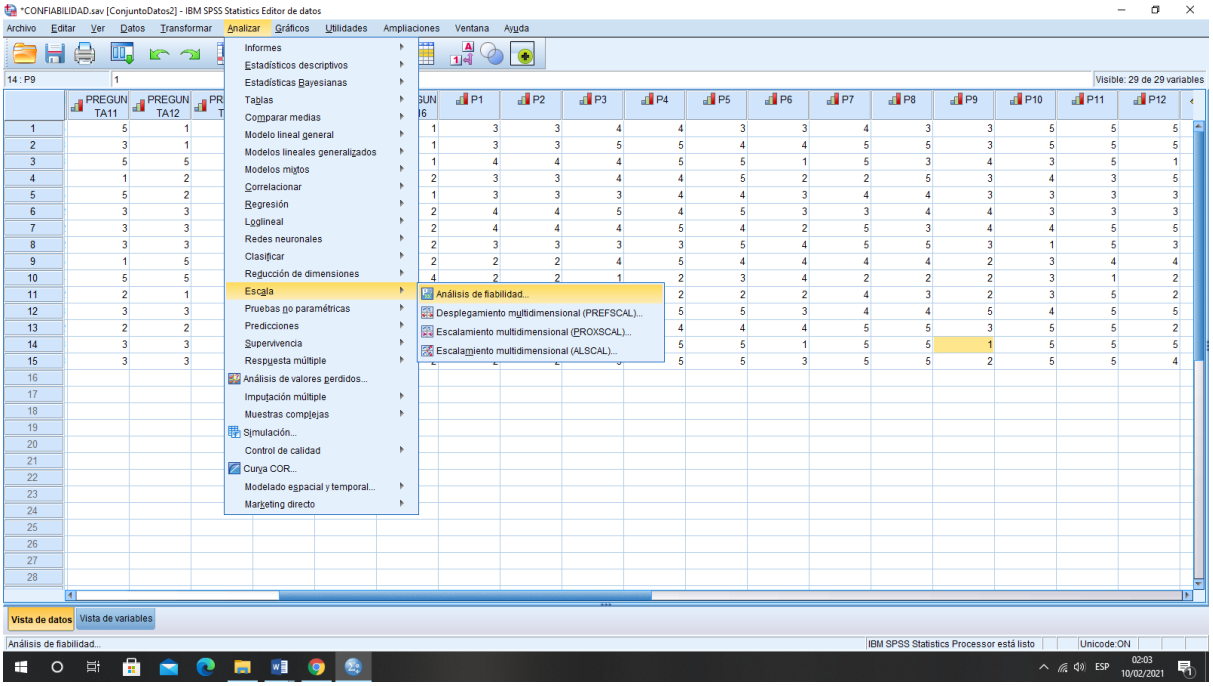
Estadísticas de fiabilidad

Alfa de Cron Bach	N de elementos
,799	16

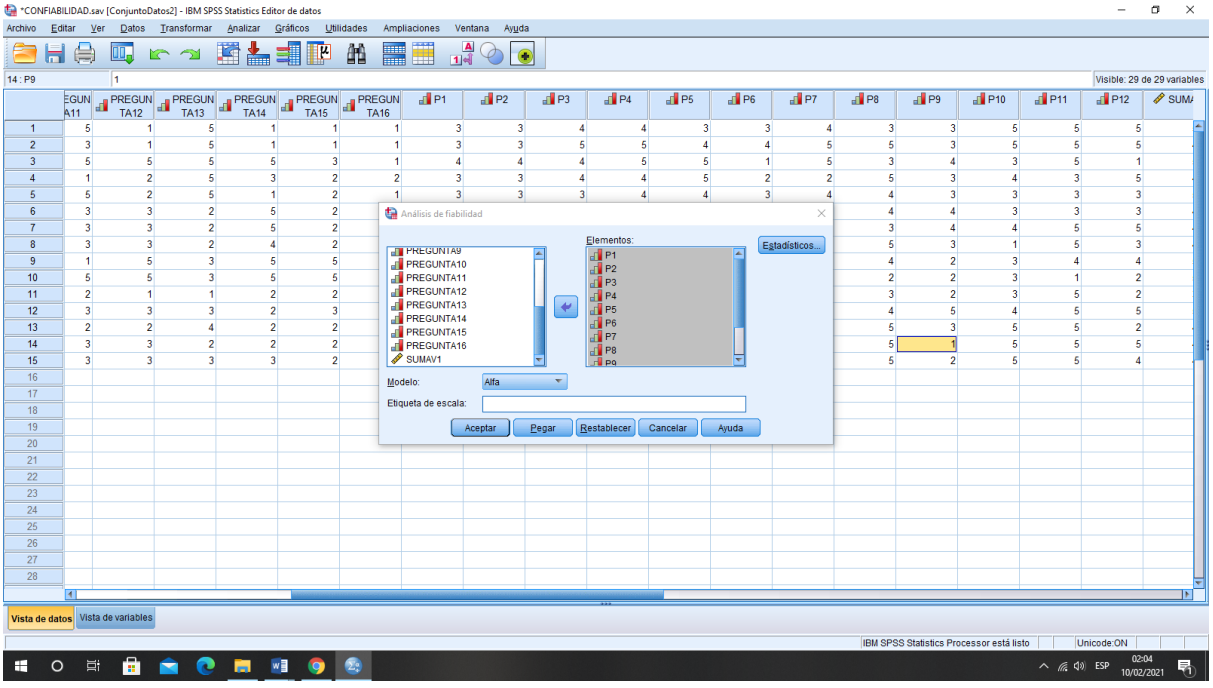
De acuerdo a Rosas & Zúñiga (2010) la confiabilidad debe ser superior a 0,75, por lo tanto, el instrumento es confiable

Para el instrumento de la Variable 2: Evidencia Digital

PASO 1



PASO 2:



Estadísticas de fiabilidad

Alfa de Cron Bach	N de elementos
,762	12

De acuerdo a Rosas & Zúñiga (2010) la confiabilidad debe ser superior a 0,75, por lo tanto, el instrumento es confiable.

