UNIVERSIDAD NACIONAL HERMILIO VALDIZÁN

ESCUELA DE POSGRADO

DERECHO, MENCIÓN EN CIENCIAS

PENALES

COMPETENCIAS EN CIBERSEGURIDAD DEL OPERADOR JURÍDICO Y LA INVESTIGACIÓN PENAL DE CIBERDELITOS EN EL DISTRITO FISCAL DE HUÁNUCO DURANTE EL PERIODO 2020

LÍNEA DE INVESTIGACIÓN: DERECHO

TESIS PARA OPTAR EL GRADO DE MAESTRO EN DERECHO,

MENCIÓN EN CIENCIAS PENALES

TESISTA: VILCA MORALES LEONARDO EDGARD

ASESOR: DR. NAJAR FARRO CESAR ALFONSO

HUÁNUCO – PERÚ

2022

DEDICATORIA

Dedico esta tesis a mi madre Marilú Morales Calderón, quien con su incesante apoyo y motivación hizo posible el poder culminar satisfactoriamente este trabajo de investigación, con el cual doy un nuevo paso trascendental en mi formación académica y profesional.

AGRADECIMIENTO

Agradezco a Dios por acompañar, iluminar y bendecir cada paso en mi vida, a mi familia y a todos mis seres queridos que de alguna forma me motivan a crecer más cada día, agradezco también de forma especial a mi asesor el Dr. Cesar Alfonso Najar Farro por su valiosa guía y asesoramiento a lo largo de todos estos años.

RESUMEN

La presente investigación, se abocó en el estudio de las competencias en ciberseguridad del operador jurídico y la investigación penal de ciberdelitos en el distrito fiscal de Huánuco en el año 2020, en ese sentido, en su primer capítulo se planteó como objetivo principal determinar la relación que existe entre las variables, para lo cual se formularon cuatro objetivos específicos.

El segundo capítulo, se precisó la hipótesis general y específicas, las mismas que al tener que corroborarse estadísticamente, contaron cada una con una hipótesis alternativa y nula; asimismo partiendo de las variables y su correspondiente operacionalización, se hallaron siete dimensiones y veintisiete indicadores.

Respecto al marco teórico que sustenta esta investigación, fue abordado en el tercer capítulo, para tal efecto se presentó los antecedentes encontrados organizados en internacionales, nacionales y locales, para en seguida abordarse el teóricamente las variables de estudio.

En el cuarto capítulo, se explicó el marco metodológico, precisándose que es una investigación básica de nivel explicativo, cuyo ámbito fue el distrito fiscal de Huánuco, con una población conformada por los operadores jurídicos, asimismo, se calculó una muestra probabilística compuesta por tres subgrupos: abogados, jueces y fiscales; se precisó que la investigación posee un diseño transeccional, cuya técnica utilizada fue la encuesta, elaborándose un instrumento validado por expertos, y también se precisó lo concerniente al procesamiento y análisis de datos.

En el quinto capítulo, se realizó un análisis descriptivo de los datos recabados mediante representaciones gráficas, para en seguida realizar la contrastación de las hipótesis, utilizándose el coeficiente de correlación de Spearman, hallándose que la correlación entre las variables de estudio si existiría, ello pese a que una tres las cuatro hipótesis específicas no mostró algún grado de correlación, por tanto, en base a estos resultados se afirma que se cumplió con el objetivo planteado en este estudio.

Palabras clave: Ciberseguridad, investigación penal, ciberdelitos, operador jurídico.

ABSTRACT

The present research focused on the study of the cybersecurity competencies of the legal operator and the criminal investigation of cybercrimes in the fiscal district of Huánuco in the year 2020, in this sense, in its first chapter the main objective was to determine the relationship that exists between the variables, for which four specific objectives were formulated.

The second chapter, the general and specific hypotheses were specified, the same ones that, having to be statistically corroborated, each had an alternative and null hypothesis; Likewise, starting from the variables and their corresponding operationalization, seven dimensions and twenty-seven indicators were found.

Regarding the theoretical framework that supports this research, it was addressed in the third chapter, for this purpose the antecedents found organized in international, national and local were presented, to then theoretically address the study variables.

In the fourth chapter, the methodological framework was explained, specifying that it is a basic investigation of an explanatory level, whose scope was the fiscal district of Huánuco, with a population made up of legal operators, likewise, a probabilistic sample composed of three subgroups was calculated. : lawyers, judges and prosecutors; It was specified that the research has a cross-sectional design, whose technique was the survey, developing an instrument validated by experts, and it was also specified what concerns data processing and analysis.

In the fifth chapter, a descriptive analysis of the data collected through graphic representations was carried out, to immediately carry out the contrasting of the hypotheses, using the Spearman correlation coefficient, finding that the correlation between the study variables would exist, despite this. to the fact that one of the four specific hypotheses did not show some degree of correlation, therefore, based on these results, it is affirmed that the objective set out in this study was met.

Keywords: Cybersecurity, criminal investigation, cybercrime, legal operator

ÍNDICE

INTRODUCCIÓN

En la actualidad mucho se habla acerca del peligro que representan los ciberdelitos, en especial cuando se considera su complejidad técnica, o como menciona Acurio (2020, p. 9), el que tengan esa cualidad transfronteriza, catalogándose al problema de la ciberdelincuencia como un asunto de interés internacional, por el cual muchos países, teniendo en cuenta su peligrosidad, emprenden acciones a fin de confrontar dicho problema, las mismas que al día de hoy son objeto de evaluación, como ocurre con el Modelo de Madurez de la Capacidad de Ciberseguridad para las Naciones elaborado por el Centro Global de Capacidad en Seguridad Cibernética de la Universidad de Oxford (2020, p. 42), el cual aplicado a paises alrededor del mundo, nos permite comprender en que situación se encuentran los paises en materia de ciberdelincuencia y ciberseguridad. Por ello, el Perú no es ajeno al problema de la ciberdelincuencia, y con mayor frecuencia se aborda dicho problema desde el plano gubernamental, lo cual contrasta mucho con lo que ocurría hace unos años , en los cuales se veía poco relevante, por este motivo, podemos repasar que en el plano jurídico los primeros pasos serios para su abordaje se pueden considerar desde la promulgación de la Ley 30086 Ley de Delitos Informáticos, la creación de la División de Investigación de Delitos de Alta Tecnología de la Policía Nacional del Perú, la suscripción del Convenio de Budapest (Andina, 2019) y más recientemente la creación de Unidad Fiscal Especializada en Ciberdelincuencia del Ministerio Público (El Peruano, 2020), lo cual en suma debería permitir que los casos de ciberdelitos puedan ser investigados adecuadamente dentro de un proceso penal, en el cual existan mecanismos que permitan desarrollar investigaciones eficaces que esclarezcan los hechos y se puedan hallar responsabilidades.

De otro lado, si nos centramos en el proceso penal peruano, encontraremos que en la etapa de investigación preparatoria (e investigación preliminar) en la cual se investiga la comisión de los delitos (Ministerio Público, 2020) y por ende los ciberdelitos, que como en cualquier otro delito, se requerirá del apoyo por parte de la Policía, y la participación de peritos y personal especializado, a fin de practicar las diligencias que el Ministerio Público estime pertinentes. Es en este el contexto en el

cual se desenvuelven los operadores jurídicos, los mismos que conforme nos explica Vilca (2018, pág. 162) deben demostrar ser competentes en informática básica, derecho informático e informática jurídica. No obstante, en el ciberespacio se sabe que existen toda clase de riesgos, los mismos que también puede llegar afectar en alguna forma la investigación de los ciberdelitos, por ello se aborda el campo de la seguridad informática y por ende el de la ciberseguridad.

Por lo expuesto, se deduce que en la actualidad el operador jurídico tiene sobre sí la exigencia de adquirir y dominar competencias profesionales en informática que le permitan comprender el fenómeno de la cibercriminalidad y los ciberdelitos, tanto más si participa en su investigación, no obstante y como se ha mencionado, la informática viene acompañada de riesgos que deben ser afrontados a fin de evitar perjuicios que demoren una investigación o más la frustren, por tanto aunado a las competencias mencionadas se entiende que estas deberían de incluir también las relacionadas a la ciberseguridad, rama especializada de la informática, que desde un enfoque práctico aborda los incidentes informáticos para su respectivo tratamiento, en consecuencia la interrogante principal de este estudio es hallar si existe relación entre dichas competencias y la investigación de ciberdelitos.

