FACULTAD DE DERECHO Y HUMANIDADES

ESCUELA PROFESIONAL DE DERECHO

Análisis de los delitos informáticos y el valor probatorio de la evidencia digital en la Corte Superior de Justicia de Lima - 2021

TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE:
Abogado

AUTOR:

Espinoza Prado, Victor (ORCID: 0000-0002-5493-9270)

ASESORA:

Mg. Lázaro Ortíz, Yanira Guisella (ORCID: 0000-0002-5628-4394)

LÍNEA DE INVESTIGACIÓN:

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

LÍNEA DE RESPONSABILIDAD SOCIAL UNIVERSITARIA:

Fortalecimiento de la democracia, liderazgo y ciudadanía

LIMA - PERÚ

2022

Dedicatoria

Dedico esta tesis a Dios y mis ángeles (padre, madre e hija) que desde el cielo me dieron la fuerza necesaria para llegar hasta este momento tan importante de mi formación profesional. A mi familia que siempre estuvo a mi lado en los momentos de alegría y tristeza, porque sin su apoyo incondicional, no hubiera logrado esta meta.

Agradecimiento

Agradecer a Dios, por permitirme el haber llegado hasta este momento y a la Policía Nacional del Perú por permitirme conocer más de cerca la carrera de Derecho y a su vez, darme la oportunidad de poder culminar mi formación profesional. Asimismo, agradecer a mi familia por ser el pilar más importante y demostrarme siempre su cariño y apoyo incondicional para el logro de todas mis metas.

Índice de contenidos

Índice de tablas

Índice de figuras

Resumen

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.

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.

Palabras clave: Delitos informáticos, valor probatorio, evidencia digital.

Abstract

Crime today has already surpassed all schemes with the arrival of technology. The appearance of the internet has made it possible to globalize the opportunities to carry out these crimes, moving it to unforeseen points on planet earth.

In this order of ideas, the problem of cybercrime has increased and is developing new sophisticated modes of operation, it is difficult to discover the bad intentions of people who take advantage of the great advantage offered by computer systems, compared to this reality, criminal law of many countries have been unable to discover these criminals who hide in many ways, our Penal Code has certain gaps despite the modifications introduced in a generic way in relation to cybercrime is not enough, so criminal law requires applying rules more drastic and highly trained personnel who are investigating these cases.

Our country is not exempt from this great global responsibility; therefore, the real importance of this problem is to be at the forefront with the new updates and the new types of strategies committed by the authors of computer crimes.

Keywords: Computer crimes, probative value, digital evidence.

I. INTRODUCCIÓN

A nivel mundial, es conocido que el ciberespacio representa un importantísimo avance con respecto a tecnología se refiere, haciendo que muchas de las tareas que realizamos como parte de nuestro quehacer diario, constituyan tareas fáciles de realizar, optmizando tiempos y recursos en su desarrollo. Sin embargo, también debemos coincidir que el ciberespacio constituye una fuente de potenciales amenazas frente a la seguridad de las personas y los Estados. Conocedores de esta problemática, la comunidad internacional viene desarrollando una serie de dispositivos normativos que promuevan abordar de manera más frontal y eficiente la ciberdelincuencia. A partir de intentar superar las serias deficiencias evidenciadas en los marcos legales de las naciones, puesto que hasta el momento no se ha logrado articular estrategias debidamente consensuadas y multilaterales. A pesar de importantes iniciativas internacionales que buscan reducir las nefastas consecuencias que conlleva la consumación de estos actos delictivos, como es el caso del Convenio de Budapest iniciativa europea que busca convertirse en una estrategia de lucha contra la ciberdelincuencia a un nivel regional.

En el caso peruano, de acuerdo con Andina (2020), los ilícitos penales en el ámbito informático que acontecen con mayor frecuenca según la DIVINDAT de la PNP, registró alrededor de tres mil denuncias relacionados a delitos informáticos durante el año 2019, la gran mayoría de denuncias se relacionan con ilícitos que atentan contra el patrimonio y que tienen como contexto el ciberespacio. Seguidamente de los fraudes electrónicos que alcanzaron un total de dos mil denuncias durante este mismo período. En tanto, la pornografía infantil representa una alarmante cifra que supera los 200 casos, lo cual representa una problemática muy preocupante para nuestra actual sociedad, dicha situación evidencia serias deficiencias de nuestras autoridades para identificar las verdaderas causales y de esta manera poder tomar decisiones que permitan reducir la incidencia de este delito. Pese a que existe un marco legal que busca mitigar el efecto de los delitos informático, como es el caso de la Ley Nº 30096, aún se evidencian serias falencias al sistema que se deben mejorar o perfeccionar a nivel de la ley misma y de su reglamentación.

Resulta evidente que las nuevas tecnologías se han vuelto parte fundamental de nuestras vidas, en aspectos tan rutinarios como el uso de una

cuenta de correo electrónico, el uso de los celulares, agendas electrónicas, los smartwatch que permiten monitorear hasta funciones vitales de la persona, programando sus tareas y pendientes dentro del día, de esta manera se hace imprescindible el uso de las tecnologías con la finalidad de interactuar adecuadamente con el resto de la comunidad. Así como las nuevas tecnologías nos han simplificado la vida, tambien los delincuentes han sabido sacar provecho de sus enormes ventajas y de la dependencia de las personas hoy en día a la tecnología. La delincuencia ha cambiado su accionar, se ha modernizado con el uso de herramientas tecnológicas para la consumación de acciones ilícitas que transgreden principalmente el patrimonio y la identidad.

La conjunción formada por las nuevas tecnologías y las habilidades delincuenciales amparadas sobretodo en el anonimato que rige sus acciones ilícitas. Si bien es cierto, el Perú cuenta con una norma específica en torno a los delitos informáticos, sin embargo se evidencia serias falencias de las mismas, lo cual obedece en gran medida al hecho de que no todas las acciones ilícitas corresponden a ciberdelincuentes, puesto que hoy en día se utiliza la tecnología para cometer delitos tradicionales, lo cual genera una nueva versión más fortalecida de este tipo de delitos (Manual de evidencia digital, 2017). Ante esto, Osco (2019) señala que el uso inadecuado de las nuevas tecnologías es perpetrado por los llamados ciberdelincuentes, los rastros que deja la realización de estos ilícitos se denominan pruebas digitales, estas pruebas deben estar contenidas en un marco legal bien definido, a fin de poder mitigarlas de manera eficaz a través de un proceso judicial que busque determinar sus causales.

Actualmente, el documento electrónico cuenta con una valoración legal dentro de un proceso judicial. En las normas sustantivas se reconoce la eficacia jurídica del documento electrónico, como lo es la rúbrica digital. Sin embargo, cuando se trata de pruebas digitales es necesario se invoque y analicen códigos civiles, penales, procesales penales, comerciales, a fin de poder establecer el tratamiento más adecuado que deberá asignarle a la prueba digital dentro de un proceso judicial. La verdadera problemática de la evidencia digital, obedece principalmente a deficiencias en su tratamiento y a las diversas limitantes que existen alrededor de esta. Además, de que el actual sistema judicial no se

encuentra totalmente adecuado para que los procesos judiciales admitan pruebas de naturaleza digital, puesto que aún se percibe en nuestro sistema un tratamiento tradicionalista de los expedientes, en donde se prioriza el uso del papel.

Problema principal: ¿Cuál es la relación entre los delitos informáticos y el valor probatorio de la evidencia digital en la Corte Superior de Justicia de Lima – 2021?. Problemas específicos: 1) ¿Cuál es la relación entre los delitos informáticos y el bien juridico protegido de la evidencia digital en la Corte Superior de Justicia de Lima - 2021?, 2) ¿Cuál es la relación entre los delitos informáticos y la previsión en la evidencia digital en la Corte Superior de Justicia de Lima - 2021?, 3) ¿Cuál es la relación entre los delitos informáticos y las sanciones de la evidencia digital en la Corte Superior de Justicia de Lima - 2021?, 4) ¿Cuál es la relación entre los delitos informáticos y la legalidad de la evidencia digital en la Corte Superior de Justicia de Lima - 2021?, 5) ¿Cuál es la relación entre los delitos informáticos y la custodia de la evidencia digital en la Corte Superior de Justicia de Lima - 2021?, 6) ¿Cuál es la relación entre los delitos informáticos y el tratamiento de la evidencia digital en la Corte Superior de Justicia de Lima - 2021?, 7) ¿Cuál es la relación entre los delitos informáticos y la atención de la evidencia digital en la Corte Superior de Justicia de Lima - 2021?.

El desarrollo de la presente investigación se justifica plenamente, debido al incremento vertiginoso que han tenido los casos de delitos informáticos en el ámbito nacional e internacional. En los delitos informáticos, muchos de los procesos se fundamentan en la existencia de evidencias digitales como elemento de prueba para iniciar el proceso punitivo sobre el imputado, motivo por el cual la valoración de la prueba constituye un elemento determinante para la acción efectiva de la justicia en la resolución de estos casos.

Objetivo general: Determinar la relación entre los delitos informáticos y el valor probatorio de la evidencia digital en la Corte Superior de Justicia de Lima – 2021. Objetivos específicos: 1) Determinar la relación entre los delitos informáticos y el bien juridico protegido de la evidencia digital en la Corte Superior de Justicia de Lima - 2021, 2) Determinar la relación entre los delitos informáticos y la previsión en la evidencia digital en la Corte Superior de Justicia de Lima - 2021, 3) Determinar la relación entre los delitos informáticos y las sanciones de la evidencia digital en la

Corte Superior de Justicia de Lima - 2021, 4) Determinar la relación entre los delitos informáticos y la legalidad de la evidencia digital en la Corte Superior de Justicia de Lima - 2021, 5) Determinar la relación entre los delitos informáticos y la custodia de la evidencia digital en la Corte Superior de Justicia de Lima - 2021, 6) Determinar la relación entre los delitos informáticos y el tratamiento de la evidencia digital en la Corte Superior de Justicia de Lima - 2021, 7) Determinar la relación entre los delitos informáticos y la atención de la evidencia digital en la Corte Superior de Justicia de Lima - 2021.

Hipótesis general: Los delitos informáticos se relacionan significativamente con el valor probatorio de la evidencia digital en la Corte Superior de Justicia de Lima – 2021. Hipótesis específicas: 1) Los delitos informáticos se relacionan siginificativamente con el bien juridico protegido de la evidencia digital en la Corte Superior de Justicia de Lima - 2021, 2) Los delitos informáticos se relacionan significativamente con la previsión en la evidencia digital en la Corte Superior de Justicia de Lima - 2021, 3) Los delitos informáticos se relacionan significativamente con las sanciones de la evidencia digital en la Corte Superior de Justicia de Lima - 2021, 4) Los delitos informáticos se relacionan significativamente con la legalidad de la evidencia digital en la Corte Superior de Justicia de Lima - 2021, 5) Los delitos informáticos se relacionan significativamente con la custodia de la evidencia digital en la Corte Superior de Justicia de Lima - 2021, 6) Los delitos informáticos se relacionan significativamente con el tratamiento de la evidencia digital en la Corte Superior de Justicia de Lima - 2021, 7) Los delitos informáticos se relacionan significativamente con la atención de la evidencia digital en la Corte Superior de Justicia de Lima - 2021.

II. MARCO TEÓRICO

En el ámbito internacional encontramos la investigación realizada por Rincón (2015), titulada: "*El delito en la cibersociedad y la justicia penal internacional"*. Concluyó en la universalidad de los delitos informáticos, y que su investigación, persecución y lucha debe corresponder a la comunidad internacional, puesto que no representa sólo una problemática que atañe a algunos países, puesto que los beneficios y consecuencias del uso inadecuado de la misma es responsabilidad 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*", teniendo como objetivo el análisis de la victimización de alumnos universitarios en relación a la comisión de delitos informáticos. Concluyó que el miedo de los alumnos universitarios obedece principalmente a ser víctimas de algún fraude por el uso de sus tarjetas de crédito.

Wang (2016) según la tesis titulada "*Estudio comparativo de la ciberdelincuencia en Derecho Penal: China, Estados Unidos, Inglaterra, Singapur y el Consejo de Europa*", tuvo como objetivo el analizar la problemática de la ciberdelincuencia en diferentes marcos normativos a nivel mundial. Concluyó que en China existe un índice menor de ciberdelincuencia, debido en gran medida a las estrictas regulaciones existentes en este país, las cuales representan elementos disuasivos ante estos ilícitos. En los demás países que forman parte del estudio se observa una tendencia creciente ante la ocurrencia de estos delitos, debido a una regulación débil o muy poco articulada, lo cual representa un índice de vulnerabilidad muy alto frente a los delitos suscitados en el ciberespacio.