INFORME DE OPINIÓN DE EXPERTOS DEL INSTRUMENTO DE INVESTIGACIÓN

DATOS GENERALES:

1.1. Apellidos y nombres del informante (Experto):
HUAMAN HUAMAN, ROLANDO V.

1.2. Profesion y Grado Académico: ABOGADO PENALISTA.

1.3. Institución donde labora: ESTUDIO JURIDICO PROPIO

1.5. Cargo que desempeña: DEFENSA TECNICA.

1.6 Denominación del Informe Final de Tesis: "Delitos informaticos y la evidencia digital en el proceso peruano del Distrito Judicial de Junin,2020".

1.7. Autores del instrumento: Bruno Galeno Olivares Ramon y Maribel Marlene Ceras Rodriguez.

II. VALIDACIÓN

INDICADORES DE EVALUACIÓN DEL INSTRUMENTO	CRITERIOS Sobre los ítems del instrumento	Muy Malo 1	Malo 2	Regular 3	Bueno 4	Muy Bueno 5
1 CALIDAD	Están formulados de manera apropiada que facilita su comprensión	1	2	3	4	5 ✓
2.OBJETIVIDAD	Están expresados de manera que son observables, medibles y alcanzables.	1	2	3	4	5 ✓
3.CONSISTENCA	Existe una organización lógica en los contenidos y relación con la teoria	1	2	3	4	5 ✓
4.COHERENCIA	Existe relación de los contenidos con los indicadores de la variable.	1	2	3	4	5 ✓
5.PERTINENCIA	Las categorias de respuestas y sus valores son apropiados.	1	2	3	4	5 ✓
6. SUFICIENCIA	Son suficientes la cantidad y calidad de items presentados en el instrumento.	1	2	3	4	5 ✓
SUMATORIA TOTAL		TREINTA				