CAPÍTULO I. ASPECTOS BÁSICOS DEL PROBLEMA DE INVESTIGACIÓN

1.1 Fundamentación del Problema

Cuando se analiza la sociedad humana actual, resulta ineludible hacer referencia a los avances tecnológicos alcanzados, y por ende reflexionar sobre la influencia que ha tenido la ciencia informática, cuyo desarrollo y aplicación permitió un vertiginoso avance en los diversos campos del conocimiento en el último siglo, conforme se destaca en innumerables las publicaciones que se han hecho y se vienen haciendo acerca de sus ventajas alrededor del mundo, destacando principalmente su papel esencial para la creación de lo que hoy se conoce como INTERNET, llamada también como la red de redes, un sistema global interconectado con toda clase de redes informáticas que según cifras del Banco Mundial (2021), solo en 2017 accedían el 48,997 % de personas a nivel mundial, a través de más de 20.000 millones de dispositivos, conforme lo reportado por la OECD (como se cita en BID, 2020).

Reflexionar sobre el impacto de la ciencia informática no solo implica valorar sus ventajas sino también los peligros que su evolución conlleva, en ese sentido, su expansión en el mundo ha venido acompañada desde un principio con la aparición de riesgos, en donde el enfoque orientado al aprovechamiento de determinadas vulnerabilidades conllevó a la creación de los primeros "virus informáticos", los cuales a su vez dieron un visión de la potencial amenaza que representarían en el futuro, ejemplo de ello es el históricamente famoso programa informático "Creeper", considerado uno de los primeros en ser etiquetado como virus informático y que tuvo como mayor mérito el haber infectado ARPANET en la década de los años 70, una red de computadoras de uso militar de los Estados Unidos de América (Mozilla, 2021) de significativa importancia, siendo este evento el primero de una ola de eventos similares que se replicarán hasta la actualidad, los cuales tendrán como denominador común el vulnerar la información proveniente de personas, empresas u gobiernos alrededor del mundo, con impactos económicos variados, algunos de ellos multimillonarios y de impacto global, dándose así forma al fenómeno criminal de la ciberdelincuencia.

Por presentar algunas cifras, según un informe de la empresa McAfee (como se cita en Business Insider, 2020), solo en el año 2019 se calculó que las pérdidas económicas ocasionadas por la ciberdelincuencia representaban más de un billón de dólares, que en perspectiva correspondería a cerca del 1% del PIB (Producto Interno Bruto) mundial, asimismo, según el Registro de Direcciones de Internet de América Latina y Caribe (como se cita en OEA, 2020), en la región el costo económico de este fenómeno delictivo se calcula en 90.000 millones de dólares al año. De otro lado en cuanto al Perú, según la empresa Kaspersky (2021) se tiene una tendencia de crecimiento en los ciberataques (+71%), con 96 ataques por minuto aproximadamente, lo cual tiene concordancia con lo reportado por el Ministerio Público (Andina, 2021), que informó que hubo un incremento del 92.9% de denuncias por ciberdelitos en comparación con el año 2020.

En la ciencia informática, la existencia de riesgos y vulnerabilidades conllevó a que sea abordada desde el enfoque de la seguridad de la información, dando nacimiento a la ciberseguridad, disciplina que en términos muy generales se encarga de asegurar la información en el ciber espacio, ya sea mitigando los riesgos y amenazas o respondiendo de alguna manera a estos.

Desde el ámbito jurídico, la ciencia informática ha sido de especial interés en los últimos años, la creación del ciberespacio y la aparición de sus consiguientes riesgos y amenazas han sido motivo suficiente para que el derecho intervenga regulando los fenómenos jurídicos que se desarrollan en este espacio virtual a través del llamado derecho informático; de igual modo ha generado suficiente interés como para nutrirse de sus ventajas dando lugar a la informática jurídica, mediante la incorporación de innovaciones tecnológicas en las instituciones que conforman los diversos sistemas de administración de justicia en el mundo, y los cuales el operador jurídico toma un rol protagónico, al ser quien deberá conocer y utilizar dichas innovaciones para un eficiente desempeño profesional, por estos motivos, se advierte que a la actualidad, todas las ramas del derecho ya abordan en diferente forma y grado la ciencia informática y sus fenómenos.

Sin embargo, cuando nos ocupamos de los riesgos y amenazas del ciberespacio, probablemente ninguna otra rama del derecho abordará tanto este tema como el derecho penal, ya que es esta la rama jurídica en la cual se aborda el tema de los ciberdelitos o delitos informáticos, conductas delictuosas que evolucionan constantemente a la par de las grandes innovaciones tecnológicas, y que tanto en sus modalidades como en sus alcances requieren de normas que sean objeto de constante revisión y actualización, y que también desde el ámbito procesal penal requieren que se tome en consideración su complejidad y constante evolución, a efectos de que se implemente con prontitud innovaciones tecnológicas que por ejemplo favorezcan la investigación y el juzgamiento; bajo este razonamiento resulta entonces necesario que el operador jurídico cuente con competencias profesionales especiales orientadas tanto en derecho informático como en informática jurídica, no obstante, como se ha mencionado en párrafos anteriores, cualquiera sea el campo en que se aplique la informática, esta conlleva riesgos y amenazas, por consiguiente aunque el derecho se nutra de las innovaciones tecnológicas para la investigación de ciberdelitos, y los operadores dominen competencias profesionales en derecho informático e informática jurídica, emerge la duda si con ello es suficiente para mitigar las vulnerabilidades que conlleva la utilización de la informática, en especial cuando se trata del proceso penal (por abocarse a la investigación del ciberdelito), pues se entendería que aunado a lo mencionado, el operador jurídico debería contar también con conocimientos en ciberseguridad, una disciplina especializada de la ciencia informática que parecería guardar distancia del campo del derecho, sin embargo y como bien se desarrolla en esta disciplina, es innegable destacar la importancia que tienen las competencias en ciberseguridad en el personal que labora en organizaciones de cualquier índole, por cuanto se tiene evidencia que el error humano es una gran vulnerabilidad en materia de seguridad informática, un problema que no se soluciona solo con la implementación de herramientas y sistemas de seguridad (o la contratación de personal especializado), sino que se debe de abordarse desde el ámbito de la formación y capacitación del personal.

Por lo expuesto, en la presente investigación se aborda esta cuestión problemática desde el ámbito penal y procesal penal del derecho, pues se analizó si

este requerimiento de competencias profesionales en ciberseguridad del operador jurídico resultan importantes durante la investigación ciberdelitos, surgiendo de este tema la interrogante central de este trabajo de investigación, es decir, el saber cuál es la relación entre las competencias en ciberseguridad y la investigación penal de ciberdelitos, una pregunta relevante considerando la creciente carga de casos sobre ciberdelitos en el Perú.