González y Barbosa (2013) en su investigación titulada "*Delincuencia informática: daños informáticos del artículo 264 del Código Penal y propuesta de Reforma*", tuvo como objetivo analizar desde una perspectiva integral los delitos informáticos, a fin de proponer acciones que promuevan su mitigación. Concluyó que los delitos informáticos disponen de un carácter muy versátil, debido a la naturaleza cambiante de la tecnología y a su avance vertiginoso. Además, señala

que los delitos informáticos no pueden considerarse dentro de los arquetipos ya conocidos de los delitos comunes, puesto que el bien jurídico protegido en muchas ocasiones es inmaterial, y los elementos probatorios responden a pruebas digitales cuyo tratamiento demanda un tratamiento especial, con un régimen jurídico-normativo que abarque todas las implicancias que la consumación de estos delitos conlleva. Asimismo, el autor concluye en el carácter transnacional de estos delitos, puesto que para la lucha eficaz contra este delito no hace faltan sólo regulaciones a nivel país, sino que hace falta políticas regionales, debidamente articuladas que permitan cubrir todo el radio de acción que emplea la ciberdelincuencia para sus ilícitos.

En el contexto nacional, también se han realizado una serie de investigaciones relacionadas al tópico de estudio, tales como la realizada por Nuñez (2016) en su tesis "*Derecho de identidad digital en internet*", tuvo como objetivo analizar las implicancias del derecho de identidad digital en el ciberespacio. Concluyó que el uso de internet en el actual contexto representa un riesgo latente ante la incursión de agentes delictivos que atenten vulnerar sus derechos fundamentales, ejerciendo una falsa identidad a partir del uso de medios tecnológicos, aprovechando los vacíos legales y diversos aspectos que aún no se encuentran debidamente regulados, el autor sostiene que el derecho a la identidad se ve claramente en riesgo en cuatro operaciones o procesos específicos, tales como el gobierno electrónico, la educación a distancia o a modo remoto, las empresas virtuales y el *e-commerce* (comercio electrónico), todas estas operaciones o procesos tienen en común que para iniciarlos deben proporcionar su identidad en sus plataformas digitales, motivo por lo cual el riesgo a ser vulnerado crece de manera exponencial. Asimismo, el autor logró determinar que así como el Estado se muestra como un garante de los derechos fundamentales en un contexto real, también debe de realizar los esfuerzos necesarios para poder regular el marco normativo que proporcione la seguridad jurídica a las personas que interactúan en el ciberespacio.

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*", que tuvo como objetivo determinar la eficacia de la

estrategia de cibeseguridad adoptada por una unidad administrativa de una entidad castrense. Concluyó que la estrategia de ciberseguridad tiene una influencia determinante en la protección de información sensible en la dependencia que sirvió de unidad de estudio. Asimismo, logró determinar la carencia de estrategias que hagan frente ante un eventual ataque ciberterrorista, que busque atentar contra las bases de datos que maneja la entidad castrense, la falta de equipamiento informático de última generación en el procesamiento y manejo de la información lo hace más vulnerable a potenciales ataques gestados desde el ciberespacio.

Alarcón y 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*", tuvo como objetivo determinar la relación entre el uso del internet y los casos de delitos informáticos en los estudiantes universitarios. Concluyó que el uso del internet que implica la obtención de información de índole académico, aunado a la factores sociales del propio personal del estudiante, determinan el incremento de acontecer delitos informáticos en ese contexto.

Espinoza (2017) en la tesis titulada "*Derecho penal informático: deslegitimación del poder punitivo en la sociedad de control*". Concluyó que por las implicancias de los delitos informáticos, estos deben ser regulados dentro del marco del derecho penal. Además, el autor reafirma que estos delitos tienen un alcance transnacional, y su regulación eficaz debe obedecer a políticas transnacionales, debidamente articuladas entre los Estados que permitan reducir los efectos negativos que conlleva la práctica de estos ilícitos penales. Asimismo, considera el carácter multidisciplinario de este delito y concluye aseverando que para hacer frente a sus efectos nocivos, las acciones de los Estados deben abarcar a todas las entidades involucradas en el espectro de acción de estos delitos, logrando de esta manera soluciones debidamente articuladas y con el nivel de coordinación necesario que permita hacerles frente de manera decidida y con resultados auspiciosos y sobretodo que estos se mantengan en el tiempo.

Tenorio y 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 tuvo como objetivo determinar la relación entre

la Ley del Secreto Financiero y el robo informático de dinero mediante la violación de claves secretas. Concluyó que la actual Ley del Secreto Bancario no se encuetra debidamente adecuada con los avances tecnológicos que se dan en el contexto mundial actualmente, presentando una serie de desfases y carencias desde el aspecto técnico, lo cual acrecenta de manera alarmante el índice de vulnerabilidad ante estos delitos. Asimismo, el autor se reafirma en sostener que el secreto financiero representa un obstáculo ante las acciones de investigación por parte de los órganos jurisdiccionales, ya que sólo y exclusivamente puede levantarse este secreto bancario mediante una resolución judicial expresa y sólo para casos concretos. Agregando que en la actualidad no existe una base de datos acerca de delitos relacionados al hurto de caudales y que ninguna entidad maneja datos estadísticos acerca de esta modalidad delictiva que consiste en vulnerar las claves secretas, principalmente mediante prácticas nuevas como el *phishing* o *pharming*.

Según Rayon y Gomez (2014) conceptualizan al ciberdelito como cualquier forma de vulneración ilícita de un espacio virtual con el objeto de obtener información privada y/o confidencial, utilizando como medio para consumarlo, el uso de cualquier tipo de dispositivo tecnológico.

Para Gerke (2014) los términos de ciberdelincuencia y ciberseguridad necesariamente van de la mano en un contexto actual en donde prima el uso de redes que permiten la proliferación de sistemas interconectados en nuestras actividades diarias. La comunidad internacional ha visto con gran preocupación el uso inadecuado de la tecnología, lo cual se traduce en la perpetración de delitos consumados en el ciberespacio y que representan cuantiosas pérdidas para los Estados, y cuya regulación normativa suele ser muy compleja, debido en gran medida a la versatilidad de la tecnología, a su carácter cambiante y a la falta de mecanismos que permitan su regulación integral. La ciberdelincuencia no es una problemática reciente, puesto que ya viene siendo abordado por la comunidad internacional, a través de una serie de dispositivos normativos-legales que buscan su mitigación, prueba de ello es la Resolución de la ONU realizada en el año 2010 sobre la ciberseguridad, es aquí en donde se aborda el ciberdelito como una problemática que atañe al mundo y que requiere de acciones multinacionales para combatirlas de manera eficiente. Es importante señalar, que como la

ciberdelincuencia tiene como ámbito de acción delincuencial el ciberespacio, y este a su vez no cuenta con una jurisdicción determinada, con una responsabilidad propia de algún Estado, las acciones que permitan su mitigación y erradicación deberán de poseer un carácter universal, con estrategias debidamente articuladas en donde los Estados coordinen su accionar desde el plano operativo y legal, la complejidad de estos ilícitos radica primordialmente el el avance vertiginoso que tiene la tecnología, lo cual nos lleva a pensar que las leyes que fueron eficientes hoy, no lo serán mañana, así de compleja resulta la situación que atravieza el mundo con respecto a la preservación de su ciberseguridad actualmente.

Con respecto a la evidencia digital, Santos (2013) citando a Casey, la conceptualiza como todo aquel elemento de naturaleza virtual que relacione a una persona con la comisión de un delito determinado. La evidencia digital constituye un elemento probatorio como cualquier otro que forme parte de un proceso judicial ordinario, con la característica particular que por lo general este elemento de prueba carece de materialidad, ha sido gestado a partir del uso de dispositivos tecnológicos y teniendo como ámbito de acción el ciberespacio.

Asimismo, Santos (2013) sostiene que la evidencia digital refiere a cualquier tipo de información, en la cual hubo algún tipo de intervención del ser humano para poder hacerse de la misma contenida en un dispositivo informático. Coincidimos en lo señalado por Santos, puesto que un elemento de prueba puede significar un factor determinante en cualquier tipo de proceso judicial, sin embargo la particularidad de las evidencias digitales esta representado por el grado de manipulación a la cual están expuestas las referidas pruebas, puesto que son gestadas a partir de medios informáticos, los que a su vez son manipulados por el ser humano, lo que no sucede cuando la prueba es de carácter natural, propia de las circunstancias y que en muchas ocasiones derivan en imputaciones por flagrancia.

Cabe señalar, que la naturaleza digital de este tipo de pruebas, responde en gran medida al modo en que se almacena, se dispone y se crea a partir de recursos informatizados usados de manera individual o como parte de un sistema interconectado. La evidencia digital puede presentarse de difersas formas, tales como archivos de imagen, audio o una mezcla de ambos (videos), todos estos

elementos aportarán de una u otra manera a diluscidar y tener una mayor carga de prueba en relación del delito que se le imputa al procesado, hoy en día los dispositivos informáticos y dispositivos tecnológicos, representan importantes medios para poder obtener evidencias digitales, que con un buen y adecuado tratamiento, y respaldados con hechos concretos, constituyen un elemento idóneo para comprobar la comisión de un acto delictivo hoy en día.

Dicho en otras palabras, la evidencia digital busca otorgarle valor legal a la información contenida en ella, con el propósito de que esta sea considerada como válida dentro de un proceso judicial determinado, para que se cumpla dicho presupuesto, la evidencia digital deberá pasar una serie procesos investigativos que analicen su originalidad, fiabilidad, procedencia y verdadero aporte para el proceso en curso, existen muchas inconsistencia actualmente en nuestro marco jurídico actual en relación a la valoración de la prueba digital, puesto que nuestro sistema judicial aún se rige bajo un carácter tradicional en donde la gran mayoría de elementos probatorios son admitidos a partir de su materialidad.

La evidencia judicial se entiende, según Davis (2002) como cualquier elemento que contribuye al escalrecimiento de un proceso judicial, haciendo uso de los medios y procedimientos legales, debidamente amparados por la ley. Es decir, la prueba se configura en la ley, en la medida que sus implicancias pueden materializarse como un aporte concreto en el proceso judicial que se sigue por la comisión de un ilícito, y de esta manera salvaguardar los derechos de la víctima. (Gutiérrez, 1990).

Siguiendo en esta misma línea de ideas, es necesario entender el manejo adecuado que se debe tener con respecto a la utilización de un elemento probatorio dentro de un proceso judicial, puesto que resulta relevante con miras a que el operador de justicia disponga de la información certera y precisa en torno a las circunstancias en las que se suscitaron los actos que motivaron el accionar punitivo contra el imputado y que de manera concreta y dentro del marco de legalidad del Estado de Derecho se materialice el accionar de la justicia, el cual se logra dilusidando y ejerciendo la sanción respectiva por transgredir derechos fundamentales, es decir mediante el elemento probatorio se busca hacer efectiva la acción punitiva del Estado sobre imputados a los que la presunción de inocencia

ha quedado totalmente desestimada, por los elementos probatorios existentes en su contra. (Bedoya, 2008)

Diversos juristas coinciden en señalar que no se puede establecer a priori la idoneidad de las evidencias digitales en el objetivo de encontrar la verdad de los hechos dentro de un contexto investigatorio por la comisión de un delito, más sin embargo, si se puede afirmar que estos elementos pueden resultar verdaderos obstáculos para el logro del referido fin. El actual sistema judicial busca de manera denodada la forma más idónea de ajusticiar a los delincuentes, reuniendo todos los elementos posibles para probar su acto delictivo, sin embargo en la realidad existen una serie de inconsistencias, vacíos, incoherencias y una serie de restricciones que dificultan otorgar el valor legal a las pruebas digitales, puesto que existen una serie de factores que aun no se encuentran regulados, motivo por el cual terminan siendo desestimados en la fase preliminar de la investigación. (Vivares, 2015)

III. METODOLOGÍA

3.1. Tipo y diseño de investigación

Es una investigación de tipo básica, puesto que con su desarrollo pretende satisfacer la simple curiosidad del investigador en relación a un determinado tópico de estudio. (Ñaupas, 2018)

En relación al diseño, se trata de una investigación no experimental - transeccional - correlacional. Decimos que es no experimental, puesto que su desarrollo se basa íntegramente en la observación del fenómeno acontecido, sin ejercer ningún tipo de manipulación de las variables auscultadas por el investigador. Mientras que es transeccional, debido a todo el estudio se desarrolla dentro de un lapso de tiempo determinado, previamente delimitado. Finalmente, argumentamos que se trata de una investigación correlacional, puesto que tiene por objeto establecer una posible relación entre las variables principales que motivaron la realización del estudio. (Hernández y Mendoza, 2018)

3.2. Variables y operacionalización

Análisis de los delitos informáticos (V1). Definición conceptual: Se tratan de acciones ilícitas utilizando como medio diversos dispositivos tecnológicos, la comisión de estos vulnera la privacidad o patrimonio de las personas naturales o jurídicas, estos delitos se consuman a través de la sustracción de información relevante para esta y que se encuentra alojada en el ciberespacio. (Acosta, Benavides y García, 2020)

Definición operacional: Los delitos informáticos representan ilícitos que basan su accionar en el uso inadecuado de los recursos del ciberespacio, estos delitos transgreden derechos fundamentales como el caso del derecho a la privacidad, al patrimonio o a la libertad, etc. Existen aún muchos vacíos legales alrededor de estos delitos, puesto que por tratarse de delitos relacionados a la tecnología y esta avanza de manera vertiginosa, la aparición de nuevas modalidades, demandan una regulación versátil desde el aspecto normativo-jurídico.