NOTA:
FAVORABLE : 20-30
DEBE MEJORAR : 15-20
NO FAVORABLE : 10-15

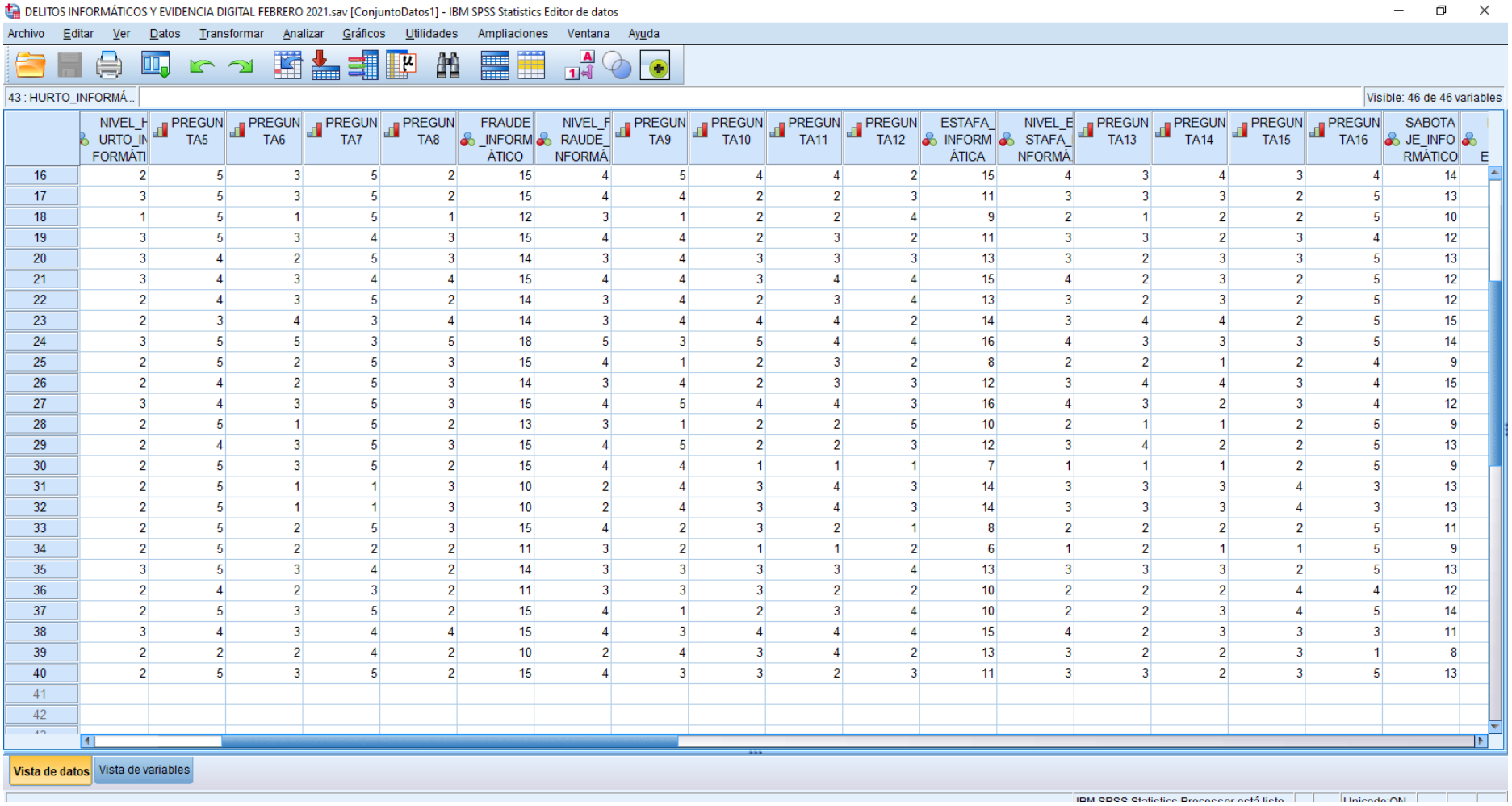
III. RESULTADOS DE LA VALIDACIÓN

3.1. Valoracion cuantitativa :
3.2. Opinion : FAVORABLE DEBE MEJORAR NO FAVORABLE
3.3. OBSERVACIONES :

Huancayo, 18 de enero del 2021

Rolando V. Huamán Huamán
CAJ. 2120
ABOGADO
Firma del Experto

Anexo 06: Data de Procesamiento de Datos



	NIVEL_HURTO_INFORMÁTI	PREGUNTA5	PREGUNTA6	PREGUNTA7	PREGUNTA8	FRAUDE_INFORMÁTICO	NIVEL_FRAUDE_NFORMÁ	PREGUNTA9	PREGUNTA10	PREGUNTA11	PREGUNTA12	ESTAFA_INFORMÁTICA	NIVEL_ESTAFA_NFORMÁ	PREGUNTA13	PREGUNTA14	PREGUNTA15	PREGUNTA16	SABOTAJE_INFORMÁTICO	E
16	2	5	3	5	2	15	4	5	4	4	2	15	4	3	4	3	4	14	
17	3	5	3	5	2	15	4	4	2	2	3	11	3	3	3	2	5	13	
18	1	5	1	5	1	12	3	1	2	2	4	9	2	1	2	2	5	10	
19	3	5	3	4	3	15	4	4	2	3	2	11	3	3	2	3	4	12	
20	3	4	2	5	3	14	3	4	3	3	3	13	3	2	3	3	5	13	
21	3	4	3	4	4	15	4	4	3	4	4	15	4	2	3	2	5	12	
22	2	4	3	5	2	14	3	4	2	3	4	13	3	2	3	2	5	12	
23	2	3	4	3	4	14	3	4	4	4	2	14	3	4	4	2	5	15	
24	3	5	5	3	5	18	5	3	5	4	4	16	4	3	3	3	5	14	
25	2	5	2	5	3	15	4	1	2	3	2	8	2	2	1	2	4	9	
26	2	4	2	5	3	14	3	4	2	3	3	12	3	4	4	3	4	15	
27	3	4	3	5	3	15	4	5	4	4	3	16	4	3	2	3	4	12	
28	2	5	1	5	2	13	3	1	2	2	5	10	2	1	1	2	5	9	
29	2	4	3	5	3	15	4	5	2	2	3	12	3	4	2	2	5	13	
30	2	5	3	5	2	15	4	4	1	1	1	7	1	1	1	2	5	9	
31	2	5	1	1	3	10	2	4	3	4	3	14	3	3	3	4	3	13	
32	2	5	1	1	3	10	2	4	3	4	3	14	3	3	3	4	3	13	
33	2	5	2	5	3	15	4	2	3	2	1	8	2	2	2	2	5	11	
34	2	5	2	2	2	11	3	2	1	1	2	6	1	2	1	1	5	9	
35	3	5	3	4	2	14	3	3	3	3	4	13	3	3	3	2	5	13	
36	2	4	2	3	2	11	3	3	3	2	2	10	2	2	2	4	4	12	
37	2	5	3	5	2	15	4	1	2	3	4	10	2	2	3	4	5	14	
38	3	4	3	4	4	15	4	3	4	4	4	15	4	2	3	3	3	11	
39	2	2	2	4	2	10	2	4	3	4	2	13	3	2	2	3	1	8	
40	2	5	3	5	2	15	4	3	3	2	3	11	3	3	2	3	5	13	
41																			
42																			

Anexo 6-A
Cuadro de Correlación

R	Correlación
0	Correlación nula
0.1 a 0.49	Correlación directa débil
0.5 a 0.79	Correlación directa moderada
0.8 a 0.9	Correlación directa alta
1	Correlación directa perfecta
-0.1 a -0.49	Correlación inversa débil
-0.5 a -0.79	Correlación inversa moderada
-0.8 a -0.9	Correlación inversa alta
-1	Correlación inversa perfecta

Fuente: Rosas y Zúñiga (2010)

Anexo 6-B

Baremos

VARIABLE 1

NIVELES	HURTO INFORMATICO	FRAUDE INFORMATICO	ESTAFA INFORMATICA	SABOTAJE INFORMATICA	DELITOS INFORMÁTICOS
SOBRESALIENTE	18-20	18-20	18-20	18-20	68-80
SUFICIENTE	15-17	15-17	15-17	15-17	55-67
MEDIANAMENTE SUFICIENTE	11-14	11-14	11-14	11-14	43-54
POCA	8-10	8-10	8-10	8-10	30-42
MUY POCA	4 - 7	4 - 7	4 - 7	4 - 7	16-29
MAX	20	20	20	20	80
MIN	4	4	4	4	16