1.2 Justificación e Importancia de la Investigación

Conforme lo describe Hernández et al (2014), la justificación de una investigación científica implica fundamentalmente indicar las razones por las cuales un determinado estudio debió de efectuarse; por consiguiente, para justificar la importancia y conveniencia de esta investigación se debió de seguir criterios claros que permitieran evaluar su utilidad, siendo que Hernández et al ya los proveyó a partir de una adaptación de los criterios propuestos en forma de preguntas por los autores Ackoff, Miller y Salkind, y que se enumeran a continuación con la fundamentación correspondiente:

a) **Conveniencia:** En cuanto a este primer criterio de evaluación, esta investigación resultó conveniente, debido al contexto en el cual se realizó el estudio, pues la pandemia del virus Covid-19 supuso la implementación y uso casi obligatorio de soluciones informáticas para confrontar los efectos negativos de la crisis sanitaria y económica, lo cual a su vez expuso con mayor notoriedad a la sociedad a los nuevos riesgos y amenazas que hay en el ciberespacio.
b) **Relevancia Social:** En cuanto a la trascendencia social de esta investigación, se tiene que esta beneficia, en gran medida, a la comunidad jurídica nivel nacional e a nivel internacional, pues los resultados aquí plasmados pueden llegar a motivar a que se tomen medidas más efectivas que permitan mitigar los efectos de los riesgos y amenazas que hay en el ciberespacio.
c) **Implicaciones prácticas:** En la actualidad, al existir una fuerte disyuntiva en cuanto a las competencias que requiere el profesional de hoy, el presente estudio responde a esta interrogante a través del planteamiento de que el profesional del

derecho requiere adquirir nuevas competencias en ciberseguridad que le permitan lidiar con la investigación de ciberdelitos.

d) **Valor teórico:** Aunque los temas abordados en esta investigación han sido desarrollados ampliamente en países extranjeros, como es el caso de la informática, la ciberseguridad o los ciberdelitos, no ha ocurrido lo mismo con el problema que aquí se aborda, pues son escasas las investigaciones que se ocupen del estudio de la correlación que tendría la ciberseguridad con la investigación de ciberdelitos, por ello, esta investigación se propuso ayudar a abordar esta carencia, a efectos de que la información que aquí se comparte sirviera para el desarrollo de nuevos estudios e incluso sirviera de base para formulación de nuevas teorías.

e) **Utilidad Metodológica:** En el presente estudio, no se contó con algún instrumento estandarizado para estudiar la correlación de las variables de estudio, por tanto, ha sido necesario diseñar un instrumento que sirviera al propósito del estudio, el cual, es factible de ser perfeccionado por otros investigadores para analizar sus datos en la medida que les sea útil.

Tal y como menciona Hernández et al (2014), es muy difícil que una investigación pueda cumplir de manera positiva con todos estos criterios, sin embargo, el investigador confía en que estos han quedado satisfechos en la medida de lo posible, pues el presente estudio ha buscado abordar un problema de actualidad respondiendo a su vez a una necesidad académica y social que destaca aún más su importancia, no solo en el ámbito jurídico, sino en el de la investigación en general, ello considerándose que una investigación puede llegar alcanzar la trascendencia suficiente aún si solo cumpliera uno de los criterios aquí expuestos.

1.3 Viabilidad de la Investigación

Conforme explica Hernández et al et al (2014), la viabilidad o factibilidad de un estudio, implica tomar en cuenta la disponibilidad de tiempo, recursos financieros, humanos y materiales que ayudaron a determinar los alcances que tendrá una investigación (p. 41), es así que para el presente estudio, se contó en primer lugar con la disponibilidad de tiempo, pues el investigador tuvo que programar cada una de las etapas, en cuanto a los recursos financieros se contó con el presupuesto necesario, el

cual se vio favorecido con el uso de las TIC's, en donde herramientas de software profesional permitieron una recolección eficiente y confiable de los datos, asimismo ligado a este último punto, no hubo necesidad de contar con un potencial humano amplio pues la actual tecnología permite ordenar y sistematizar los datos de forma automática sin la necesidad de que la operen muchas personas; finalmente en cuanto a los recurso materiales, son contó con todas las herramientas de hardware requeridas para realizar la investigación durante toda su ejecución.

1.4 Formulación del Problema

De acuerdo con Carrasco (2007) la formulación del problema en una investigación científica consiste en expresar el problema mediante una fórmula interrogativa, el cual debe tener un sustento teórico y empírico para el posterior tratamiento metodológico, siendo que además dicho problema debe ser redactado de forma clara y precisa (p. 99).

1.4.1 Problema General

De acuerdo a Carrasco (2007, pág. 106) el problema general expresa la motivación total que indujo al investigador a realizar su labor probatoria, es decir contrastar la hipótesis, lo cual agrega debe ser formulado considerando el tipo y diseño de la investigación; en consecuencia, para el presente estudio el problema general fue generado relacionando las dos variables, como son las competencias en ciberseguridad y la investigación penal de ciberdelitos, formulándose el siguiente problema:

PG. ¿Cuál es la relación de las competencias en ciberseguridad del operador jurídico y la investigación penal de ciberdelitos en el distrito fiscal de Huánuco durante el periodo 2020?

1.4.2 Problemas Específicos

En esencia, los problemas específicos en una investigación se derivan de los problemas generales, que como menciona Carrasco (2007, pág. 108) se realiza siguiendo un procedimiento metodológico, el cual para el presente estudio consistió en elaborar un cuadro de variables e indicadores que permitiera elaborar problemas

específicos correlaciones (en razón a la tipología correlacional del problema general), lo cual se detallará más adelante. A continuación, se presenta los problemas específicos formulados:

PE1. ¿Cuál es la relación entre el reconocimiento de tecnologías para la seguridad de la información por el operador jurídico y la investigación penal de ciberdelitos?

PE2. ¿Cuál es la relación entre la aplicación de procedimientos para la seguridad de la información en el ciberespacio por el operador jurídico y la investigación penal de ciberdelitos?

PE3. ¿Cuál es la relación entre la identificación de incidentes de seguridad de la información en el ciberespacio por el operador jurídico y la investigación penal de ciberdelitos?

PE4. ¿Cuál es la relación entre la respuesta a incidentes de seguridad de la información en el ciberespacio por el operador jurídico y la investigación penal de ciberdelitos?

1.5 Formulación de Objetivos

Para Carrasco (2007) los objetivos de una investigación son: "(…) los propósitos esenciales que se van a lograr como consecuencia del desarrollo del trabajo de investigación" (p. 159), agregando que estos se formulan en virtud del diseño de la investigación, asimismo, y conforme indica Hernández et al (2014, p. 37) se deben expresar con claridad, pues son las guías de estudio.

1.5.1 Objetivo General

Para la presente investigación, y en concordancia con lo explicado por Carrasco (2007, pág. 161), se generó el objetivo general considerando las variables de estudio, y relacionando la variable independiente con la variable dependiente, formulándose el siguiente objetivo general:

OG. Determinar la relación entre las competencias en ciberseguridad del operador jurídico y la investigación penal de ciberdelitos en el distrito fiscal de Huánuco durante el periodo 2020.

1.5.2 Objetivos Específicos

Conforme señala Ñaupas et al (2018), los objetivos específicos son "enunciados proposicionales desagregados, derivados de un objetivo general (…)" (p. 218), los cuales se derivan o deducen con fines metodológicos y operativos; asimismo, en razón de que el objetivo general fue formulado en el marco de una investigación correlacional de dos variables, para los objetivos específicos se tuvo que aplicar de forma semejante la misma metodología, en donde los objetivos específicos se obtuvieron de la correlación de las variables con los indicadores, lo cual se explicará a detalle más adelante en el capítulo correspondiente. A continuación, se presenta los objetivos específicos que fueron formulados:

OE1. Determinar la relación entre el reconocimiento de tecnologías para la seguridad de la información por el operador jurídico y la investigación penal de ciberdelitos.

OE2. Determinar la relación entre la aplicación de procedimientos para la seguridad de la información en el ciberespacio por el operador jurídico y la investigación penal de ciberdelitos.

OE3. Determinar la relación entre la identificación de incidentes de seguridad de la información en el ciberespacio por el operador jurídico y la investigación penal de ciberdelitos.

OE4. Determinar la relación entre la respuesta a incidentes de seguridad de la información en el ciberespacio por el operador jurídico y la investigación penal de ciberdelitos.

CAPÍTULO II. SISTEMA DE HIPÓTESIS

2.1 Formulación de la hipótesis

Según Hernández et al et al (2014, pág. 104), la hipótesis viene a ser la guía dentro del desarrollo de una investigación o estudio, entendiéndose como explicaciones tentativas del fenómeno que fue investigado, es decir si en el problema de investigación hemos formulado una pregunta, con la hipótesis estaríamos formulando una posible respuesta a dicha pregunta (Carrasco, 2007, pág. 184), y aunque no hay consenso respecto de la definición de lo que es una hipótesis, podemos tomar la definición planteada por Carrasco al decir que son "enunciados que contienen la respuesta probable al problema de investigación y hace referencia al desenvolvimiento empírico de la variable o relación entre variables (…)" (2007, pág. 186).