Valor probatorio de la evidencia digital (V2). Definición conceptual: Es la valoración que se le otorga como elemento probatorio a toda aquella información digitalizada que acredite fehacientemente la consumación de algún ilícito que contravenga la ley, y que a su vez aporte cierta nivel de certeza en un determinado proceso judicial. (De La Torre, 2019)

Definición operacional: Es el valor de la evidencia digital como elemento probatorio dentro de un proceso judicial, en donde el operador judicial (Juez) valorará la licitud, pertinencia, necesidad, autenticidad, integridad y cumplimiento de los requisitos procesales que permitan su admisibilidad procedimental de la misma.

3.3. Población, muestra y muestreo

La población es la agrupación de elementos de diversa índole y que guardan alguna característica en común entre ellos, que justifique la selección por parte del investigador, con el propósito de obtener información de parte de estos para fines investigativos. (Caballero, 2014)

En este caso, la población estuvo conformada por los fiscales que laboran en la Fiscalía Corporativa Especializada en Delitos de Ciberdelincuencia de Lima, cuya sede judicial esta compuesta por 14 fiscales especializados en delitos informáticos. Asimismo, se tomó en cuenta la opinión vertida por la División de Investigación de Delitos de Alta Tecnología de la PNP, con sede en la DIRINCRI, ubicada en Lima Cercado, dicha unidad especializada cuenta con 23 efectivos policiales especialistas en delitos digitales. Además se consideró oportuno tomar en cuenta la opinión vertida por abogados litigantes con experiencia en casos de ciberdelincuencia.

Para efectos de la presente investigación, la muestra fue determinada aplicando un muestro por conveniencia, siendo la proximidad y disponibilidad las razones principales de su selección (QuestionPro, 2018). En consecuencia, la muestra quedó determinada de la siguiente manera: 12 fiscales pertenecientes a la Fiscalía Corporativa Especializada en Delitos de Ciberdelincuencia de Lima, 15 efectivos policiales de la División de Investigación de Delitos de Alta Tecnología de la PNP y 10 abogados litigantes con experiencia en casos de ciberdelincuencia.

3.4. Técnicas e instrumentos de recolección de datos

La encuesta fue la técnica seleccionada para la recolección de datos y esta a su vez se instrumentalizó mediante un cuestionario de preguntas orientadas a conocer la situación de las variables planteadas, a través de las respuestas proporcionadas por nuestra muestra definida.

3.5. Procedimientos

A fin de recolectar la información haciendo uso del instrumento seleccionado, se realizó un cuestionario de preguntas, estructurado a partir de los indicadores planteados en la operacionalización de variables. Con la finalidad de garantizar la validez y confiabilidad del referido instrumento se recurrió al método de juicio de expertos, que en nuestro caso fueron docentes de la UCV de la carrera profesional de Derecho (ver tabla 1), quienes mediante su criterio y experiencia determinaron la aplicabilidad del instrumento sometido a juicio.

Tabla 1

Expertos validadores del instrumento de recolección de datos

Validador	Cargo e institución a la que pertenece	Promedio de valoración (%)	Criterio
Yanira Guisella Lázaro Ortiz	Docente UCV	90%	Aplicable
Liliam Lesly Castro Rodríguez	Docente UCV	85%	Aplicable

Nota: Los formatos de validación del instrumento se encuentran dispuestos en la sección de anexos.

Mientras que la confiabilidad fue determinada de manera estadística, aplicando el coeficiente Alfa de Cronbach, el cual se encuentra dispuesto dentro de las funcionalidades del programa computacional SPSS de la IBM en su versión 25. Los resultados de la confiabilidad se muestran en la Tabla 2:

Tabla 2

Confiabilidad del instrumento - Alfa de Cronbach

Alfa de Cronbach	N de elementos
,924	30

Fuente: SPSS 25.0

Una vez validado y con la confiabilidad necesaria, se virtualizó el instrumento, a fin de aplicarlo de manera remota, se utilizó el aplicativo *Google forms* para digitalizar el cuestionario y poder remitirlo a los individuos que

componen la muestra seleccionada, para ello previamente se confeccionó un listado con los correos electrónicos de cada individuo, las respuesta emitidas por estos, se derivaron de manera automática y en tiempo real al Google drive del investigador, a fin de acopiar las respuestas y de esta manera puedan ser procesadas y analizadas como parte del capítulo de resultados.

3.6. Método de análisis de datos

Los resultados obtenidos como parte del trabajo de campo, se analizaron y procesaron de manera estadística, específicamente haciendo uso de la estadística descriptiva e inferencial. La primera de ellas, sirvió para la elaboración de los cuadros y demás elementos gráficos que reflejan los resultados obtenidos del trabajo de campo, mientras que la estadística inferencial se utilizó principalmente para la contrastación de las hipótesis planteadas y que permitieron abordar la discusión de resultados, y por ende llegar a conclusiones más precisas y proponer recomendaciones más eficaces para mitigar la problemática que motivó el desarrollo del presente estudio. Debemos indicar que para el tratamiento, procesamiento y posterior análisis de la información recabada se utilizó el programa estadístico SPSS, apoyándonos con el programa Microsoft Excel 2019 para la tabulación de la base de datos provenientes de nuestras fuentes primarias.

3.7. Aspectos éticos

El desarrollo íntegro del presente estudio se ciñó a los lineamientos y directrices establecidas por la UCV para efectos de la realización de trabajos de investigación para la obtención del título profesional. Además, toda la información contenida se encuentra debidamente referenciada y citada bajo la normativa APA en su edición vigente, garantizando de esta manera no incurrir en actos de plagio que contravengan a los derechos de autor, para ello se sometió a la evaluación del porcentaje de similitud del trabajo de investigación, haciendo uso del software antiplagio Turnitin, con el cual verificamos que el porcentaje de similitud no supere el máximo permitido por la Universidad, el cual asciende a un 25%. Cabe señalar, que en la aplicación del cuestionario, se respetó el anonimato de los individuos, garantizando la confidencialidad de los mismos, reafirmando que la información obtenida sea utilizada sólo y exclusivamente para fines académicos.

IV. RESULTADOS Y DISCUSIÓN

4.1. Resultados

Tabla 3

Relación entre la variable análisis de los delitos informáticos y la variable valor probatorio de la evidencia digital

			Valor probatorio de la evidencia digital			Total
			BAJO	MEDIO	ALTO	
Análisis de los delitos informáticos	BAJO	Recuento	1	2	2	5
		% del total	2,7%	5,4%	5,4%	13,5%
	MEDIO	Recuento	0	13	13	26
		% del total	0,0%	35,1%	35,1%	70,3%
	ALTO	Recuento	0	1	5	6
		% del total	0,0%	2,7%	13,5%	16,2%
Total		Recuento	1	16	20	37
		% del total	2,7%	43,2%	54,1%	100,0%

Fuente: Elaboración propia.

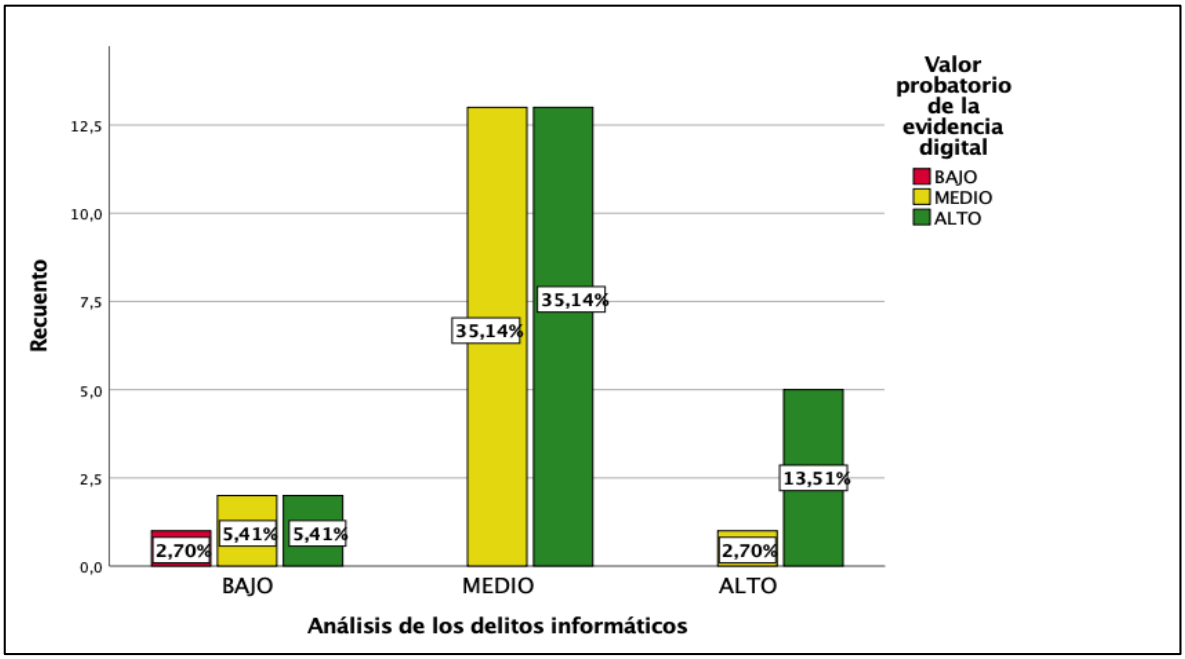


Figura 1. Relación entre la variable análisis de los delitos informáticos y la variable valor probatorio de la evidencia digital. Fuente: Elaboración propia.

Interpretación.- En la tabla 3 y figura 1, se observa que un 70,3% de los informantes considera una incidencia media de los delitos informáticos. Mientras que un 54,1% refiere que en la mayoría de casos de delitos informáticos se evidencia un valor probatorio de la evidencia digital alto.

Tabla 4

Relación entre la variable análisis de delitos informáticos y la dimensión bien jurídico protegido

			Bien jurídico protegido			Total
			MALO	REGULAR	BUENO	
Análisis de los delitos informáticos	BAJO	Recuento	2	2	1	5
		% del total	5,4%	5,4%	2,7%	13,5%
	MEDIO	Recuento	6	14	6	26
		% del total	16,2%	37,8%	16,2%	70,3%
	ALTO	Recuento	0	2	4	6
		% del total	0,0%	5,4%	10,8%	16,2%
Total		Recuento	8	18	11	37
		% del total	21,6%	48,6%	29,7%	100,0%

Fuente: Elaboración propia.

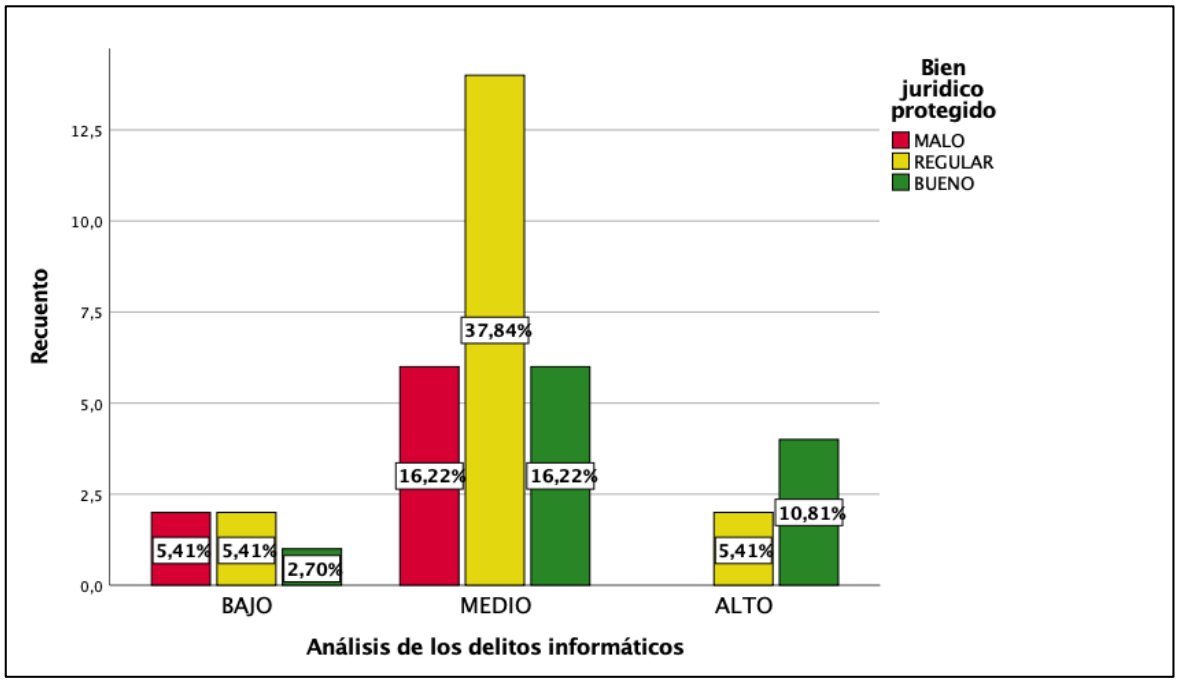


Figura 2. Relación entre la variable análisis de delitos informáticos y la dimensión bien jurídico protegido. Fuente: Elaboración propia.