VARIABLE 2

NIVELES	VALOR PROBATORIO	ALCANCES DE REGULACION	INFORMACION DIGITAL	EVIDENCIA DIGITAL
MUY ALTO	18-20	18-20	18-20	51-60
ALTO	15-17	15-17	15-17	42-50
MEDIO	11-14	11-14	11-14	32-41
BAJO	8-10	8-10	8-10	23-31
MUY BAJO	4 - 7	4 - 7	4 - 7	12-22
MAX	20	20	20	60
MIN	4	4	4	12

Anexo 07: Consentimiento Informado

CONSENTIMIENTO INFORMADO DE PARTICIPACIÓN

YO, _____, identificado con DNI N° Domiciliado en _____, egresado de la Facultad de Derecho y Ciencias Políticas de la Universidad Peruana Los Andes, acepto voluntariamente participar en el trabajo de investigación titulado: "Los delitos informáticos y la evidencia digital en el proceso peruano del Distrito Judicial de Junin, 2020.", el cual tiene como tiene como propósito Determinar la relación entre los delitos informáticos y la evidencia digital en el proceso peruano del Distrito Judicial de Junín, 2020.

Toda información que se obtenga a través de este cuestionario será usada por el investigador responsable con la finalidad de elaborar un trabajo de investigación.

Se garantiza el anonimato y la confiabilidad en su totalidad de la información obtenida. Habiendo sido informado en forma adecuada sobre los objetivos del estudio, acepto y firmo este documento.

Huancayo, enero de 2021

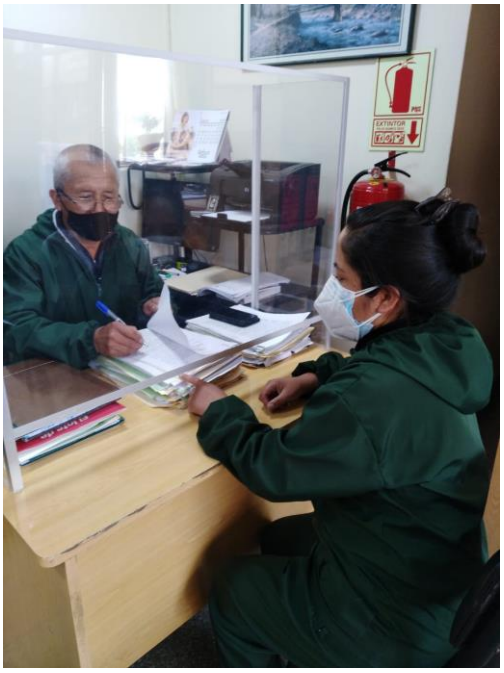
_____

Firma del colaborador

Anexo 08: Evidencia (Fotos)

1 BACHILLER MARIBEL MARLENE CERAS RODRIGUEZ: ENTREVISTA AL ABOGADO JULIO CESAR SALOME, EN RELACION AL CUESTIONARIO LA EVIDENCIA DIGITAL

2. BACHILLER MARIBEL MARLENE CERAS RODRIGUEZ: ENTREVISTA AL ABOGADO EULOGIO CARHUANCHO ORIHUELA SOBRE LOS DELITOS INFORMATICOS



3. BACHILLER MARIBEL MARLENE CERAS RODRIGUEZ: ENTRVISTA AL ABOGADO ALBERTO HUAMANI FERNADEZ, EN RELACION AL CUESTIONARIO LA EVIDENCIA DIGITAL

5: BACHILLER MARIBEL MARLENE CERAS RODRIGUEZ: ENTREVISTA AL ABOGADO PERCY PEÑA HINOSTROZA SOBRE LOS DELITOS INFORMATICOS

6: BACHILLER BRUNO GALENO OLIVARES RAMÓN : ENTREVISTA AL ABOGADO Y CONTADOR, KOKY MEZA S. EN RELACION AL CUESTIONARIO LA EVIDENCIA DIGITAL

7. BACHILLER BRUNO GALENO OLIVARES RAMÓN: REALIZANDO LA ENTREVISTA AL ABOGADO DR. FRANK TAIPE, EN RELACION AL CUESTIONARIO LA EVIDENCIA DIGITAL

8: BACHILLER BRUNO GALENO OLIVARES RAMÓN: REALIZANDO LA ENTREVISTA A LA TECNICA KATHERINE HERRERA SOBRE LOS DELITOS INFORMATICOS

Anexo 09: Fichas de Entrevista

FICHA DE ENTREVISTA

Título: Delitos informáticos y la evidencia digital en el proceso penal peruano del Ditrito Judicial de Junin,2020.

ENTREVISTADO: Dr. Guillermo Peña Hinostroza

CARGO Y PROFESION: Docente Universitario - Derecho Penal

INSTITUCION: Universidad Continental - Huancayo

LUGAR Y FECHA: Huancayo. 26-01-21

Objetivo general: Determinar la relación entre los delitos informáticos y la evidencia digital en el proceso peruano del Distrito Judicial de Junín, 2020.

1.- En su opinión, ¿Considera que se tiene un buen nivel de legislación nacional e internacional para la ayuda en la investigación de los Delitos Informáticos?