2.1.1 Hipótesis general

Según Carrasco (2007, pág. 189), una hipótesis debe contener elementos metodológicos y referenciales, al respecto en el presente estudio se consideró en su formulación los siguientes elementos metodológicos: las variables (las competencias en ciberseguridad y la investigación penal de ciberdelitos), las unidades de análisis (los operadores jurídicos) y el uso de conectores lógicos; de igual modo se consideró los siguientes elementos referenciales: el espacio (el distrito fiscal de Huánuco) y el tiempo (el periodo 2020). Es así como también en concordancia con el problema y objetivo de la investigación, y atendiendo que estamos ante una investigación de enfoque cuantitativo, se generó una hipótesis que negara la relación de influencia entre las variables, llamada hipótesis nula (Ho), y una hipótesis general que afirme dicha relación, llamada hipótesis alternativa (Ha), por tanto, las hipótesis formuladas son las siguientes:

Ho. Las competencias en ciberseguridad del operador jurídico no se relacionan con la investigación penal de delitos informáticos en el distrito fiscal de Huánuco durante el periodo 2020

Ha. Las competencias en ciberseguridad del operador jurídico se relacionan con la investigación penal de delitos informáticos en el distrito fiscal de Huánuco durante el periodo 2020.

2.1.2 Hipótesis Específicas

Conforme nos ilustra Carrasco (2007, pág. 204), las hipótesis específicas guardan una estrecha relación con los problemas específicos, y se derivan de la hipótesis general, por tanto, las hipótesis específicas fueron formuladas considerando su respectiva hipótesis nula, que se presentan a continuación:

- **Hipótesis específica 1:**

Ho1. El reconocimiento de tecnologías para la seguridad de la información por el operador jurídico no se relaciona con la investigación penal de ciberdelitos en el distrito fiscal de Huánuco durante el periodo 2020.

Ha1. El reconocimiento de tecnologías para la seguridad de la información por el operador jurídico no se relaciona con la investigación penal de ciberdelitos en el distrito fiscal de Huánuco durante el periodo 2020.

- **Hipótesis específica 2:**

Ho2. La aplicación de procedimientos para la seguridad de la información en el ciberespacio por el operador jurídico no se relaciona con la investigación penal de ciberdelitos en el distrito fiscal de Huánuco durante el periodo 2020.

Ha2. La aplicación de procedimientos para la seguridad de la información en el ciberespacio por el operador jurídico se relaciona con la investigación penal de ciberdelitos en el distrito fiscal de Huánuco durante el periodo 2020.

- **Hipótesis específica 3:**

Ho3. La identificación de incidentes de seguridad de la información en el ciberespacio por el operador jurídico no se relaciona con la investigación penal de ciberdelitos en el distrito fiscal de Huánuco durante el periodo 2020.

Ha3. La identificación de incidentes de seguridad de la información en el ciberespacio por el operador jurídico se relaciona con la investigación penal de ciberdelitos en el distrito fiscal de Huánuco durante el periodo 2020.

- **Hipótesis especifica 4**

Ho4. La respuesta a incidentes de seguridad de la información en el ciberespacio por el operador jurídico no se relaciona con la investigación penal de ciberdelitos en el distrito fiscal de Huánuco durante el periodo 2020.

Ho4. La respuesta a incidentes de seguridad de la información en el ciberespacio por el operador jurídico se relaciona con la investigación penal de ciberdelitos en el distrito fiscal de Huánuco durante el periodo 2020.

2.2 Operacionalización de Variables

Tabla 1

Operacionalización de variables

VARIABLES	DIMENSIONES	INDICADORES
V1: Competencias en ciberseguridad del operador jurídico	Reconocimiento de tecnologías en ciberseguridad por el operador jurídico	Identifica tecnologías en ciberseguridad
		Identifica problemas, riesgos y vulnerabilidades de tecnologías en ciberseguridad
		Identifica aplicaciones de tecnologías en ciberseguridad
	Aplicación de procedimientos en ciberseguridad por el operador jurídico	Realiza copias de seguridad de datos informáticos
		Identifica límites de acceso y uso de datos y tecnologías informáticas
		Aplica protocolos de seguridad de datos de datos y tecnologías informáticas
	Identificación de incidentes en ciberseguridad por el operador jurídico	Identifica la clasificación de incidentes en ciberseguridad
		Identifica las características de incidentes en ciberseguridad
		Identifica los riesgos, amenazas y relevancia jurídica de incidentes en ciberseguridad
	Respuesta de incidentes en ciberseguridad por el operador jurídico	Identifica roles y responsabilidades en incidentes en ciberseguridad

		Identifica el marco jurídico aplicable en incidentes de ciberseguridad
		Aplica la informática forense en la investigación de incidentes en ciberseguridad.
V2: Investigación penal de ciberdelitos	Investigación penal de delitos que afectan datos informáticos	Identifica si la conducta incriminada es delictuosa.
		Identifica las circunstancias y/o móviles del hecho.
		Identifica la identidad del autor, participe y víctimas.
		Identifica la existencia del daño causado.
	Investigación penal de delitos que afectan sistemas informáticos	Identifica si la conducta incriminada es delictuosa.
		Identifica las circunstancias y/o móviles del hecho.
		Identifica la identidad del autor, participe y víctimas.
		Identifica la existencia del daño causado.
	Investigación penal de delitos que afectan otros bienes jurídicos de relevancia penal mediante la utilización de las tecnologías de la información y las comunicaciones	Identifica si la conducta incriminada es delictuosa.
		Identifica las circunstancias y/o móviles del hecho.
		Identifica la identidad del autor, participe y víctimas.
		Identifica la existencia del daño causado.

Nota. Elaboración propia

2.3 Definición Operacional de las Variables

Según Reynolds (2014, pág. 120) una definición operacional "constituye el conjunto de procedimientos que describe las actividades que un observador debe realizar para recibir las impresiones sensoriales, las cuales indican la existencia de un concepto teórico en mayor o menor grado.", es así como considerando que la presente investigación considero dos variables de estudios, estas tuvieron la siguiente definición operacional:

V1. Competencias en ciberseguridad del operador jurídico: Competencias en ciberseguridad para el reconocimiento de tecnologías y aplicación de procedimientos, así como la identificación y respuesta de incidentes por el operador jurídico.

V2. Investigación penal de ciberdelitos: Investigación de delitos que afectan sistemas o datos informáticos u otros bienes jurídicos de relevancia penal mediante la utilización de las tecnologías de la información y las comunicaciones.

CAPÍTULO III. MARCO TEÓRICO

3.1 Antecedentes de la Investigación

3.1.1 Antecedentes Internacionales

A nivel internacional, se pudo recabar los siguientes trabajos de investigación:

- Rodríguez (2021) en su trabajo de investigación "Ciberseguridad en la justicia digital: recomendaciones para el caso colombiano", concluyó que la ciberseguridad "es un elemento indispensable en cada aspecto de la justicia digital" agregando en relación con los operadores jurídicos que:

  > Los hallazgos aquí presentados permiten que los servidores judiciales y profesionales jurídicos comprendan el panorama del uso de las TIC, los riesgos cibernéticos y posibles recomendaciones por etapa judicial. (p. 38)

- Montgomery (2017) en su trabajo de investigación "New security for a new era: an investigation into law enforcement cybersecurity threats, obstacles, and community applications" [Nueva seguridad para una nueva era: una investigación sobre las amenazas, los obstáculos y las aplicaciones comunitarias de la seguridad cibernética de las fuerzas del orden], concluye que:

  > Failure to update technology has resulted in law enforcement lagging behind in technology policies and practices, particularly in the area of cybersecurity. As an organization that possesses confidential data and is a required component of critical infrastructure, law enforcement has become an attractive target for cyber-attacks." [La falta de actualización de la tecnología ha resultado en que las fuerzas del orden se retrasen en políticas y prácticas tecnológicas, particularmente en el área de la seguridad cibernética. Como organización que posee datos confidenciales y es un componente necesario de la infraestructura crítica, la aplicación de la ley se ha convertido en un objetivo atractivo para los ataques cibernéticos]. (p. 63)

- Lundquist (2016) en su trabajo de investigación “An Examination of Failed Digital Forensics and the Criminal Justice System” [Un examen de análisis forenses digitales fallidos y el sistema de justicia penal] concluye que:

  > Within the Literature Review, this capstone addressed the research questions with the most current literature on the technical issues facing digital investigators. The literature identified technical issues such as the seizure of digital evidence, digital evidence chain of custody within law enforcement, authentication, and admissibility as key obstacles within digital forensic investigations. [Dentro de la Revisión de la literatura, esta piedra angular abordó las preguntas de investigación con la literatura más actual sobre los problemas técnicos que enfrentan los investigadores digitales. La literatura identificó problemas técnicos como la incautación de evidencia digital, la cadena de custodia de evidencia digital dentro de la aplicación de la ley, la autenticación y la admisibilidad como obstáculos clave dentro de las investigaciones forenses digitales]. (p. 60)

- Caamaño & Gil (2020) en su trabajo de investigación “Prevención de riesgos por ciberseguridad desde la auditoria forense: conjugando el talento humano organizacional” llegó a la conclusión que:

  > La ciberseguridad organizacional debe concebirse como un sistema integrado, de tal forma, que sus componentes al interrelacionarse entre sí, con la gestión del conocimiento y la auditoría forense, se blinde a las organizaciones modernas, mediante la exigencias y puesta en práctica de valores y principios corporativos, propios del buen gobierno, así como, de política, planes y programas que fortalezcan las competencias del talento humano. (p. 76)

3.1.2 Antecedentes nacionales

A nivel nacional, se pudo recabar los siguientes trabajos de investigación:

- Rossi (2021) en su trabajo de investigación “La Seguridad y Defensa en la era de la Cuarta Revolución Industrial: Elementos para una propuesta de estrategia de

política exterior para el fortalecimiento de las capacidades del Perú en materia de ciberdefensa y amenazas híbridas" arribó entre sus conclusiones que "(…) el mayor uso de las tecnologías de la información por parte del Estado y por parte de la población en general no ha traído consigo una mayor concientización ni uso de herramientas de ciberseguridad para su propia protección." (p. 144).

- Ormachea (2019) en su trabajo de investigación "Estrategias integradas de ciberseguridad para el fortalecimiento de la seguridad nacional", concluye que:

  > (…) la megatendencia del uso del ciberespacio y las facilidades que presenta se obtiene en un gran impacto para la reducción de las brechas de acceso a la información en el acceso de bienes y servicios que auguran nuevas oportunidades de negocios y de desarrollo, pero a su vez configura la apertura de una gran brecha a los ladrones de información que acechan el ciberespacio (…). (p. 46)

- Huamantingo (2022) en su trabajo de investigación "Modelo para el Análisis de Vulnerabilidades Digitales en una entidad pública de Lima, 2021", considera que "(…) un modelo para el análisis de vulnerabilidades digitales en una entidad pública, debe tener estos tres pilares que son: la gestión de vulnerabilidades, la metodología para el análisis y la tecnología defensiva (…)" (p. 33).

3.1.3 Antecedentes Locales

A nivel local, se pudo recabar los siguientes trabajos de investigación:

- Sandoval (2020) en su trabajo de investigación titulado "Propuesta de diseño de un sistema de gestión de seguridad de la información basado en la NTPISO/IEC 27001 para la Dirección Regional de Trabajo y Promoción del Empleo – Huánuco", concluyó que:

  > Para el análisis y gestión de riesgos permitió observar las amenazas internas y externas a las que está expuesta la organización, su impacto y los riesgos que lleva consigo. Según el análisis realizado, la Dirección Regional de Trabajo y Promoción del Empleo – Huánuco se encontraba en un nivel intolerable, dado

> que, la mayor cantidad de sus activos estaban fuera del apetito de riesgo. (p. 82)

- Vilca (2018) en su trabajo de investigación "La formación profesional en derecho informático y la persecución penal de delitos informáticos en el distrito fiscal de Huánuco - 2017" concluyó entre otros puntos que:

> Existe una relación significativa entre la aplicación de la informática jurídica y las Tecnologías de la Información y las Comunicaciones con la persecución penal de delitos informáticos, por cuanto ambas áreas son parte importante del derecho informático, y juegan en este siglo XXI un rol preponderante en la vida del profesional del derecho, el cual debe mantenerse constantemente actualizado en las nuevas aplicaciones que tiene la informática jurídica, así como el de conocer también las aplicaciones de las Tecnologías de la Información y las Comunicaciones, las cuales vienen evolucionando de manera acelerada a cada momento con nuevas invenciones, ya sea para que las aplique para mejorar su desempeño como profesional, como también para identificar posibles aplicaciones maliciosas que se pueden derivar en la comisión de delitos informáticos. (p. 162)

3.2 Bases Teóricas

3.2.1 La ciberseguridad

3.2.1.1 Concepto y definición de ciberseguridad. En principio se tiene que las ciencias de la computación dieron origen a la informática, una disciplina que conceptualmente se ocupa del tratamiento automatizado de la información, el cual según la RAE (2021) se define como el "Conjunto de conocimientos científicos y técnicas que hacen posible el tratamiento automático de la información por medio de computadoras." (p. 01); esta disciplina a su vez da lugar diversas ramas, como son la cibernética, las tecnologías de la información y las comunicaciones, la robótica, etc, también da nacimiento al de la seguridad informática, como aquella que se ocupará de la seguridad de la información en el ciberespacio. La seguridad informática a su vez es un área muy ligada a la seguridad de la información, por cuanto se ocupa de proteger

la integridad de la información almacenada en medios informáticos, una acción que despliega a través de la gestión de los riesgos que se presentan durante su tratamiento, siendo así, dentro de la propia seguridad informática encontraremos a la ciberseguridad, que en esencia protege la información que se almacena en sistemas informáticos interconectados, en ese sentido, empresas como Karspersky (2021) la definen como "(…) la práctica de defender las computadoras, los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos." (p. 1), o CISCO (CISCO, 2021) que entiende que es "la práctica de proteger sistemas, redes y programas de ataques digitales.", sin embargo, al día de hoy este concepto se ha visto renovado y ampliado continuamente, hasta llegar a definiciones como las que nos provee el Instituto Nacional de Estándares y Tecnología (2021) que la define como "Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation" [Prevención de daños, protección y restauración de computadoras, sistemas de comunicaciones electrónicas, servicios de comunicaciones electrónicas, comunicaciones por cable y comunicaciones electrónicas, incluida la información contenida en ellos, para garantizar su disponibilidad, integridad, autenticación, confidencialidad y no repudio.] (p.1), del mismo modo podemos citar la definición que nos provee la norma ISO 27100 (2020) que la define como "safeguarding of people, society, organizations and nations from cyber risks" [protección de las personas, la sociedad, las organizaciones y las naciones de los riesgos cibernéticos] (p.1).

3.2.1.2 Antecedentes históricos de la ciberseguridad. Los antecedentes de la ciberseguridad se encuentran ligados a los de la informática, sin embargo, si se quiere repasar sus antecedentes históricos, debemos adelantarnos en su historia hasta llegar al momento en que hizo su aparición el primer ensayo de lo que ahora se conoce como malware, denominado Creeper, un software malicioso creado en el año de 1971 y que fue desarrollado como parte de un experimento en donde se demostró como un programa informático podía virtualmente "viajar" entre computadoras (la red ARPANET) sin mediar acto de autorización previa alguna, ciertamente es discutible

dada su naturaleza experimental catalogarlo tajantemente como malware, empero no se puede negar que dentro un análisis de seguridad informática, Creeper fue la representación de lo que significa vulnerar una red y sistema informático. Luego de Creeper, el mundo vio como fueron apareciendo programas informáticos de similares características, pero programados para generar un efecto negativo dañino, por todo ello nació la denominación de los "virus", de la mano de Fred Cohen, que como parte de una recordada presentación demostró como un programa informático programado de forma maliciosa puede llegar a aprovechar las vulnerabilidades de un sistema para infectarlo, lo cual se puede resaltar como un motivo importante para la adopción de medidas que ayuden a paliar dichas vulnerabilidades y confrontar la amenazas.