Interpretación.- En la tabla 4 y figura 2, se observa que, un 70,3% de los informantes considera una incidencia media de los delitos informáticos. Mientras que, un 48,6% señala que se percibe como regular el bien jurídico protegido por la evidencia digital en el caso de delitos informáticos.

Tabla 5

Relación entre la variable análisis de delitos informáticos y la dimensión previsión

			Previsión			Total
			MALA	REGULAR	BUENA	
Análisis de los delitos informáticos	BAJO	Recuento	4	0	1	5
		% del total	10,8%	0,0%	2,7%	13,5%
	MEDIO	Recuento	3	8	15	26
		% del total	8,1%	21,6%	40,5%	70,3%
	ALTO	Recuento	1	1	4	6
		% del total	2,7%	2,7%	10,8%	16,2%
Total		Recuento	8	9	20	37
		% del total	21,6%	24,3%	54,1%	100,0%

Fuente: Elaboración propia.

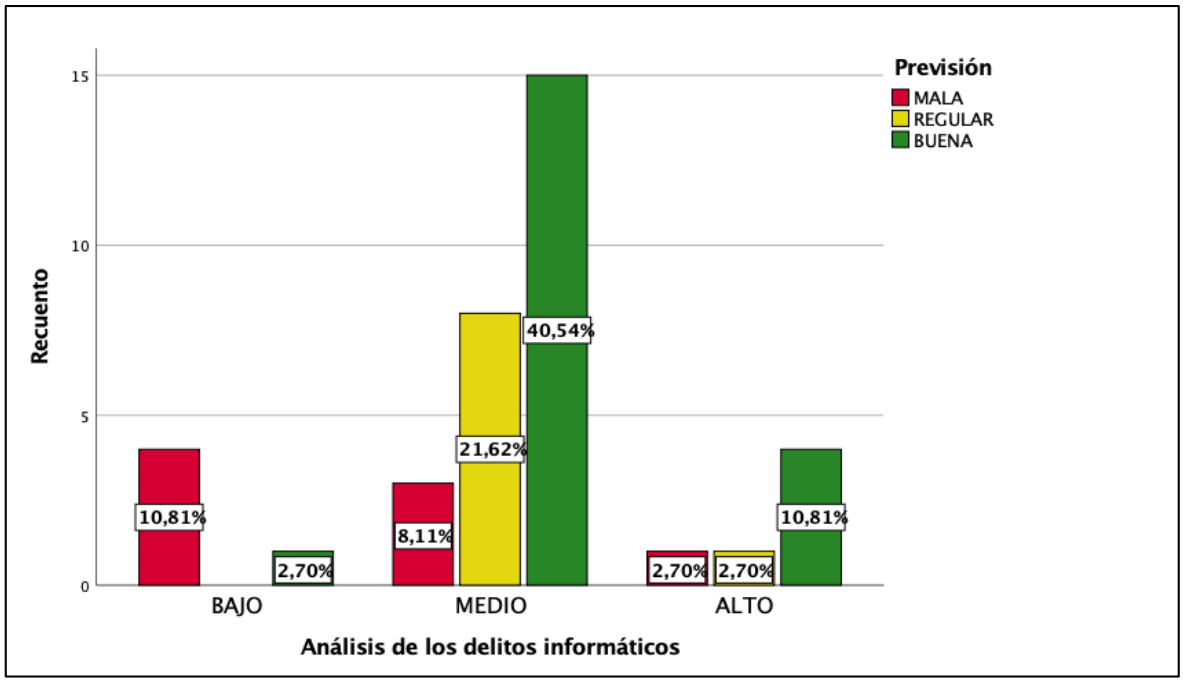


Figura 3. Relación entre la variable análisis de delitos informáticos y la dimensión previsión. Fuente: Elaboración propia.

Interpretación.- En la tabla 5 y figura 3, se observa que, un 70,3% de los informantes refieren una incidencia media de los delitos informáticos. Mientras que, un 54,1% considera que existe una previsión buena con respecto a la evidencia digital en los delitos informáticas.

Tabla 6

Relación entre la variable análisis de delitos informáticos y la dimensión sanciones

			Sanciones			Total
			Poco efectivas	Regularmente efectivas	Altamente efectivas	
Análisis de los delitos informáticos	BAJO	Recuento	1	3	1	5
		% del total	2,7%	8,1%	2,7%	13,5%
	MEDIO	Recuento	2	15	9	26
		% del total	5,4%	40,5%	24,3%	70,3%
	ALTO	Recuento	0	2	4	6
		% del total	0,0%	5,4%	10,8%	16,2%
Total		Recuento	3	20	14	37
		% del total	8,1%	54,1%	37,8%	100,0%

Fuente: Elaboración propia.

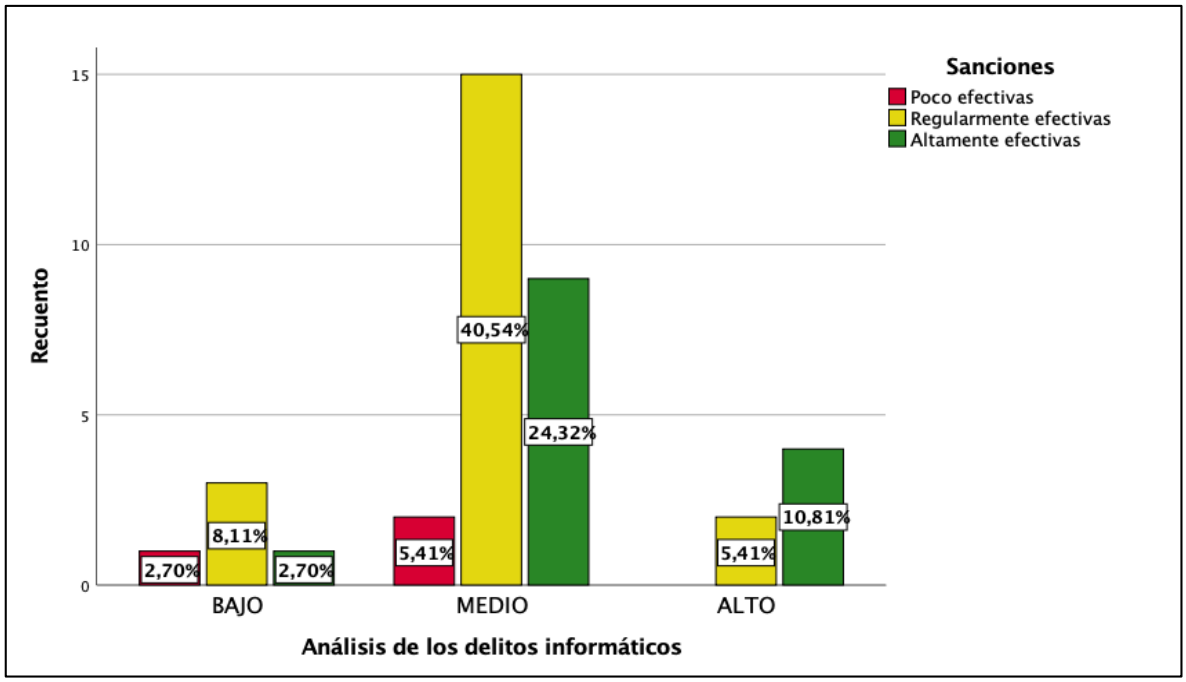


Figura 4. Relación entre la variable análisis de delitos informáticos y la dimensión sanciones. Fuente: Elaboración propia.

Interpretación.- En la tabla 6 y figura 4, se observa que, un 70,3% de los informantes refieren una incidencia media de los delitos informáticos. Mientras que, un 54,1% considera que las sanciones en los delitos informáticos se muestran regularmente efectivas frente a la mitigación de este ilícito.

Tabla 7

Relación entre la variable análisis de delitos informáticos y la dimensión legalidad

			Legalidad			Total
			BAJO	MEDIO	ALTO	
Análisis de los delitos informáticos	BAJO	Recuento	1	3	1	5
		% del total	2,7%	8,1%	2,7%	13,5%
	MEDIO	Recuento	1	15	10	26
		% del total	2,7%	40,5%	27,0%	70,3%
	ALTO	Recuento	0	2	4	6
		% del total	0,0%	5,4%	10,8%	16,2%
Total		Recuento	2	20	15	37
		% del total	5,4%	54,1%	40,5%	100,0%

Fuente: Elaboración propia.

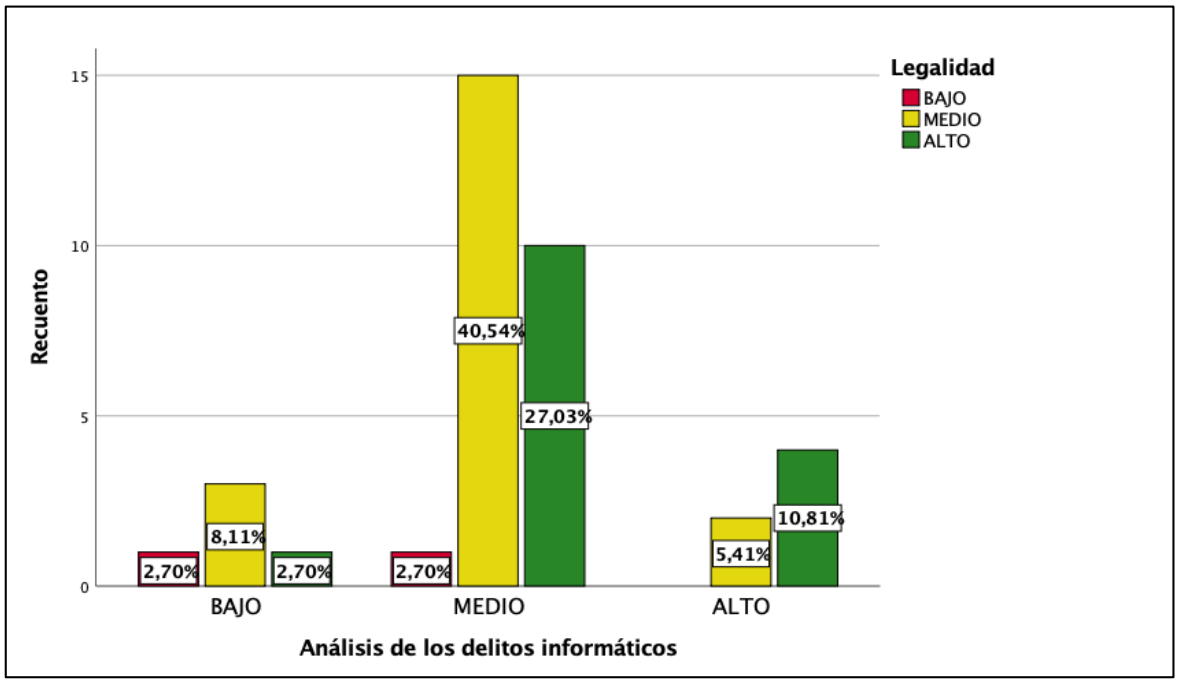


Figura 5. Relación entre la variable análisis de delitos informáticos y la dimensión legalidad. Fuente: Elaboración propia.

Interpretación.- En la tabla 7 y figura 5, se observa que, un 70,3% de los informantes refieren una incidencia media de los delitos informáticos. Mientras que, un 54,1% considera que en los casos por delitos informáticos, el factor legalidad se muestra con una incidencia media con respecto a la evidencia digital como parte del proceso por este tipo de ilícitos.

Tabla 8

Relación entre la variable análisis de delitos informáticos y la dimensión custodia

			Custodia			Total
			MALO	REGULAR	BUENO	
Análisis de los delitos informáticos	BAJO	Recuento	1	4	0	5
		% del total	2,7%	10,8%	0,0%	13,5%
	MEDIO	Recuento	8	12	6	26
		% del total	21,6%	32,4%	16,2%	70,3%
	ALTO	Recuento	1	0	5	6
		% del total	2,7%	0,0%	13,5%	16,2%
Total		Recuento	10	16	11	37
		% del total	27,0%	43,2%	29,7%	100,0%

Fuente: Elaboración propia.