En mi opinion y de acuerdo a mi experiencia puedo mencionar que no hay norma que compare y sancione este delito.

2.- De su conocimiento, ¿Considera que los operadores de derecho están suficientemente capacitados para manejar temas de delitos informáticos?.

Por su puesto; pero requiere de experiencia y formación en los temas informaticos

3.- ¿Considera que los peritos informáticos están suficientemente capacitados y el personal es suficiente para la carga de investigaciones?

El problema ocurre que nuestra Policia Nacional del Perú, tiene muchas dificultades para hallar a los responsables

4.- ¿Considera que las herramientas utilizadas en la Informática Forense son óptimas para la investigación?

En nuestro país es notorio que existe poca preparación en informatica forense.

Objetivo especifico 1: Determinar la relación entre los delitos informáticos y el valor probatorio en el proceso peruano del Distrito Judicial de Junín, 2020.

5.- De su experiencia, ¿Le parece que abarcamos todos los delitos informáticos que tiene como objeto la vulneración de la información en nuestro marco legal?

Efectivamente un vacio en nuestro Código Penal que aun contemple todos los delitos informaticos ya por penalización.

6.- ¿Considera que esta correctamente regulado los delitos informáticos que utilizan las Tics como medio para realizar los delitos convencionales?

La Tecnologia de la Información requiere de mayor difusión y preparación.

7.-En su opinión, ¿Cree usted que la estructura de la Tipicidad Objetiva en los Delitos Informáticos es la adecuada?

La tipicidad objetiva es la adecuada, el problema es que no se pueden encontrar evidencias digitales de los actos de los delincuentes.

8.- De su experiencia, ¿Considera que ha existido una evolución sobre lo conocido tradicionalmente en la tipicidad subjetiva de los Delitos Informáticos?

La evolución es a diario, vivimos en un mundo donde la informatica se hace inevitable es mas en estos momentos de la presencia del COVI-19.

Objetivo específico 2: Determinar la relación entre los delitos informáticos y los alcances de la regulación en el proceso peruano del Distrito Judicial de Junín, 2020.

9.- ¿Considera que se tiene el conocimiento adecuado sobre el manejo de la evidencia digital en cuanto a metodología de reconocimiento y recolección?

Justamente nuestra preocupacion gira en torno a que no se pueden encontrar evidencias digitales de las fascinerosas medidas en estos delitos.

10.- De su conocimiento, ¿Le parece que es relevante la calidad de análisis del informe realizado por los peritos informáticos para la admisión de la evidencia digital en el proceso penal?

Los peritos informáticos realizan su labor de acuerdo a la preparacion que tienen, pero no es suficiente.

Objetivo específico 3: 3. Determinar la relación entre los delitos informáticos y la información digital en el proceso peruano del Distrito Judicial de Junín, 2020.

11.- De su perspectiva ¿Cree usted que el marco legal que tiene la cadena de custodia sobre evidencia digital es el necesario?

Por su puesta debe haber una cadena de custodia de los delitos que cometen los delincuentes de los delitos informáticos.

FICHA DE ENTREVISTA

Título: Delitos informáticos y la evidencia digital en el proceso penal peruano del Ditrito Judicial de Junín,2020.

ENTREVISTADO: Dr. Guillermo Peñe Hinostroza

CARGO Y PROFESION: Docente Universitario - Derecho Penal

INSTITUCION: Universidad Continental - Huancayo

LUGAR Y FECHA: Huancayo, 26-01-21

Objetivo general: Determinar la relación entre los delitos informáticos y la evidencia digital en el proceso peruano del Distrito Judicial de Junín, 2020.

1.- En su opinión, ¿Considera que se tiene un buen nivel de legislación nacional e internacional para la ayuda en la investigación de los Delitos Informáticos?

En mi opinion y de acuerdo a mi experiencia puedo mencionar que no hay norma que tampare y sancione este delito.

2.- De su conocimiento, ¿Considera que los operadores de derecho están suficientemente capacitados para mancjar temas de delitos informáticos?.

Por su puesto; pero requiere de experiencia y formación en los temas informaticos

3.- ¿Considera que los peritos informáticos están suficientemente capacitados y el personal es suficiente para la carga de investigaciones?

El problema ocurre que nuestra Policia Nacional del Perú, tiene muchas dificultades para hallar a los responsables

4.- ¿Considera que las herramientas utilizadas en la Informática Forense son óptimas para la investigación?

En nuestro pais es notorio que existe poca preperación en informatica forense.

Objetivo específico 1: Determinar la relación entre los delitos informáticos y el valor probatorio en el proceso peruano del Distrito Judicial de Junín, 2020.

5.- De su experiencia, ¿Le parece que abarcamos todos los delitos informáticos que tiene como objeto la vulneración de la información en nuestro marco legal?

Efectivamente un vacio en nuestro Codigo Penal que no contempla todos los delitos informaticos y su penalización.

6.- ¿Considera que esta correctamente regulado los delitos informáticos que utilizan las Tics como medio para realizar los delitos convencionales?

Exactamente el personal de la Policía Nacional del Perú es inexperto en estos temas.

7.-En su opinión, ¿Cree usted que la estructura de la Tipicidad Objetiva en los Delitos Informáticos es la adecuada?

Como en su momento se dio vigencia al nuevo Código Procesal Penal; falta incrementar y penalizar algunos delitos informáticos.

8.- De su experiencia, ¿Considera que ha existido una evolución sobre lo conocido tradicionalmente en la tipicidad subjetiva de los Delitos Informáticos?