Ciertamente se podría atribuir al malware el motivo por el cual se desarrolló el concepto de ciberseguridad, el cual está muy ligado a la seguridad de la información, sin embargo es menester recordar que en la década de los años 70, junto con la aparición de estos primeros programas maliciosos también se tuvo la mala praxis por parte de personas con conocimientos en uso de programas informáticos el cometer delitos, como espionaje, estafas, piratería, extorsiones, etc; en estos delitos los sistemas informáticos no son vulnerados para alterar o sustraer los datos que en ellos residen, sino que sirven como puente para que se comentan delitos en el mundo físico.

Para la década de 1980, numerosas compañías se nutrieron de los avances en la informática y las ciencias computacionales en general para agilizar sus procesos productivos, la administración de sus cadenas de producción y suministro, atención al cliente, etc., de igual manera los países mas desarrollados incorporaron estos avances dentro de sus instituciones a fin de beneficiarse, aunque como era de esperarse toda esta adopción de los avances informáticos estuvieron acompañados de riesgos y amenazas, los cuales a su vez aumentaban la frecuencia de su ocurrencia, evolucionando no solo en número sino en complejidad técnica pues dichos riesgos y amenazas eran cada vez más elaboradas.

3.2.1.3 Las dimensiones de la seguridad informática. Como se ha mencionado, la ciberseguridad se encuentra muy ligada a la seguridad informática, la misma que teóricamente tiene una serie de dimensiones (disponibilidad, integridad,

autenticación, confidencialidad y no repudio) para proteger la información en el cibersespacio, dichas dimensiones son de vital consideración dentro de la ciberseguridad, en ese sentido se tiene las siguientes:

a) Disponibilidad: En esencia, la disponibilidad significa que la información debe encontrarse disponible en los sistemas informáticos siempre que así se requiera, en ese sentido podemos citar la ISO 27000:2018 en la cual se la define como "property of being accessible and usable on demand by an authorized entity" [propiedad de ser accesible y utilizable bajo demanda por una entidad autorizada]. De otro lado, cuando se detectan situaciones en las cuales la información podría no encontrarse disponible o no se encuentre restringida a accesos no autorizados, estaríamos hablando de amenazas informáticas que atentan la disponibilidad de la información, las mismas que pueden ser producto de un hecho fortuito (un fallo de software o hardware), negligencia (brechas de seguridad) o acciones provocadas (malware).

b) Integridad: La información en el ciberespacio debe conservar su integridad desde el momento de su creación, y aunque puede ser objeto de modificaciones y/o cambios, estos deben ser realizados solo por el creador o agentes autorizados, el objetivo de garantizar la integridad es evitar cambios o alteraciones no autorizadas, en ese sentido la ISO 27000:2018 la define como "property of accuracy and completeness" [propiedad de ser accesible y utilizable bajo demanda por una entidad autorizada].

c) Autenticidad: Con la autenticidad se garantiza que la información que se encuentra en el ciberespacio corresponda al origen o autoría de quien se dice es, en ese sentido la ISO 27000:2018 define la autenticidad "property that an entity is what it claims to be" [propiedad de que una entidad es lo que dice ser]. Es importante verificar la autenticidad de la información considerando que de no serlo se puede ser vulnerable a fraudes o ataques de malware.

d) Confidencialidad: La confidencialidad implica que la información en el ciberespacio solo debe ser accesible para quienes cuenten con la autorización necesaria, en ese sentido de acuerdo a la norma ISO 27000:2018 se la define como "property that information is not made available or disclosed to unauthorized

individuals, entities, or processes" [propiedad de que la información no se pone a disposición ni se revela a personas, entidades o procesos no autorizados].

e) No repudio: El no repudio de la información implica que durante su transmisión, la información no debe ser negada por quienes la reciben, es decir por los receptores, evitando así que se cuestione su origen, en ese sentido se tiene que en la norma ISO 27000:2018 se lo define como "ability to prove the occurrence of a claimed event or action and its originating entities" [capacidad para probar la ocurrencia de un evento o acción reclamada y sus entidades de origen].

3.2.1.4. Normas y estándares en ciberseguridad. En este punto, desglosaremos los normas y estándares en ciberseguridad, partiendo desde el ámbito internacional al nacional, conforme detalla a continuación:

3.2.1.4.1 Estándares internacionales. En marco del derecho internacional público, a la fecha no se tiene una norma jurídica o tratado que regule la ciberseguridad, esto en razón de que cada país o bloque de países (como la Unión Europea) elaboran sus propias normas en esta materia, sin embargo, si nos abocamos a la definición de la norma como estándar, encontraremos un conjunto de estándares emanados de organismo internacionales de prestigio que se abocan al tema de la seguridad de la información; asimismo aunque muchas no son de obligatorio cumplimiento en muchos países, de igual forma nos proveen de las pautas necesarias para alcanzar la calidad en la adopción de medidas que aseguren la información en el ciberespacio. Siendo así, se procede a repasar uno a uno, los principales "estándares" internacionales en materia de seguridad informática:

- **Las normas ISO:** Al respecto se puede decir que son un conjunto de estándares emanados y gestionados por el Organismo Internacional de Normalización – ISO y la Comisión Electrónica Internacional - IEC, siendo las normas 27000 las que se encuentran referidas específicamente a la seguridad de la información, y en las cuales se aborda de forma amplia el cómo implementar, mantener y gestionar un Sistema de gestión de la seguridad de la información (SGSI), en ese sentido se

sintetiza en el siguiente cuadro una descripción de cada una de las normas ISO pertenecientes a esta familia:

Tabla 2

Normas ISO en ciberseguridad

NORMA ISO		DESCRIPCIÓN
Que especifican requisitos	ISO 27001	Referida a los requisitos que se necesitan para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un SGSI.
	ISO 27006	Referida a los requisitos que se necesitan para certificar el cumplimiento de la ISO 27001.
	ISO 27009	Define los requisitos para el uso de la ISO 27001 en cualquier sector específico (campo, área de aplicación o sector de mercado), así como el cómo adicionar o mejorar los requisitos.
Que describen directrices generales	ISO 27002	Describe una lista de objetivos de control aceptados y de mejores prácticas para que sean utilizados en el SGSI.
	ISO 27003	Provee una explicación del cómo implementar la norma ISO 27001.
	ISO 27004	Se proporciona las pautas para evaluar el desempeño de la seguridad de la información y la efectividad del SGSI.
	ISO 27005	Se provee las directrices mediante las cuales se realizará la gestión de riesgos de seguridad de la información.
	ISO 27007	Se provee los procedimientos a utilizarse para realizar auditorías del SGSI, asimismo se provee orientaciones enfocadas a la competencia de los auditores de SGSI.
	ISO 27008	Se brinda orientaciones sobre la revisión de la

		implementación y operación de controles, incluyendo la verificación del cumplimiento técnicos de los controles del sistema de información.
	ISO 27013	Se brinda orientación sobre la implementación integrada de las normas ISO/IEC 27001 e ISO/IEC 20000-1 para organizaciones que tienen la intención de implementar ambas.
	ISO 27014	Se brinda orientaciones referidas a los principios y procesos para la gobernanza de la seguridad de la información, a través de los cuales una organización podrá evaluar, dirigir y monitorear la gestión de la seguridad de la información.
	ISO 27016	Se brinda la metodología para comprender económicamente el cómo valorar con mayor precisión sus activos de información identificados, valorar los riesgos potenciales y apreciar el valor que los controles de protección de la información brinda a dichos activos, así como determinar el nivel óptimo de recursos que se aplicaran para asegurar los mencionados activos.
	ISO 27021	Se especifican los requisitos de competencias para los profesionales ISMS que lideren o participen en el establecimiento, implementación, mantenimiento y mejora continua de uno o más procesos del SGSI

Normas que describen directrices específicas del sector	ISO 27010	Se proporcionan pautas adicionales a las dadas en familia ISO/IEC 27000 para la gestión de seguridad de la información Provee las directrices en adición a la guía dada en la familia de estándares de la ISO/IEC 27000 para la administración de implementacion en seguridad de la información.
	ISO 27011	Se proporciona pautas que respaldan la implementación de controles de seguridad de la información en las organizaciones de telecomunicaciones.
	ISO 27017	Proporciona pautas para los controles de seguridad de la información aplicables a la provisión y el uso de servicios que funcionan en la nube.
	ISO 27018	Se establece objetivos de control, controles y directrices comúnmente aceptados para implementar medidas para proteger la información de identificación personal (PII) de acuerdo con los principios de privacidad de ISO/IEC 29100.
	ISO 27019	Se proporciona una guía basada en ISO/IEC 27002:2013 aplicada a los sistemas de control de procesos utilizados por la industria de servicios públicos de energía.
	ISO 27799	Se brinda pautas para los estándares de seguridad de la información de la organización y las prácticas de gestión de la seguridad de la información

Nota. Elaboración propia.