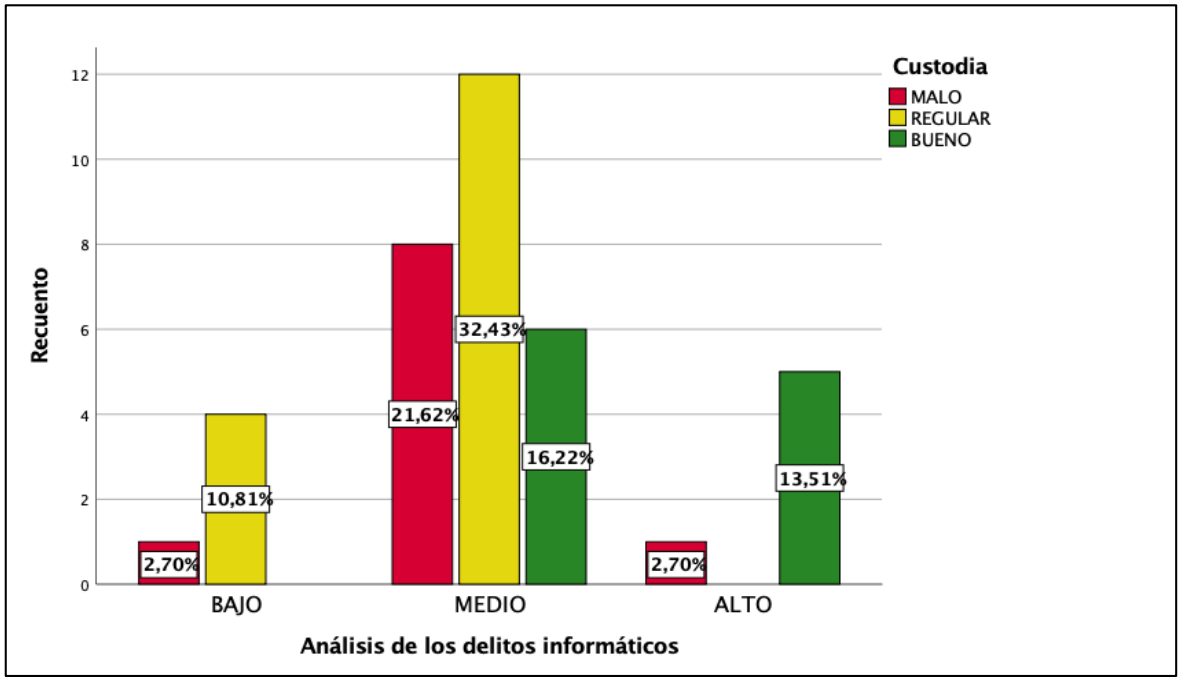


Figura 6. Relación entre la variable análisis de delitos informáticos y la dimensión custodia. Fuente: Elaboración propia.

Interpretación.- En la tabla 8 y figura 6, se observa que, un 70,3% de los informantes refieren una incidencia media de los delitos informáticos. Mientras que, un 43,2% consideran que el nivel de custodia con respecto a la evidencia digital se muestra con una efectividad regular.

Tabla 9

Relación entre la variable análisis de delitos informáticos y la dimensión tratamiento

			Tratamiento			Total
			MALO	REGULAR	BUENO	
Análisis de los delitos informáticos	BAJO	Recuento	1	2	2	5
		% del total	2,7%	5,4%	5,4%	13,5%
	MEDIO	Recuento	5	12	9	26
		% del total	13,5%	32,4%	24,3%	70,3%
	ALTO	Recuento	0	2	4	6
		% del total	0,0%	5,4%	10,8%	16,2%
Total		Recuento	6	16	15	37
		% del total	16,2%	43,2%	40,5%	100,0%

Fuente: Elaboración propia.

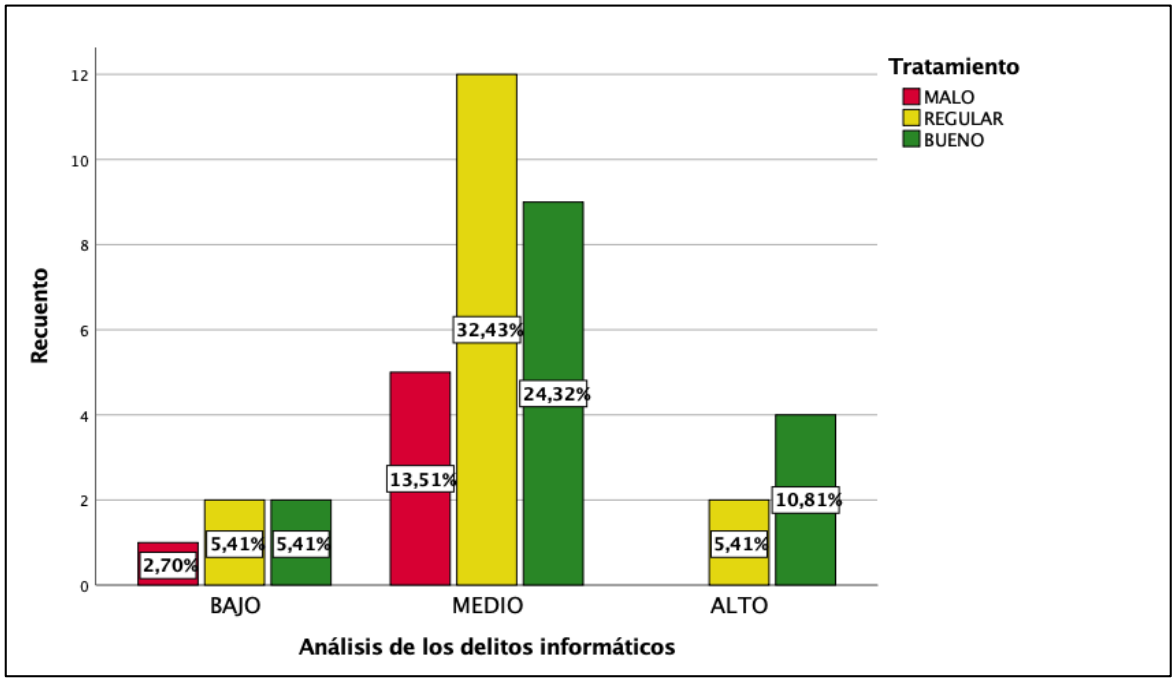


Figura 7. Relación entre la variable análisis de delitos informáticos y la dimensión tratamiento. Fuente: Elaboración propia.

Interpretación.- En la tabla 9 y figura 7, se observa que, un 70,3% de los informantes refieren una incidencia media de los delitos informáticos. Mientras que, un 43,2% consideran que el nivel de tratamiento con respecto a la evidencia digital se muestra con una efectividad regular.

Tabla 10

Relación entre la variable análisis de delitos informáticos y la dimensión atención

			Atención			Total
			MALO	REGULAR	BUENO	
Análisis de los delitos informáticos	BAJO	Recuento	2	2	1	5
		% del total	5,4%	5,4%	2,7%	13,5%
	MEDIO	Recuento	3	15	8	26
		% del total	8,1%	40,5%	21,6%	70,3%
	ALTO	Recuento	0	3	3	6
		% del total	0,0%	8,1%	8,1%	16,2%
Total		Recuento	5	20	12	37
		% del total	13,5%	54,1%	32,4%	100,0%

Fuente: Elaboración propia.

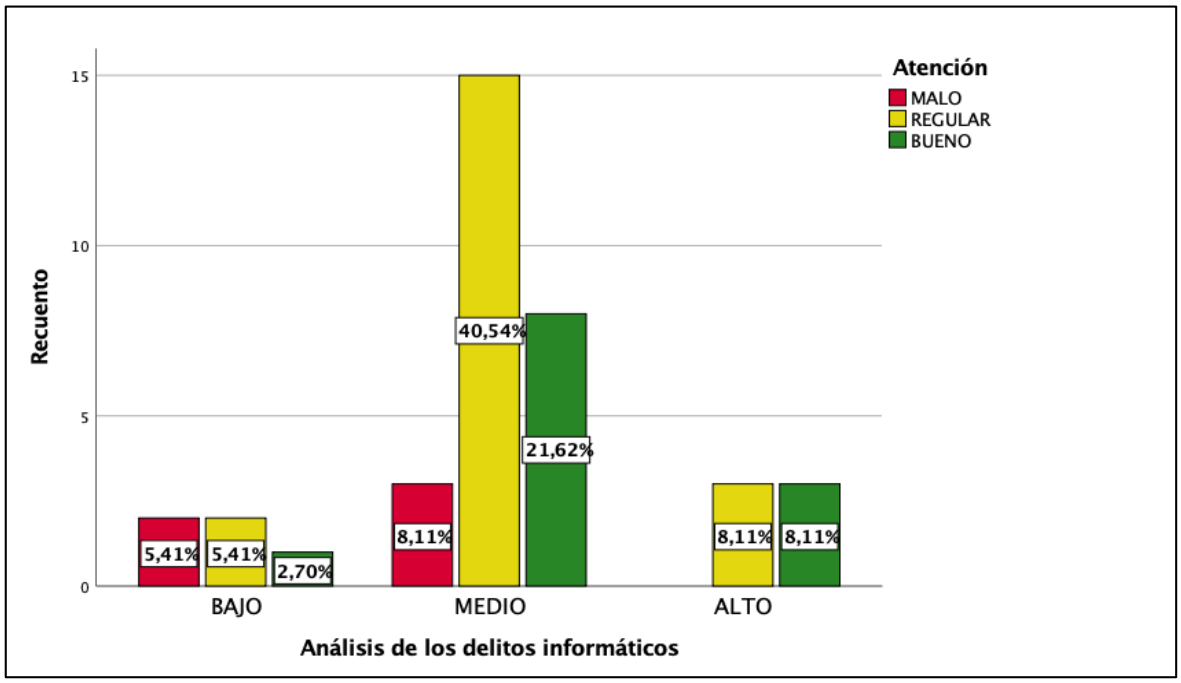


Figura 8. Relación entre la variable análisis de delitos informáticos y la dimensión atención. Fuente: Elaboración propia.

Interpretación.- En la tabla 10 y figura 8, se observa que, un 70,3% de los informantes refieren una incidencia media de los delitos informáticos. Mientras que, un 54,1% consideran que el nivel de atención con respecto a la evidencia digital se muestra con una efectividad regular.

4.2. Discusión

Tabla 11

Correlación entre las variables Análisis de los delitos informáticos y Valor probatorio de la evidencia digital

			Análisis de los delitos informáticos	Valor probatorio de la evidencia digital
Rho de Spearman	Análisis de los delitos informáticos	Coeficiente de correlación	1,000	,283**
		Sig. (bilateral)	.	,000
		N	37	37
	Valor probatorio de la evidencia digital	Coeficiente de correlación	,283**	1,000
		Sig. (bilateral)	,000	.
		N	37	37

**. La correlación es significativa en el nivel 0,01 (bilateral).

Fuente: SPSS - Elaboración propia.

Se observa en la tabla 11, que el coeficiente de correlación de Rho Spearman ha obtenido un nivel de significancia 0,000, teniendo como resultado 0,283, que indica que existe una correlación positiva entre las variables Análisis de los delitos informáticos y Valor probatorio de la evidencia digital. Como el nivel de significancia obtenido es inferior a 0,5 (0,000 < 0,5), indica que se rechaza la hipótesis nula y por el contrario se acepta la hipótesis afirmativa, esto quiere decir que, el Análisis de los delitos informáticos se relaciona de manera significativa con el Valor probatorio de la evidencia digital en la Corte Superior de Justicia de Lima - 2021.

Tabla 12

Correlación entre la variable Análisis de los delitos informáticos y el Bien jurídico protegido

			Análisis de los delitos informáticos	Bien jurídico protegido
Rho de Spearman	Análisis de los delitos informáticos	Coeficiente de correlación	1,000	,345**
		Sig. (bilateral)	.	,000
		N	37	37
	Bien jurídico protegido	Coeficiente de correlación	,345**	1,000
		Sig. (bilateral)	,000	.
		N	37	37

**. La correlación es significativa en el nivel 0,01 (bilateral).

Fuente: SPSS - Elaboración propia.

Se observa en la tabla 12, que el coeficiente de correlación de Rho Spearman ha obtenido un nivel de significancia 0,000, teniendo como resultado 0,345, que indica que existe una correlación positiva entre la variable Análisis de los delitos informáticos y el Bien jurídico protegido de la evidencia digital. Como el nivel de significancia obtenido es inferior a 0,5 (0,000 < 0,5), indica que se rechaza la hipótesis nula y por el contrario se acepta la hipótesis afirmativa, esto quiere decir que, el Análisis de los delitos informáticos se relaciona de manera significativa con el Bien jurídico protegido de la evidencia digital en la Corte Superior de Justicia de Lima - 2021.

Tabla 13

Correlación entre la variable Análisis de los delitos informáticos y la Previsión

			Análisis de los delitos informáticos	Previsión
Rho de Spearman	Análisis de los delitos informáticos	Coeficiente de correlación	1,000	,320**
		Sig. (bilateral)	.	,000
		N	37	37
	Previsión	Coeficiente de correlación	,320**	1,000
		Sig. (bilateral)	,000	.
		N	37	37

**. La correlación es significativa en el nivel 0,01 (bilateral).

Fuente: SPSS - Elaboración propia.

Se observa en la tabla 13, que el coeficiente de correlación de Rho Spearman ha obtenido un nivel de significancia 0,000, teniendo como resultado 0,320, que indica que existe una correlación positiva entre la variable Análisis de los delitos informáticos y la Previsión de la evidencia digital. Como el nivel de significancia obtenido es inferior a 0,5 (0,000 < 0,5), indica que se rechaza la hipótesis nula y por el contrario se acepta la hipótesis afirmativa, esto quiere decir que, el Análisis de los delitos informáticos se relaciona de manera significativa con la Previsión de la evidencia digital en la Corte Superior de Justicia de Lima - 2021.