La evolución es permanente y a diario existen cada vez mas avezados que cometen delitos informáticos.

Objetivo específico 2: Determinar la relación entre los delitos informáticos y los alcances de la regulación en el proceso peruano del Distrito Judicial de Junín, 2020.

9.- ¿Considera que se tiene el conocimiento adecuado sobre el manejo de la evidencia digital en cuanto a metodología de reconocimiento y recolección?

La dificultad es que por el avance diario de estos delitos se cometen estos hechos con suma habilidad, que es imposible su captura.

10.- De su conocimiento, ¿Le parece que es relevante la calidad de análisis del informe realizado por los peritos informáticos para la admisión de la evidencia digital en el proceso penal?

El problema radica en que el personal que egresa de la Institución Policial; no tiene la formación adecuada en este tipo de delitos.

Objetivo específico 3: 3. Determinar la relación entre los delitos informáticos y la información digital en el proceso peruano del Distrito Judicial de Junín, 2020.

11.- De su perspectiva ¿Cree usted que el marco legal que tiene la cadena de custodia sobre evidencia digital es el necesario?

Debe haber el amparo necesario, para encontrar al delincuente y castigar por cada delito.

12.- En su opinion, ¿Cree usted que la instrumentalización aplicada en la evidencia digital es la adecuada para su admisión el proceso penal peruano?

Se tiene que reestructurar todo la instrumentalización para efectuar una verdadera justicia social.

Que habiendo culminado de manera exitosa la entrevista, se agradece su importante colaboración.

Huancayo,16 de Enero del 2021

Firma del entrevistado

Guillermo P. Peña Hinostroza
ABOGADO
Reg. CAL. N° 19257

Anexo 10: Jurisprudencia

DELITOS INFORMÁTICOS: UN IMPORTANTE PRECEDENTE

Alberto Contreras Clunes

I. PLANTEAMIENTO DEL TEMA

a) Cuestiones previas: En los últimos meses hemos observado a través de los distintos medios de comunicación, varios hechos punibles en los que la característica fundamental para su comisión ha sido el empleo de una computadora. En efecto, el caso sobre «espionaje informático» seguido contra la empresa Inverlink S.A.; el periodísticamente denominado caso «coimas», seguido en contra del Ministerio de Obras Públicas, son sólo algunos de los que aparecen a diario en los noticieros.

Los medios de comunicación en general han calificado estos hechos como «delitos modernos», «delitos tecnológicos», «delitos nuevos». En rigor la mayoría de ellos puede agruparse dentro de los Delitos Informáticos, previstos y sancionados en la Ley N°19.366, publicada en el *Diario Oficial* el 7 de junio de 1993. Esta ley en sus cuatro artículos tipifica conductas que utilizan las tecnologías de la información como medio de comisión de hechos punibles.

b) Análisis de la Ley N°19.366: El bien jurídico protegido, según la historia fidedigna de esta ley, es: La calidad, pureza e idoneidad de la información en cuanto tal, contenida en un sistema automatizado de tratamiento de la misma y de los productos que de su operación se obtengan.

Sin embargo, importante doctrina sostiene que los Delitos Informáticos son «pluriofensivos, por lo que atentan contra diversos bienes jurídicos, a saber, la propiedad, la intimidad, etc.»

La doctrina suele clasificar los tipos penales de esta ley en: a) delitos de espionaje informático y b) delitos de sabotaje informático[2].

Esta ley consta de tan solo cuatro artículos, de los cuales los artículos 1, 3 y 4 exigen un dolo específico o directo en la comisión del delito, al exigir el tipo un actuar «malicioso».

Artículo 1° «El que maliciosamente destruya o inutilice un sistema de tratamiento de información o sus partes o componentes, o impida, obstaculice o modifique su funcionamiento, sufrirá la pena de presidio menor en su grado medio a máximo.

Si como consecuentita de estas conductas se afectaren los datos contenidos en el sistema, se aplicará la pena señalada en el inciso anterior, en su grado máximo».

Parte de la doctrina sostiene que no se trata de un Delito Informático propiamente tal, sino más bien de un «delito de daños convencional». Además, en esta disposición se mezcla erróneamente el daño producido al «software» con el «hardware».

Artículo 2° «El que, con el ánimo de apoderarse, usar o conocer indebidamente de la información contenida en un sistema de tratamiento de la misma, lo intercepte, interfiera o acceda a él, será castigado con presidio menor en su grado mínimo a medio».

Se trata de un delito de espionaje informático, requiriendo el sujeto activo actuar con una determinada motivación, precisamente aquellas que el mismo tipo penal describe: «con ánimo de apoderarse, usar o conocer indebidamente de la información contenida en él».

Artículo 3° «El que maliciosamente altere, dañe o destruya los datos contenidos en un sistema de tratamiento de la información, será castigado con presidio menor en su grado medio».

Nos encontramos frente a una especie de sabotaje informático, requiriendo el elemento subjetivo la concurrencia de un dolo específico o directo.

Artículo 4° «El que maliciosamente revele o difunda los datos contenidos en un sistema de información, sufrirá la pena de presidio menor en su grado medio. Si quien incurre en estas conductas es el responsable del sistema de información, la pena se aumentará en un grado».

Nuevamente se trata de una especie de espionaje informático, requiriendo el tipo un dolo específico. Además, se contempla una figura agravada, cuando quien incurre en este delito es el responsable del sistema.