- **Los estándares NIST**: Son un conjunto de estándares elaborados por el Instituto Nacional de Estándares y Tecnología (NIST por sus siglas en inglés) en los cuales se desarrolla el cómo implementar un marco (framework) de ciberseguridad, que

en esencia permita comprender mejor los riesgos que existen en ciberseguridad, administrarlos y reducirlos así como proteger las redes y datos informáticos, siendo así es importante recalcar que este marco voluntario permite gestionar mejor el tiempo y recursos económicos al momento de avocarse a la seguridad de la información. De otro lado, en cuanto al marco de ciberseguridad (Cibersecurity Framework) podemos resaltar que posee tres grandes componentes: el núcleo, los niveles de implementación y los perfiles dentro del propio marco. A continuación, describiremos cada una de estas partes:

Tabla 3

Marcos de ciberseguridad

MARCO DE CIBERSEGURIDAD	
Componentes	
El núcleo del marco de ciberseguridad (Framework Core)	En el núcleo encontramos un conjunto de estándares, pautas y prácticas que permitirán la comunicación de las actividades y resultados en materia de seguridad informática en toda la organización, desde los niveles ejecutivos hasta los niveles de implementación u operación, en ese sentido, este núcleo se encuentra subdividido en conjunto de funciones: identificar, proteger, detectar, responder y recuperar.
Niveles de implementación del marco (Framework Implementation Tiers)	En los niveles encontramos la descripción del grado en que las prácticas de gestión de riesgos de la organización exhiben las características definidas dentro del propio marco, asimismo estos niveles se encuentran a su vez divididos desde el nivel 1 que viene a ser denominado "parcial" hasta el nivel 4 que sería el "adaptativo". Cuando una organización se encuentre dentro de la selección de los niveles, deberá de considerar

	las practicas actuales en gestión de riesgos, el entorno de amenazas, los requisitos legales y reglamentarios, los objetivos comerciales y las limitaciones organizacionales.
Perfil del marco (Framework profile)	Un perfil representa los resultados basados en las necesidades comerciales que una organización ha seleccionado de las categorías y subcategorías del marco. Los perfiles se pueden usar para identificar oportunidades para mejorar la postura de seguridad cibernética comparando un perfil "actual" (el estado "tal como está") con un perfil "objetivo" (el estado "a ser", asimismo se pueden usar para respaldar la priorización y la medición del progreso hacia los perfiles objetivo, al tiempo que se tienen en cuenta otras necesidades comerciales, incluidas la rentabilidad y la innovación.

Nota. Elaboración propia.

- **COBIT**: Al respecto se puede iniciar mencionando que los “Objetivos de Control para Tecnologías de la Información Relacionadas” (COBIT en sus siglas en inglés) se definen como un marco (framework) para el gobierno y la gestión de las tecnologías de la información en la empresa, dicho marco fue elaborado por la Asociación de Auditoría y Control de Sistemas de Información (ISACA en sus siglas en inglés), una asociación internacional con sede en los Estados Unidos que se ocupa del desarrollo de metodologías y certificaciones para la ejecución de acciones de auditoria y control de sistemas de la información; la primera edición de COBIT fue lanzada en el año de 1996, siendo que en la actualidad su versión mas reciente es la del año 2019. De otro lado, en cuanto a la ciberseguridad, COBIT representa una ayuda importante para las organizaciones a la hora de minimizar riesgos, ello a través de una adecuada

administración de la seguridad, siendo que ello lo encontraremos dentro de los objetivos de gestión (Dominio Entregar, Dar servicio y Soporte), específicamente en el objetivo SS05 referido a "Gestionar los servicios de seguridad".

- **Modelo COSO**: El marco integrado de control interno (COSO por sus siglas en inglés), elaborado por el Comité de Organizaciones Patrocinadoras de la Comisión Treadway con sede en los Estados Unidos de América, es un marco diseñado para el control interno de riesgos por parte de las empresas, el cual a su vez se encuentra plasmado en una publicación de Gestión de Riesgos Empresariales (ERM en sus siglas en inglés) siendo su publicación más reciente la del 2017 (ERM 2017), la misma que puede ser objeto de revisión desde su sitio web oficial.

3.2.1.4.2 Normas nacionales relacionadas a ciberseguridad. En cuanto a normas jurídicas de trascendencia, el precedente más reciente que se tiene es el ocurrido en el año 2019 cuando se estuvo muy cerca de contar en el Perú con una "ley de ciberseguridad", la misma que ya tenía aprobado su dictamen en Congreso de la República, no obstante, por desidia de los parlamentarios de ese entonces dicha ley nunca se promulgó, y aunque se han presentado posteriormente nuevas iniciativas legislativas al respecto, estas aún siguen pendientes de debate; sin embargo, se debe recalcar que a la fecha si se puede enumerar todo un conjunto de normas que abordan de alguna forma temas relacionados al ciberespacio, por ello, considerando la amplia dispersión que hay entre estas normas, las presentaremos a continuación en un cuadro, en donde se describirá los datos de la norma en cuestión y los artículos y/o incisos en donde se aborda en algún sentido la seguridad informática y la ciberseguridad:

Tabla 4

Normas jurídicas nacionales relacionadas a ciberseguridad

NORMA JURÍDICA	DESCRIPCIÓN	SOBRE SEGURIDAD INFORMÁTICA Y/O CIBERSEGURIDAD
Constitución Política del Perú	La constitución política del Perú vista como norma jurídica, viene a ser la más importante dentro del	En su artículo 2 inciso 6 se establece que toda persona tiene derecho "A que los servicios informáticos, computarizados o

	ordenamiento jurídico nacional.	no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar".
Decreto Legislativo N° 604 Ley de Organización y funciones del Instituto Nacional de Estadística e Informática	Mediante este decreto legislativo se establece la organización y funciones del INEI.	En artículo 9 inciso t) se establece como función del INEI "Producir y consolidar información e instrumentos informáticos para los fines de la seguridad nacional".
Ley Nº 27806 Ley de Transparencia y Acceso a la Información Pública y su reglamento aprobado mediante Decreto Supremo N° 072-2003-PCM	La finalidad fundamental de esta ley es la de regular el derecho fundamental de acceso a la información se encuentra contenida en la Constitución Política del Perú.	De acuerdo con el reglamento de dicha ley, en su artículo 3 inciso e) se establece que los máximos responsables de las entidades tienen la obligación de "Disponer se adopten las medidas de seguridad que permitan un adecuado uso y control de seguridad de la información de acceso restringido".
Ley Nº 27444 Ley de Procedimiento Administrativo General	A través de esta ley esencial del derecho administrativo peruano, se establece el régimen jurídico que resulta aplicable dentro de la administración pública.	Dentro del contenido de la ley, se aborda lo relacionado al procedimiento administrativo electrónico (art. 30) y el expediente electrónico (art. 31), en ese sentido, en el capítulo V sobre la ordenación del procedimiento, en su Art. 164.3 se menciona que "Las entidades podrán emplear tecnología de microformas y medios informáticos para el archivo y tramitación de expedientes, previendo las