Tabla 14

Correlación entre la variable Análisis de los delitos informáticos y las Sanciones

			Análisis de los delitos informáticos	Sanciones
Rho de Spearman	Análisis de los delitos informáticos	Coeficiente de correlación	1,000	,299**
		Sig. (bilateral)	.	,001
		N	37	37
	Sanciones	Coeficiente de correlación	,299**	1,000
		Sig. (bilateral)	,001	.
		N	37	37

**. La correlación es significativa en el nivel 0,01 (bilateral).

Fuente: SPSS - Elaboración propia.

Se observa en la tabla 14, que el coeficiente de correlación de Rho Spearman ha obtenido un nivel de significancia 0,001, teniendo como resultado 0,299, que indica que existe una correlación positiva entre la variable Análisis de los delitos informáticos y las Sanciones de la evidencia digital. Como el nivel de significancia obtenido es inferior a 0,5 (0,001 < 0,5), indica que se rechaza la hipótesis nula y por el contrario se acepta la hipótesis afirmativa, esto quiere decir que, el Análisis de los delitos informáticos se relaciona de manera significativa con las Sanciones de la evidencia digital en la Corte Superior de Justicia de Lima - 2021.

Tabla 15

Correlación entre la variable Análisis de los delitos informáticos y la Legalidad

			Análisis de los delitos informáticos	Legalidad
Rho de Spearman	Análisis de los delitos informáticos	Coeficiente de correlación	1,000	,301**
		Sig. (bilateral)	.	,000
		N	37	37
	Legalidad	Coeficiente de correlación	,301**	1,000
		Sig. (bilateral)	,000	.
		N	37	37

**. La correlación es significativa en el nivel 0,01 (bilateral).

Fuente: SPSS - Elaboración propia.

Se observa en la tabla 15, que el coeficiente de correlación de Rho Spearman ha obtenido un nivel de significancia 0,000, teniendo como resultado 0,301, que indica que existe una correlación positiva entre la variable Análisis de los delitos informáticos y la Legalidad de la evidencia digital. Como el nivel de significancia obtenido es inferior a 0,5 (0,000 < 0,5), indica que se rechaza la hipótesis nula y por el contrario se acepta la hipótesis afirmativa, esto quiere decir que, el Análisis de los delitos informáticos se relaciona de manera significativa con la Legalidad de la evidencia digital en la Corte Superior de Justicia de Lima - 2021.

Tabla 16

Correlación entre la variable Análisis de los delitos informáticos y la Custodia

			Análisis de los delitos informáticos	Custodia
Rho de Spearman	Análisis de los delitos informáticos	Coeficiente de correlación	1,000	,336**
		Sig. (bilateral)	.	,000
		N	37	37
	Custodia	Coeficiente de correlación	,336**	1,000
		Sig. (bilateral)	,000	.
		N	37	37

**. La correlación es significativa en el nivel 0,01 (bilateral).

Fuente: SPSS - Elaboración propia.

Se observa en la tabla 16, que el coeficiente de correlación de Rho Spearman ha obtenido un nivel de significancia 0,000, teniendo como resultado 0,336, que indica que existe una correlación positiva entre la variable Análisis de los delitos informáticos y la Custodia de la evidencia digital. Como el nivel de significancia obtenido es inferior a 0,5 (0,000 < 0,5), indica que se rechaza la hipótesis nula y por el contrario se acepta la hipótesis afirmativa, esto quiere decir que, el Análisis de los delitos informáticos se relaciona de manera significativa con la Custodia de la evidencia digital en la Corte Superior de Justicia de Lima - 2021.

Tabla 17

Correlación entre la variable Análisis de los delitos informáticos y el Tratamiento

			Análisis de los delitos informáticos	Tratamiento
Rho de Spearman	Análisis de los delitos informáticos	Coeficiente de correlación	1,000	,192**
		Sig. (bilateral)	.	,001
		N	37	37
	Tratamiento	Coeficiente de correlación	,192**	1,000
		Sig. (bilateral)	,001	.
		N	37	37

**. La correlación es significativa en el nivel 0,01 (bilateral).

Fuente: SPSS - Elaboración propia.

Se observa en la tabla 17, que el coeficiente de correlación de Rho Spearman ha obtenido un nivel de significancia 0,001, teniendo como resultado 0,192, que indica que existe una correlación positiva entre la variable Análisis de los delitos informáticos y el Tratamiento de la evidencia digital. Como el nivel de significancia obtenido es inferior a 0,5 (0,001 < 0,5), indica que se rechaza la hipótesis nula y por el contrario se acepta la hipótesis afirmativa, esto quiere decir que, el Análisis de los delitos informáticos se relaciona de manera significativa con el Tratamiento de la evidencia digital en la Corte Superior de Justicia de Lima - 2021.

Tabla 18

Correlación entre la variable Análisis de los delitos informáticos y la Atención

			Análisis de los delitos informáticos	Atención
Rho de Spearman	Análisis de los delitos informáticos	Coeficiente de correlación	1,000	,277**
		Sig. (bilateral)	.	,000
		N	37	37
	Atención	Coeficiente de correlación	,277**	1,000
		Sig. (bilateral)	,000	.
		N	37	37

**. La correlación es significativa en el nivel 0,01 (bilateral).

Fuente: SPSS - Elaboración propia.

Se observa en la tabla 18, que el coeficiente de correlación de Rho Spearman ha obtenido un nivel de significancia 0,000, teniendo como resultado 0,277, que indica que existe una correlación positiva entre la variable Análisis de los delitos informáticos y la Atención de la evidencia digital. Como el nivel de significancia obtenido es inferior a 0,5 (0,000 < 0,5), indica que se rechaza la hipótesis nula y por el contrario se acepta la hipótesis afirmativa, esto quiere decir que, el Análisis de los delitos informáticos se relaciona de manera significativa con la Atención de la evidencia digital en la Corte Superior de Justicia de Lima - 2021.

V. CONCLUSIONES

1. De acuerdo a los resultados obtenidos, se ha podido determinar la existencia de una relación significativa entre los delitos informáticos y el valor probatorio de la evidencia digital en la Corte Superior de Justicia de Lima durante el período 2021. Dicha situación obedece principalmente al hecho de que actualmente nuestro sistema judicial no está otorgando el debido valor probatorio a la evidencia digital para poder atribuir la culpabilidad de un acusado por delitos informáticos, esta situación obedece a que no se realiza una eficiente valoración de la evidencia digital, y hasta en muchos casos se observa que se desestima la evidencia, debido a un inadecuado tratamiento de la misma, motivo por el cual no puede ser considerada dentro del proceso, este tratamiento erróneo, se produce en gran medida por el desconocimiento y la falta de expertíz; asimismo, se observa que si bien es cierto la tecnología avanza a pasos agigantados, más no sucede lo mismo con la legislación nacional en lo que respecta a delitos acontecidos en el ciberespacio y usando medios digitales, nuestra legislación aún se encuentra muy incipiente en regulación de delitos informáticos, por ello existen serias falencias sobretodo en el tratamiento y disposición de la evidencia digital que permita considerarla como un elemento probatorio objetivo que permita aportar en la resolución de los casos por delitos informáticos.
2. Se ha podido determinar la existencia de una relación significativa entre los delitos informáticos y el bien jurídico protegido en la Corte Superior de Justicia de Lima durante el período 2021. Dicha situación obedece principalmente a la falta de reconocimiento de la funcionalidad informática como bien jurídico específico, cabe señalar que la funcionalidad informática constituye un presupuesto necesario para que las personas e instituciones puedan realizar una serie de actividades que permitan una mejor calidad de vida y optimizar el servicio que brindan a la ciudadanía respectivamente. La funcionalidad informática representa el conjunto de factores que permiten que los sistemas informáticos puedan realizar eficientemente operaciones como almacenar, procesar y transferir datos, todo ello dentro de un nivel tolerable de riesgo. En este contexto, la funcionalidad informática representa

un aspecto relevante de interés, cuyo sentido y alcance debe ser preciso y dinámico, así mismo es necesario considerar la operatividad del uso de las redes computacionales, en diversas sistemas interconectados. Ello constituye, un bien jurídico instrumental de carácter colectivo, cuya tutela penal debe ser sometida a constante verificación en términos acotados de manera particular.

3. Se ha logrado determinar la existencia de una relación significativa entre los delitos informáticos y procedimientos realizados de manera adecuada aseguran el valor probatorio de la evidencia digital, tales como la previsión, sanciones, legalidad, custodia, tratamiento y atención. Dicha situación obedece principalmente a la falta de un marco normativo adecuado para el tratamiento eficiente de la evidencia digital en el caso de delitos informáticos, es menester una legislación autónoma que permita implementar políticas sectoriales que permitan combatir frontalmente el poder pluriofensivo de los delitos informáticos. Actualmente, los delitos informáticos han sido “insertados” a la legislación existente, lo cual consideramos que no es adecuado, porque el avance de la tecnología es vertiginoso y así como representa un enorme beneficio para la humanidad en general, también constituye un peligro constante e inminente por la dependencia que tenemos hoy en día las personas a los medios tecnológicos. La falta de una normativa autónoma, bien definida y adecuada a la realidad peruana, ha devenido en serias deficiencias en la forma que vienen siendo abordado los procedimientos investigatorios para el desarrollo de un proceso judicial con todos los elementos necesarios que garanticen un debido proceso, respetando los derechos y garantías de ambas partes. Las serias deficiencias en los procedimientos que aseguran el valor probatorio de la evidencia digital, es producto de la falta de programas y eventos de capacitación al personal responsable de su tratamiento y disposición, en muchas ocasiones la falta de pericia en este aspecto, ha determinado la invalidez de la evidencia, la cual pudo resultar siendo determinante para su eficiente resolución.

VI. RECOMENDACIONES

1. Se recomienda que los operadores de justicia realicen una mejor valoración probatoria de la evidencia digital, se debe realizar una reforma integral de la legislación actual e incluirlo dentro de la legislación penal, dotándolo de un carácter autónomo, a fin de que pueda contemplar todos los delitos y modalidades que vienen aconteciendo por los avances de la tecnología, y no sólo debe incluirse dentro de una normativa ya constituida, puesto que actualmente se encuentra incluida como parte de los delitos contra el patrimonio en materia penal, sin embargo es necesario que se logre su autonomía como un delito con sus alcances, motivaciones y presupuestos propios.
2. Se recomienda considerar de una forma más integral el bien jurídico protegido de los delitos informáticos, pues en la actualidad sólo considera al patrimonio como el bien jurídico protegido en este tipo de ilícitos, se debe dotar a la legislación actual de los presupuestos necesarios para extender el alcance del bien jurídico protegido, puesto que a nuestro entender no sólo implica una afectación sólo al patrimonio personal, lo cual no corresponde a la realidad, puesto que se trata de un delito pluriofensivo, puesto que no sólo atentan contra el patrimonio personal sino al orden económico, seguridad nacional, derechos fundamentales, etc., lo cual demanda acciones que reformulen el bien jurídico en este tipo de delitos, se debe plantear una visión más integral y multisectorial, puesto que este ilícito tiene consecuencias que atañen a varios sectores del Estado y a todos sus niveles.
3. Se recomienda desarrollar programas de capacitación e inducción dirigidos a los funcionarios judiciales para el adecuado proceso, tratamiento y disposición de la evidencia digital y de esta manera se asegure el valor probatorio que pueden aportar estos elementos en los procesos judiciales llevados por a cabo por la comisión de delitos informáticos, programas de capacitación que permitan conocer más a fondo acerca de la previsión, sanciones, legalidad, custodia, tratamiento y atención que se debe tener acerca de la evidencia digital.

REFERENCIAS

Ñaupas, P. H., Valdivia, D. M., Palacios, V. J., & Romero, D. H. (2018). *Metodología de la investigación cuantitativa-cualitativa y redacción de tesis.* Bogotá: Ediciones de la U.

Hernández, S. R., & Mendoza, T. C. (2018). *Metodología de la investigación. Las rutas cuantitativa, cualitativa y mixta.* México D.F.: McGraw-Hill .

Higa, S. C. (2015). El derecho a la presunción de inocencia desde un punto de vista constitucional. *Derecho & Sociedad*, 113-120. Obtenido de file:///C:/Users/User/Downloads/12793-Texto%20del%20art%C3%ADculo-50866-1-10-20150525.pdf

Nuevo Código Procesal Penal (2004).

Ruíz, B. C. (2013). *Instrumentos y Técnicas de Investigación Educativa. Un Enfoque Cuantitativo para la Recolección y Análisis de Datos* (Vol. III). Houston, USA: DANAGA Training and Consulting. Obtenido de https://www.academia.edu/37886948/Instrumentos_y_Tecnicas_de_Investigaci%C3%B3n_Educativa_Carlos_Ruiz_Bolivar_pdf

De La Torre, R. P. (11 de Febrero de 2019). *La prueba digital en el proceso judicial*. Obtenido de indalics. Peritos informáticos: https://indalics.com/blog-peritaje-informatico/prueba-digital-proceso-judicial

Acosta, M. G., Benavides, M. M., & García, N. P. (2020). Delitos informáticos: Impunidad organizacional y su complejidad en el mundo de los negocios. *Revista Venezolana de Gerencia, 25*(89), 351-368.