II. LOS HECHOS

Entre los días 28 de diciembre de 2001 y 8 de enero de 2002, un ex empleado de la empresa ATI Chile, realizó diversas intromisiones ilegales al servidor de ésta, alterando, dañando y conociendo indebidamente información contenida en éste. Los sitios Web afectados fueron: www.guestbook.cl y www.metabuscador.cl

El imputado era un joven de 19 años, conocido en el Chat IRC con el seudónimo «P0key», el cual habría actuado por «venganza» en contra de la empresa, pues había sido despedido de ésta.

El «cracker»al ingresar ilegalmente a estos sitios, alteró el contenido de éstos, creando una nueva página Web (index.html) en reemplazo de la existente, que mostraba mensajes ofensivos hacia la empresa e indicaba que el sitio había sido hackeado.

El administrador del sistema informático procedió a efectuar una inmediata auditoría de todos los archivos «LOG» del servidor y pudo comprobar que dichos sitios habían sido víctima de una serie de ataques e intromisiones, además, la eliminación de algunos archivos de auditoría de transacciones de cuentas de FTP, para borrar rastros desde dónde se efectuaban los ataques. Incluso, mientras se realizaban las auditorías, se pudo comprobar que el «cracker» intentaba ingresar al correo electrónico del gerente general de la empresa, hecho que pudo ser controlado a tiempo.

Se pudo comprobar que el 90% de los ataques provenía desde una IP fija, que correspondía a un Ciber Café en el cual el imputado trabajaba como administrador. El resto de los ataques provenía desde cuentas conmutadas de acceso a Internet, fundamentalmente desde el domicilio del imputado.

Una vez iniciada la investigación y presentada la querella criminal por delitos informáticos, el caso tomó especial importancia en la prensa de la ciudad de Talca y entre los usuarios del Chat IRC. Aprovechando este momento, el imputado concurrió en forma voluntaria al diario *El Centro* de Talca y entregó una entrevista, siendo portada, bajo el título: *«Yo soy el ciber pirata»*. De esta manera lograba la fama y reconocimiento por sus pares, hecho buscado

comúnmente entre los «crackers». Incluso ofrecía sus servicios para reparar las fallas de seguridad del sistema.

III. EL JUICIO ABREVIADO

El día fijado para la audiencia de preparación del juicio oral, los intervinientes: Ministerio Público, Defensor Penal Público y Querellante, acordaron proceder conforme al Procedimiento Abreviado[5]. Para ello el querellante tuvo que desistirse de otros dos delitos a fin de cumplir con los requisitos establecidos en el Código Procesal Penal. Una vez realizadas las preguntas de rigor al acusado, la Juez de Garantía señora Marta Asiaín Madariaga, autoriza la realización del juicio abreviado y da la palabra al fiscal para que exponga el caso.

El fiscal jefe de la ciudad de Talca don Carlos Olivos Muñoz, realizó una clara exposición respecto de los hechos, la investigación realizada, todos los medios de prueba reunidos durante ocho meses de investigación y solicitó la aplicación de una pena de 3 años y un día de presidio, por tres delitos informáticos: artículos 1, 2 y 3 de la Ley 19.223.

El querellante, abogado Alberto Contreras Clunes, ratifica todo lo señalado por el fiscal y recalca la gravedad de los delitos imputados, los perjuicios ocasionados a la empresa y el actuar malicioso del acusado. También resalta el hecho que el acusado confiesa su participación en su declaración policial y el jactarse de ello en la entrevista del diario *El Centro.*

Importante resulta la inclusión de un peritaje informático realizado por la Brigada del Ciber Crimen de la Policía de Investigaciones de Chile. En efecto, se realizó un peritaje a la computadora que ocupaba el acusado en el Ciber Café, como a su computadora personal. Por medio de un sofisticado programa, inaugurado en esta ocasión, se logra recuperar diversos archivos borrados del disco duro de la CPU del Ciber Café. Merece especial atención uno, consistente en un correo electrónico enviado por el acusado a su pareja en el cual le cuenta: *«estoy borrando unas («weas») que me pueden comprometer en los asuntos judiciales …»,* enviado precisamente en la tarde del día anterior al que prestó declaración policial.

En sus conclusiones el peritaje señala que: *«El computador en cuestión cuenta con las capacidades técnicas necesarias y los programas adecuados tanto para navegar por Internet como para efectuar daños a sistemas informáticos».* En efecto, se pudo determinar que el disco duro contenía 24 programas: *«… de uso frecuente por los Hackers, Crackers o Criminales Informáticos».*

Finaliza el querellante señalando la importancia que tiene la informática en la actualidad, las potenciales víctimas de este tipo de delitos y los graves perjuicios que se causan a las empresas, pudiendo éstas llegar a quebrar económicamente por el desprestigio que estos delitos le provocan, solicitando la imposición de una pena de cinco años de presidio, en atención a tratarse de reiteración de delitos, contemplados en los artículos 1, 2 y 3 de la Ley 19.223.

Por su parte el defensor penal público don Joaquín Lagos León, alegó indicando que no se encontraba acreditada la participación de su defendido en los hechos, negándole valor a la declaración policial.

Introdujo una novedosa jurisprudencia del derecho norte americano, en la cual se penaliza a las empresas que ofrecen servicios de seguridad informática y son víctimas de «hackers», puesto que no dan cumplimiento a los servicios ofrecidos

Trata en detalle las circunstancias personales del acusado, indicando que se trata de un joven autodidacta en computación, de esfuerzo, padre de familia, casado. Solicita la absolución de su representado y en caso de condena, se aplique el mínimo de la escala, esto es, la pena de 541 días de presidio, con el beneficio de libertad vigilada, al no registrar antecedentes penales.