Manual de evidencia digital. (12 de Julio de 2017). *Portal oficial del Ministerio Público Fiscalía de la Nación.* Obtenido de Archivo central del MPFN: https://www.mpfn.gob.pe/Docs/0/files/manual_evidencia_digital.pdf

Osco, E. M. (23 de Enero de 2019). *La admisibilidad y el valor probatorio de la evidencia digital en el Sistema Jurídico Peruano 2018. [Tesis de maestría, Universidad César Vallejo].* Obtenido de Repositorio Institucional de la Universidad César Vallejo: https://repositorio.ucv.edu.pe/handle/20.500.12692/26623

Gómez, A. D. (2020). Implicaciones jurídicas de la evidencia digital en el proceso judicial colombiano. *Ratio Juris, 15*(30), 220-240.

Ñaupas, P. H., Valdivia, D. M., Palacios, V. J., & Romero, D. H. (2018). *Metodología de la investigación. Cuantitativa - Cualitativa y Redacción de la Tesis* (Quinta ed.). Bogotá, Colombia: Ediciones de la U. Obtenido de https://corladancash.com/wp-content/uploads/2020/01/Metodologia-de-la-inv-cuanti-y-cuali-Humberto-Naupas-Paitan.pdf

Casas, A. J., Repullo, L. J., & Donado, C. J. (Mayo de 2003). La encuesta como técnica de investigación. Elaboración de cuestionarios y tratamiento estadístico de los datos (I). *Atención Primaria Práctica, 31*(8), 527-538. Obtenido de https://www.elsevier.es/es-revista-atencion-primaria-27-articulo-la-encuesta-como-tecnica-investigacion--13047738#:~:text=Se%20puede%20definir%20la%20encuesta,del%20que%20se%20pretende%20explorar%2C

Morlote, S., & Celiseo, S. (2004). *Metodología de la Investigación. Cuaderno de trabajo.* México D.F.: Cengage Learning.

Caballero, R. A. (2014). *Metodología integral innovadora para planes y tesis. La metodología del cómo formularlos.* México D.F.: Cengage Learning.

QuestionPro. (10 de agosto de 2018). *¿Qué es el muestreo por conveniencia?* Obtenido de QuestionPro: https://www.questionpro.com/blog/es/muestreo-por-conveniencia/

ANEXOS

Anexo 2. Matriz de operacionalización de variables

Variables de estudio	Dimensiones	Indicadores	Items	Escala de medición
Análisis de los delitos informáticos **(V1)**	Regulación normativa	– Legislación para tratar los delitos informáticos	*1,2*	Ordinal – Likert Totalmente en desacuerdo (5) En desacuerdo (4) Ni de acuerdo, ni en desacuerdo (3) De acuerdo (2) Totalmente de acuerdo (1)
		– Regulación jurídica de sanciones para los infractores	*3,4*	
	Eficacia en el cumplimiento	– Atención a las víctimas	*5,6*	
		– Celeridad en los procesos	*7,8*	
		– Sanciones a los infractores	*9,10*	
		– Número de denuncias archivadas	*11,12*	
	Reincidencia	– Causales de reincidencia	*13,14*	
		– Acciones tomadas contra los reincidentes	*15,16*	
Valor probatorio de la evidencia digital **(V2)**	Bien jurídico protegido	– El dato	*17,18*	Ordinal – Likert Totalmente en desacuerdo (5) En desacuerdo (4) Ni de acuerdo, ni en desacuerdo (3) De acuerdo (2) Totalmente de acuerdo (1)
	Previsión	– Previsión en la etapa procesal	*19,20*	
	Sanciones	– Sanción a ilícitos tecnológicos – Falta de precisiones en el Código Penal	*21,22*	
	Legalidad	– Alcances de la Ley N° 30096 – Vacíos legales	*23,24*	
	Custodia	– Principio de la "mismidad" – Autenticidad de la evidencia – Integridad de la evidencia	*25,26*	
	Tratamiento	– Procedimientos seguidos – Conocimientos técnicos informáticos	*27,28*	
	Atención	– Cadena de custodia de la prueba digital	*29,30*	

Anexo 3. Instrumento de recolección de datos – Cuestionario

CUESTIONARIO

Objetivo: El siguiente cuestionario se ha elaborado con el objetivo principal de: Determinar la relación entre los delitos informáticos y el valor probatorio de la evidencia digital en la Corte Superior de Justicia de Lima – 2021.

Por ello, agradeceré a usted responder este breve y sencillo cuestionario, su aporte será muy importante para el logro del objetivo principal que persigue la presente investigación, por lo que a continuación encontrará una serie de preguntas las cuales deberá leer y asignarle una respuesta de acuerdo a la siguiente escala de calificación:

TD = Totalmente en desacuerdo (1) **ED =** En desacuerdo (2) **I =** Indeciso (3)

DA = De acuerdo (4) **TA =** Totalmente de acuerdo (5)

Instrucciones:

Deberá marcar con una "X" la opción que mejor describa o más se adecúe al criterio de su respuesta, únicamente puede marcar una opción por respuesta. Las respuestas serán de uso confidencial, anónimo y acumulativo; por lo que agradeceremos a los participantes proporcionar información veraz acerca de los tópicos en consulta, sólo así serán realmente útiles para la presente investigación.

PREGUNTAS		ESCALA				
Variable 1: Análisis de los delitos informáticos		**1**	**2**	**3**	**4**	**5**
Dimensión 1: Regulación normativa						
1	¿Considera usted que nuestro actual ordenamiento jurídico cuenta con una efectiva legislación para tratar los delitos informáticos?					
2	¿Considera usted que la legislación para tratar los delitos informáticos en nuestro país, se encuentra debidamente alineada con tratados y convenios internacionales para combatir la ciberdelincuencia?					
3	¿Considera usted adecuada la regulación jurídica de sanciones para los infractores en los delitos informáticos?					
4	¿Considera usted que la regulación jurídica de sanciones para los infractores se encuentra debidamente alineada con nuestra realidad?					
Dimensión 2: Eficacia en el cumplimiento						
5	¿Considera usted que el Estado provee una atención oportuna y eficiente a las víctimas de delitos informáticos?					
6	¿Considera usted que la falta de atención a las víctimas obedece en gran medida a la carencia de mecanismos de supervisión y seguimiento de los casos que acontecen?					
7	¿Considera usted que existe celeridad en los procesos llevados a cabo por los operadores de justicia frente a la comisión de delitos informáticos?					
8	¿Considera usted la celeridad en los procesos por delitos informáticos se ve limitada en gran medida por los vacíos legales existentes en el ordenamiento jurídico peruano en torno a los delitos acontecidos en el ciberespacio?					

9	¿Considera usted que las sanciones a los infractores por delitos informáticos se encuentran contenidos en un dispositivo legal específico?					
10	¿Considera usted que las sanciones a los infractores por delitos informáticos se encuentran debidamente alineadas con el principio de proporcionalidad frente al delito que se le imputa?					
11	¿Considera usted que el número de denuncias archivadas responde a que carecen de fundamento jurídico-legal para iniciar un proceso judicial?					
12	¿Considera usted que el número de denuncias archivadas responden a falta de elementos probatorios que cuenten con el valor probatorio necesario para ser considerado relevante para un proceso judicial?					
Dimensión 3: Reincidencia						
13	¿Considera usted que las causales de reincidencia en los delitos informáticos responden en gran medida a la limitada regulación de estos delitos en nuestro actual ordenamiento jurídico-legal?					
14	¿Considera usted que las causales de reincidencia obedecen en gran medida a la falta de dispositivos legales que promuevan la supervisión y el control recurrente de las operaciones en el ciberespacio?					
15	¿Considera usted suficientemente severas las acciones tomadas contra los reincidentes como medida para reducir los índices de reincidencia de delitos informáticos?					
16	¿Considera usted que las acciones tomadas contra los reincidentes cuentan con el suficiente respaldo legal que permita ejercer la acción penal contra los imputados?					
Variable 2: Valor probatorio de la evidencia digital						
Dimensión 1: Bien jurídico protegido						
17	¿Considera usted que el dato es el bien jurídico protegido en los delitos informáticos?					
18	¿Considera usted que el dato como bien jurídico protegido en los delitos informáticos se encuentra debidamente respaldado desde el punto de vista normativo-legal?					
Dimensión 2: Previsión						
19	¿Considera usted que la evidencia digital es considerada como un elemento de previsión en la etapa procesal?					
20	¿Considera usted que la previsión en la etapa procesal permite otorgar un valor probatorio a la evidencia digital dentro de un proceso por delitos informáticos?					
Dimensión 3: Sanciones						
21	¿Considera usted que se encuentra debidamente regulada en nuestro marco normativo la sanción a ilícitos tecnológicos?					
22	¿Considera usted que faltan precisiones en el Código Penal acerca de las sanciones por concepto de ilícitos tecnológicos?					
Dimensión 4: Legalidad						

23	¿Considera usted que en los alcances de la Ley Nº 30096 se encuentra debidamente estipulado los requerimientos de legalidad que debe tener la evidencia digital para ser admitida como elemento probatorio dentro de un proceso?					
24	¿Considera usted que la legalidad de la evidencia digital se ve limitada por los vacíos legales que presenta el marco legal que regula los delitos informáticos en nuestro país?					
Dimensión 5: Custodia						
25	¿Considera usted que en el marco legal existente en torno a delitos informáticos se encuentra debidamente regulado los procedimientos que garanticen la autenticidad de la evidencia?					
26	¿Considera usted que sólo desde el aspecto legal se pretenda asegurar la integridad de la evidencia, con el propósito de ser admitida como parte de un proceso seguido por delitos informáticos?					
Dimensión 6: Tratamiento						
27	¿Considera usted que la no admisibilidad de la evidencia digital en los procesos judiciales por delitos informáticos obedece en gran medida a deficiencias en los procedimientos seguidos en su tratamiento?					
28	¿Considera que existen los dispositivos legales adecuados que permitan garantizar un adecuado tratamiento de la evidencia digital, a fin de ser admitido como parte de un proceso seguido por delitos informáticos?					
Dimensión 7: Atención						
29	¿Considera usted que la cadena de custodia de la prueba digital se muestra como un proceso eficiente?					
30	¿Considera usted que deficiencias en la cadena de custodia de la prueba digital representan el mayor escollo al momento de otorgar valor probatorio a la evidencia digital por parte de los operadores de justicia?					

GRACIAS POR SU COLABORACIÓN.

Bach. Víctor **ESPINOZA PRADO**

Anexo 4. Validación de expertos

UNIVERSIDAD CÉSAR VALLEJO

FICHA DE VALIDACIÓN

INFORME DE OPINIÓN DEL JUICIO DE EXPERTOS

I. DATOS GENERALES:

1.1. Título de investigación: "ANÁLISIS DE LOS DELITOS INFORMÁTICOS Y EL VALOR PROBATORIO DE LAEVIDENCIA DIGITAL EN LA CORTE SUPERIOR DE JUSTICIA DE LIMA - 2021"

1.2. Apellidos y nombres: Mg Yanira Guisella Lázaro Ortiz.

1.3. Cargo e institución donde labora: Docente de la UCV

1.4. Nombre del instrumento motivo de evaluación: Cuestionario

1.5. Autor del instrumento: Bach. Víctor ESPINOZA PRADO

II. ASPECTOS DE VALIDACIÓN

CRITERIOS	INDICADORES	INACEPTABLE						MINIMAMENTE ACEPTABLE			ACEPTABLE			Σ
		40	45	50	55	60	65	70	76	80	85	90	95	100
1. CLARIDAD	Esta formulado con lenguaje comprensible.											X		
2. OBJETIVIDAD	Esta adecuado a las leyes y principios científicos.											X		
3. ACTUALIDAD	Este adecuado a los objetivos y las necesidades reales de la Investigación.											X		
4. ORGANIZACIÓN	Existe una organización lógica.											X		
5. SUFICIENCIA	Toma en cuenta los aspectos metodológicos esenciales											X		
6. INTENCIONALIDAD	Esta adecuado para valorar o medir las variables.											X		
7. CONSISTENCIA	Se respalda en fundamentos técnicos y/o científicos.											X		
8. COHERENCIA	Existe coherencia entre los problemas, objetivos, e hipótesis											X		
9. METODOLOGÍA	La estrategia responde una metodología y diseño aplicados para lograr verificar las hipótesis.											X		
10. PERTINENCIA	El instrumento muestra la relación entre los componentes de la investigación y su adecuación al Método Científico.											X		

III. OPINIÓN DE APLICABILIDAD

- El Instrumento cumple con los requisitos para su aplicación.
- El Instrumento no cumple con los requisitos para su aplicación

PROMEDIO DE VALORACIÓN

SI
...90 %

Lima, 27 de enero del 2022

Firma del experto
DNI N° 45189824 Cel. 986 593 151

UNIVERSIDAD CÉSAR VALLEJO

FICHA DE VALIDACIÓN

INFORME DE OPINIÓN DEL JUICIO DE EXPERTOS

I. DATOS GENERALES:

1.1. **Título de investigación: "ANÁLISIS DE LOS DELITOS INFORMÁTICOS Y EL VALOR PROBATORIO DE LAEVIDENCIA DIGITAL EN LA CORTE SUPERIOR DE JUSTICIA DE LIMA - 2021"**

1.2. **Apellidos y nombres**: Mg Liliam Lesly Castro Rodríguez.

1.3. **Cargo e institución donde labora**: Docente de la UCV

1.4. **Nombre del instrumento motivo de evaluación:** Cuestionario

1.5. **Autor del instrumento:** Bach. Victor ESPINOZA PRADO

II. ASPECTOS DE VALIDACIÓN

CRITERIOS	INDICADORES	INACEPTABLE						MINIMAMENTE ACEPTABLE			ACEPTABLE			Σ
		40	45	50	55	60	65	70	76	80	85	90	95	100
1. CLARIDAD	Esta formulado con lenguaje comprensible.										X			
2. OBJETIVIDAD	Esta adecuado a las leyes y principios científicos.										X			
3. ACTUALIDAD	Este adecuado a los objetivos y las necesidades reales de la Investigación.										X			
4. ORGANIZACIÓN	Existe una organización lógica.										X			
5. SUFICIENCIA	Toma en cuenta los aspectos metodológicos esenciales										X			
6. INTENCIONALIDAD	Esta adecuado para valorar o medir las variables.										X			
7. CONSISTENCIA	Se respalda en fundamentos técnicos y/o científicos.										X			
8. COHERENCIA	Existe coherencia entre los problemas, objetivos, e hipótesis										X			
9. METODOLOGÍA	La estrategia responde una metodología y diseño aplicados para lograr verificar las hipótesis.										X			
10. PERTINENCIA	El instrumento muestra la relación entre los componentes de la investigación y su adecuación al Método Científico.										X			

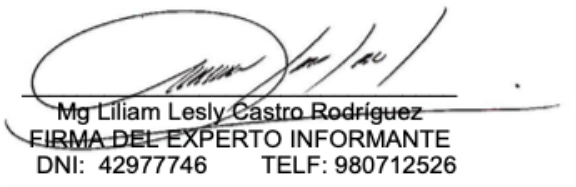
III. OPINIÓN DE APLICABILIDAD

- El Instrumento cumple con los requisitos para su aplicación.
- El Instrumento no cumple con los requisitos para su aplicación

PROMEDIO DE VALORACIÓN

SI
...85 %

Lima, 27 de enero del 2022



Mg Liliam Lesly Castro Rodríguez
FIRMA DEL EXPERTO INFORMANTE
DNI: 42977746 TELF: 980712526

Anexo 5. Matriz de consistencia

PROBLEMA	OBJETIVO	HIPÓTESIS	VARIABLES	METODOLOGÍA
Problema general ¿Cuál es la relación entre los delitos informáticos y el valor probatorio de la evidencia digital en la Corte Superior de Justicia de Lima – 2021?. **Problemas específicos** ¿Cuál es la relación entre los delitos informáticos y el bien juridico protegido de la evidencia digital en la Corte Superior de Justicia de Lima - 2021? ¿Cuál es la relación entre los delitos informáticos y la previsión en la evidencia digital en la Corte Superior de Justicia de Lima - 2021? ¿Cuál es la relación entre los delitos informáticos y las sanciones de la evidencia digital en la Corte Superior de Justicia de Lima - 2021? ¿Cuál es la relación entre los delitos informáticos y la legalidad de la evidencia digital en la Corte Superior de Justicia de Lima - 2021? ¿Cuál es la relación entre los delitos informáticos y la custodia de la	**Objetivo general** Determinar la relación entre los delitos informáticos y el valor probatorio de la evidencia digital en la Corte Superior de Justicia de Lima – 2021. **Objetivos específicos** Determinar la relación entre los delitos informáticos y el bien juridico protegido de la evidencia digital en la Corte Superior de Justicia de Lima - 2021. Determinar la relación entre los delitos informáticos y la previsión en la evidencia digital en la Corte Superior de Justicia de Lima - 2021. Determinar la relación entre los delitos informáticos y las sanciones de la evidencia digital en la Corte Superior de Justicia de Lima - 2021. Determinar la relación entre los delitos informáticos y la legalidad de la evidencia digital en la Corte Superior de Justicia de Lima - 2021.	**Hipótesis general** Los delitos informáticos se relacionan significativamente con el valor probatorio de la evidencia digital en la Corte Superior de Justicia de Lima – 2021. **Hipótesis específicas** Los delitos informáticos se relacionan siginificativamente con el bien juridico protegido de la evidencia digital en la Corte Superior de Justicia de Lima - 2021. Los delitos informáticos se relacionan significativamente con la previsión en la evidencia digital en la Corte Superior de Justicia de Lima - 2021. Los delitos informáticos se relacionan significativamente con las sanciones de la evidencia digital en la Corte Superior de Justicia de Lima - 2021. Los delitos informáticos se relacionan significativamente con la legalidad de la evidencia digital	**VARIABLE 1** Análisis de los delitos informáticos **VARIABLE 2** Valor probatorio de la evidencia digital	**Tipo:** Básica. **Diseño:** No experimental - transversal - correlacional. **Población:** 37 individuos. **Muestreo:** No probabilístico por conveniencia. **Técnica e instrumento de recolección de datos:** Encuesta - Cuestionario. **Validación:** Juicio de expertos.

evidencia digital en la Corte Superior de Justicia de Lima - 2021? ¿Cuál es la relación entre los delitos informáticos y el tratamiento de la evidencia digital en la Corte Superior de Justicia de Lima - 2021? ¿Cuál es la relación entre los delitos informáticos y la atención de la evidencia digital en la Corte Superior de Justicia de Lima - 2021?.	Determinar la relación entre los delitos informáticos y la custodia de la evidencia digital en la Corte Superior de Justicia de Lima - 2021. Determinar la relación entre los delitos informáticos y el tratamiento de la evidencia digital en la Corte Superior de Justicia de Lima - 2021. Determinar la relación entre los delitos informáticos y la atención de la evidencia digital en la Corte Superior de Justicia de Lima - 2021.	en la Corte Superior de Justicia de Lima - 2021. Los delitos informáticos se relacionan significativamente con la custodia de la evidencia digital en la Corte Superior de Justicia de Lima - 2021. Los delitos informáticos se relacionan significativamente con el tratamiento de la evidencia digital en la Corte Superior de Justicia de Lima - 2021. Los delitos informáticos se relacionan significativamente con la atención de la evidencia digital en la Corte Superior de Justicia de Lima - 2021.

Anexo 6. Base de datos de la encuesta sobre la variable 1 “ANÁLISIS DE LOS DELITOS INFORMÁTICOS”

VARIABLE 1: ANÁLISIS DE LOS DELITOS INFORMÁTICOS																
Nº	Dimensión 1: Regulación normativa				Dimensión 2: Eficacia en el cumplimiento								Dimensión 3: Reincidencia			
	preg.1	preg.2	preg.3	preg.4	preg.5	preg.6	preg.7	preg.8	preg.9	preg.10	preg.11	preg.12	preg.13	preg.14	preg.15	preg.16
1	4	4	5	5	5	5	5	5	5	4	5	4	4	4	5	5
2	4	4	4	4	3	4	3	2	3	4	4	4	4	4	4	5
3	1	1	1	1	1	4	1	5	5	1	1	1	1	1	1	1
4	2	4	1	1	1	5	1	5	4	1	2	5	4	5	1	1
5	2	2	2	2	2	4	2	3	4	2	4	4	4	4	2	2
6	4	4	2	2	2	4	2	4	4	2	4	4	4	4	2	4
7	2	4	2	2	2	4	2	4	2	2	5	4	4	4	2	2
8	2	3	2	1	1	4	1	3	2	2	4	5	4	4	1	1
9	3	1	2	2	2	4	2	4	2	2	4	4	5	4	2	2
10	4	2	2	2	2	4	2	4	2	2	4	4	4	4	2	2
11	1	4	1	2	1	2	2	1	4	4	1	4	1	5	2	2
12	2	1	4	4	2	5	2	4	4	2	4	4	4	4	2	2
13	4	3	2	2	2	2	2	4	4	4	4	4	4	4	2	2
14	1	1	2	2	1	4	2	2	4	1	2	3	2	5	1	1
15	1	1	1	1	1	5	1	5	1	1	5	5	5	5	1	1
16	2	2	1	2	2	2	2	2	2	2	5	5	5	5	5	5
17	5	5	5	1	5	5	1	5	4	1	5	5	5	5	1	1
18	1	1	1	1	1	5	1	1	5	1	5	5	5	5	1	1
19	4	4	4	4	1	5	2	4	4	4	2	2	4	5	1	1
20	2	4	1	1	1	5	1	5	5	1	5	5	5	5	1	1
21	4	4	2	2	2	4	2	4	4	2	4	4	4	4	2	2
22	2	2	3	2	2	3	2	4	4	3	4	4	4	4	2	4
23	2	2	2	2	1	1	1	4	2	1	2	4	4	4	2	2
24	2	2	2	2	2	4	1	4	4	2	2	5	4	4	2	2
25	4	4	4	4	4	4	4	4	4	4	4	5	4	5	4	4
26	3	4	3	2	3	3	3	4	4	4	2	2	3	4	3	4
27	2	2	2	2	2	4	2	4	2	2	4	4	4	4	2	2
28	2	3	3	2	1	5	3	3	3	3	4	4	4	4	3	5
29	2	3	2	2	2	4	2	4	2	2	4	4	4	4	3	2
30	2	4	1	1	1	5	1	5	1	1	3	5	3	3	3	3
31	2	2	2	2	2	2	2	4	5	2	4	4	4	4	2	2
32	4	4	2	2	2	4	4	4	2	2	4	4	4	4	2	2
33	3	3	4	4	4	4	2	4	2	2	2	2	3	3	3	3
34	2	2	2	2	2	4	1	4	4	4	4	4	4	4	4	4
35	4	4	2	1	1	5	2	5	4	2	5	5	5	5	5	2
36	5	4	4	4	4	2	4	5	5	5	2	4	4	4	4	4
37	1	2	1	1	1	1	1	1	1	1	2	1	1	1	1	1

Anexo 7. Base de datos de la encuesta sobre la variable 2 “VALOR PROBATORIO DE LA EVIDENCIA DIGITAL”

VARIABLE 2: VALOR PROBATORIO DE LA EVIDENCIA DIGITAL														
Nº	Dimensión 1		Dimensión 2		Dimensión 3		Dimensión 4		Dimensión 5		Dimensión 6		Dimensión 7	
	preg.17	preg.18	preg.19	preg.20	preg.21	preg.22	preg.23	preg.24	preg.25	preg.26	preg.27	preg.28	preg.29	preg.30
1	4	4	5	4	3	5	4	4	4	4	4	4	5	5
2	4	4	4	4	4	4	4	4	4	4	4	4	4	4
3	5	5	5	5	1	5	1	5	1	5	5	5	1	5
4	4	2	4	2	2	5	2	4	2	4	5	2	2	4
5	4	2	4	4	2	4	2	4	2	2	4	2	4	4
6	4	4	4	4	4	4	3	4	2	3	4	4	3	4
7	4	2	4	4	2	4	2	4	2	4	4	2	2	4
8	4	1	2	3	2	4	1	4	2	3	2	2	2	2
9	2	2	4	4	2	1	3	5	2	2	2	2	3	2
10	4	2	2	2	2	4	2	4	4	4	4	4	4	4
11	4	2	1	4	2	5	2	4	1	4	2	5	4	5
12	4	4	4	4	2	4	2	4	4	2	4	4	4	4
13	3	4	3	4	4	2	2	4	4	4	4	4	4	4
14	1	2	3	2	2	4	5	4	4	2	4	4	4	1
15	4	1	5	5	1	5	1	5	1	1	5	5	1	5
16	2	2	4	1	2	5	2	2	4	4	5	5	1	5
17	5	1	4	1	1	5	1	5	1	1	5	1	1	5
18	5	5	5	5	1	5	1	5	1	5	5	1	5	5
19	5	4	3	4	4	4	2	4	2	2	2	4	2	4
20	2	2	5	5	2	1	2	5	1	4	4	4	2	4
21	4	4	4	4	4	4	4	4	4	4	4	4	4	4
22	4	2	3	4	4	2	3	4	2	2	4	3	4	4
23	4	2	2	2	2	4	2	4	2	4	4	2	2	4
24	4	2	4	4	2	4	4	4	4	4	4	2	2	4
25	4	4	5	4	4	4	4	4	4	4	4	4	2	4
26	4	3	4	4	3	4	3	4	2	4	4	2	2	4
27	2	2	2	4	2	4	2	4	2	2	4	2	2	4
28	3	3	4	3	3	3	3	3	3	3	3	3	3	3
29	4	2	4	2	2	4	2	4	2	1	3	2	2	5
30	5	2	5	3	1	5	3	5	1	1	3	1	1	3
31	4	2	2	4	2	5	2	4	2	4	4	2	2	4
32	4	2	4	4	2	4	2	4	2	4	4	2	2	4
33	4	4	4	4	4	4	4	4	4	4	4	4	4	4
34	4	2	4	4	4	4	4	4	2	4	2	2	2	4
35	5	2	5	4	1	5	2	5	4	4	5	4	5	5
36	4	4	3	4	5	4	4	2	4	4	2	4	4	2
37	1	1	2	1	1	1	1	1	1	1	1	1	1	1