IV. EL FALLO

Al finalizar la audiencia, la Juez de Garantía dicta su veredicto: Culpable por los delitos N°1, 2 y 3 de la Ley 19.223, fijando la fecha de la lectura del fallo para el día 11 de abril de 2003.

El fallo consta de 13 fojas en las que pormenorizadamente se analizan todos los medios de prueba, describiendo en forma precisa el actuar delictivo y la forma en que éste se encontraba acreditado.

Al fijar la pena, la Juez advierte que tratándose de reiteración de delitos resulta más beneficioso aplicar una pena única conforme al artículo 351 del Código Procesal Penal. Señala también que lo dispuesto en el inciso cuarto de dicho artículo, es: *«una facultad para el Tribunal»* en consideración a que el querellante solicitó una pena superior a la del fiscal.

Por otra parte, afirma que: *«la entidad de las atenuantes no nos convence, teniendo presente que según quedó establecido se trata de delitos reiterados, por lo que la pena que se impondrá en el grado señalado se considera más condigna con el actuar ilícito del acusado»*.

En atención a ello aplica la pena de tres años y un día de presidio, que es el mínimo de la escala penal de presidio menor en su grado máximo.

V. COMENTARIOS

Tratar los Delitos Informáticos es en sí un tema complejo. Sin embargo, la claridad del fallo nos deja plenamente satisfechos que se ha comprendido en toda su dimensión el tipo penal y las consecuencias que de él derivan.

Siendo muchas veces la prueba pericial esencial en el esclarecimiento de los hechos y la participación del autor de estos ilícitos, ella fue cabalmente comprendida y acreditó, más allá de toda duda razonable, la participación culpable del acusado.

La oportuna incautación de la CPU del acusado y del servidor del Ciber Café, además, del análisis exhaustivo dichos equipos; logró precisar con fecha, hora, minuto y segundo cuando se cometieron los ataques, como también el lugar de origen de éstos y el usuario que los realizó.

La oportuna detección de los ataques y las rigurosas medidas de seguridad aplicadas por la empresa, evitaron que los daños y perjuicios fuesen mayores.

La adecuada colaboración entre el fiscal jefe del Misterio Público de la ciudad de Talca señor Carlos Olivos con el abogado querellante y la víctima, lograron diseñar una investigación que a lo largo de ocho meses obtuvo abundantes medios probatorios que incriminaron al imputado.

Siendo éste el primer caso sobre Delito Informático dentro de la reforma procesal penal y la meridiana claridad de los fundamentos en la sentencia condenatoria, se convertirá necesariamente en un obligado precedente.

Es necesario destacar que, más allá del éxito en la resolución del caso, existió una empresa que se atrevió a denunciar el delito, con todas las consecuencias que trajo para con sus clientes y prestigio, algo que por lo general no hacen las víctimas de estos delitos.

Como conclusión final simplemente cabe señalar que en la actualidad existe suficiente tecnología para investigar este tipo de delitos y, mejor aún, es posible sancionar a los autores de éstos, erróneamente denominados «hackers», siendo en rigor, simples delincuentes informáticos

Código Penal relacionado con los Delitos Informáticos.

ARTÍCULO	DESCRIPCIÓN
Art.182.	Constreñimiento
Art.188ª.	Trata de
Art.194.	Divulgación y empleo de documentos reservados
Art.196.	Violación ilícita de comunicaciones o correspondencia de carácter
Art.199.	Sabota
Art.203.	Daños o agravios a personas o a cosas destinadas al culto
Art.218.	Pornografía con
Art.219ª.	Utilización o facilitación de medios de comunicación para ofrecer servicios
Art.220.	Injur
Art.221.	Calum
Art.222.	Injuria y calumnia
Art.239.	Hurt
Art.244.	Extorsi
Art.246.	Estaf
Art.251.	Abuso de condiciones de inferioridad
Art.257.	Del acceso ilegal o prestación ilegal de los servicios de
Art 269ª	Acceso abusivo a un sistema informático
Art 269B	Obstaculización ilegitima de sistema informático o red de
Art 269C	Interceptación de datos
Art 269D	Daño
Art 269E	Uso de software
Art 269F	Violación de datos
Art 269G	Suplantación de sitios web para capturar datos personales
Art 269I	Hurto por medios informáticos y semejantes
Art.270.	Violación a los derechos morales de autor
Art.271.	Violación a los derecho patrimoniales de autor y derechos conexos
Art 272.	Violación a mecanismos de protección de derechos de autor y derechos conexos
Art.291.	Uso de documento
Art.292.	Destrucción, supresión u ocultamiento de documento publico
Art.293.	Destrucción, supresión y ocultamiento de documento privado
Art.294.	Docume
Art.300.	Ofrecimiento engañoso de productos y servicios
Art.302.	Pánico
Art.303.	Ilícita explotación
Art.307.	Uso ilegitimo de
Art.316.	Captación masiva y habitual de dineros
Art.317.	Manipulación fraudulenta de especies inscritas en el registro nacional de
Art.323.	Lavado de
Art.325.	Omisión de
Art.340.	Concierto para
Art.341.	Entrenamiento para actividades ilícitas
Art.343.	Terroris

Art.347.	Amenaz
Art.389.	Fraude e inscripción en