		seguridades, inalterabilidad e integridad de su contenido"
Ley N° 27269: Ley de Firmas y Certificados Digitales	Mediante esta ley se regula la utilización de la firma electrónica y los certificados digitales en el Perú.	En esta ley, se establece que son las entidades de certificación las que deben de brindar seguridad, conforme es de verse en su Art. 12 en donde se menciona "La Entidad de Certificación cumple con la función de emitir o cancelar certificados digitales, así como brindar otros servicios inherentes al propio certificado o aquellos que brinden seguridad al sistema de certificados en particular o del comercio electrónico en general"
La Ley N° 29733 Ley de Protección de Datos Personales y su reglamento aprobado mediante Decreto Supremo N° 003-2013-JUS	El objeto de esta ley es garantizar el derecho constitucional a la protección de los datos personales.	De la revisión de la ley, se establece el principio de seguridad (Art. 9), como aquel en el cual el titular de un banco de datos personales y encargado de su tratamiento debe de garantizar la seguridad de los datos personales, en ese sentido se menciona que se deben de adoptar medidas técnicas, organizativas y legales. De otro lado, en su reglamento, la ley de protección de datos personales establece que en cuanto al principio de seguridad (Art. 10 del reglamento), las medidas a adoptarse deben estar orientadas a cualquier tratamiento contrario a la ley o al reglamento, incluyendo la adulteración, perdida, deviación de información intencional o no, sea por una acción humana o de un medio técnico. Es resaltable que en cuanto a los datos personales que obtengan los operadores de

		comunicaciones o telecomunicaciones, estos deberán por velar su seguridad, confidencialidad y uso adecuado (Art. 32 del reglamento. Finalmente es esencial mencionar que en el reglamento se establece las medidas de seguridad que deben de adoptarse con los sistemas informáticos que manejen bancos de datos personales adecuado (Art. 39 del reglamento), disponiéndose entre otros puntos que en cuanto a la conservación, respaldo y recuperación de los datos personales se deberán seguir las recomendaciones contenidas en la NTP ISO/IEC 17799 EDI (Art. 40 del reglamento).
Resolución Ministerial N° 246-2007-PCM	Mediante esta resolución ministerial se aprobó el uso obligatorio de la Norma Técnica Peruana NTP-ISO/ IEC 17799:2007 EDI	La norma técnica NTP-ISO/ IEC 17799:2007 EDI tiene como principal característica el adoptar la Norma ISO/IEC 17799:2005, dicho estándar internacional desarrolla el código para la práctica de la gestión de la seguridad de la información, en donde se aborda entre otros puntos la política de la seguridad de información, organización de la seguridad de información, la gestión de los activos, la gestión de las comunicaciones y operaciones, el control de acceso, la adquisición, desarrollo y mantenimiento de los sistemas de información, la gestión de incidentes de seguridad, la gestión

		de la continuidad del negocio y el cumplimiento.
Decreto Supremo 066-2011-PCM	Decreto supremo que aprueba el Plan de Desarrollo de la Sociedad de la Información en el Perú – La Agenda Digital Peruana 2.0	En la mencionada agenda a la cual hace referencia el mencionado decreto supremo, se tiene que esta en su Objetivo N° 07 establece la necesidad de promover una administración pública de calidad, siendo que para lograr dicho objetivo, se plantea como Estrategia N° 04 la implementación de mecanismo para mejorar la seguridad de la información aunado con la necesidad de contar con una estrategia nacional de ciberseguridad, a fin de mitigar riesgos en los recursos del Estado y disuadir el crimen cibernético.
Resolución Ministerial N° 004-2016-PCM	Mediante esta resolución ministerial se aprobó el uso obligatorio de la Norma Técnica Peruana NTP-ISO/ IEC 27001:2014 EDI	De la revisión de la resolución, se tiene que la norma técnica a la cual se hace referencia aborda lo referido a los sistemas de gestión de la seguridad de la información.
Decreto Legislativo N°1412 que aprueba la Ley de Gobierno Digital	La finalidad de esta ley es establecer el marco de gobernanza del gobierno digital, así como el régimen jurídico aplicable al uso transversal de tecnologías digitales.	En la ley aprobada, se puede advertir que en su Capítulo IV se aborda lo referido a la seguridad digital, desarrollándose lo relacionado al marco de seguridad digital del Estado, la gestión del marco de seguridad digital, e incluso la responsabilidad que tiene SERVIR para que promueva el fortalecimiento de las capacidades en materia de gobierno y tecnologías digitales.

Nota. Elaboración propia.

3.2.1.5 Competencias en ciberseguridad. La palabra competencia según la RAE (Real Academia Española, 2022), tiene de entre sus tantas acepciones la que lo define como una pericia, aptitud o idoneidad; en ese sentido, bajo dicha acepción las competencias se pueden abordar principalmente desde dos ámbitos: el pedagógico y el laboral y/o profesional. En cuanto al ámbito pedagógico, se encuentra extendida la concepción de que las competencias son un conjunto de conocimientos, capacidades, habilidades, destrezas y actitudes que poseen y desarrollan los educadores y educandos (Rivadeneira, 2017); de otro lado en el ámbito laboral, se entiende como competencia a aquella capacidad para tomar decisiones, en donde se hará uso de ese conjunto de conocimientos, habilidades y actitudes que se relacionen con una determinada profesión (Galdeano & Valiente, 2010).

Por lo expuesto, cuando nos referimos a las competencias en ciberseguridad, lo primero que se debe de considerar es que se pueden conceptuar partiendo del ámbito laboral y/o profesional, por cuanto su aplicación estará orientada al trabajo, asimismo, se debe tomar en cuenta que se encuentran subsumidas en competencias más genéricas, como son las competencias en informática, que a su vez se subsumen en las denominadas competencias digitales que de acuerdo con la UNESCO (2018) son:

Conjunto de competencias que permiten usar dispositivos digitales, aplicaciones de comunicación y redes para acceder y gestionar información, crear y compartir contenido digital, comunicarse, colaborar y resolver problemas para una realización personal efectiva y creativa, el aprendizaje, el trabajo y las actividades sociales en general. (p.2)

Como se ha mencionado antes, el propósito de la ciberseguridad es proteger la información en el ciberespacio, de allí que se encuentre estrechamente ligada con la seguridad informática, sin embargo esta protección se realiza a través de diferentes acciones de prevención y respuesta, en consecuencia las competencias en ciberseguridad vienen a ser ese conjunto de competencias profesionales orientadas a

proteger la información mediante la prevención, detección, y respuesta de incidentes en el ciberespacio.

Con estas consideraciones, resulta esencial mencionar de dónde es que se determinan cuáles son las competencias en ciberseguridad que se requieren dentro del ámbito laboral, en ese sentido, encontraremos que a nivel mundial diversas entidades gubernamentales, educativas y del empresariado enumeran de distinta manera (y según sus propios intereses y necesidades) las competencias en ciberseguridad que consideran necesarias, no obstante a consideración del investigador, la fecha la mejor referencia de acceso libre que encontraremos es el Cibersecurity Competency Model [Modelo de Competencias en Ciberseguridad], el cual es un modelo elaborado por entidades gubernamentales estadounidenses como la Employment and Training Administration [Administración de Empleo y Formación], el Department of Homeland Security [Departamento de Seguridad Nacional] con la participación de los departamentos federales de más de veinte estados, todo ello como parte del National Initiative for Cybersecurity Education [Iniciativa Nacional para la Educación en Ciberseguridad], y en la cual no solo se enumeran las competencias en ciberseguridad, sino que se encuentran ordenadas, agrupadas y esquematizadas.

En base a lo mencionado, cuando se revisa a detalle el Cibersecurity Competency Model [Modelo de Competencias en Ciberseguridad] se advierte que tiene como propósito el desarrollar un modelo integral de competencias sobre seguridad informática para el ámbito laboral, en la cual encontraremos cómo se detallan las competencias que requiere tanto el trabajador en general (entendido como aquel que solo necesita conectarse a internet o a la red de la organización) como para el trabajador avocado en la ciberseguridad; dichas competencias fueron identificadas en función a lo plasmado en el Workforce Framework for Cybersecurity [Marco laboral para la ciberseguridad], y aunque no son definitivas, ya que no es propósito del modelo de que lo sean, si pudieron elaborar un listado de competencias. De esta manera, en la parte introductoria del modelo (Employment and Training Administration, 2021) se aclara el concepto de ciberseguridad que sirve de fundamento

para formular cada una de las competencias que se describen más adelante es el siguiente:

> Cybersecurity is defined as the strategy, policy, and standards regarding the security of and operations in cyber-space, whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation. [La ciberseguridad se define como la estrategia, la política y los estándares relacionados con la seguridad y las operaciones en el ciberespacio, mediante los cuales los sistemas de información y comunicaciones y la información contenida en ellos están protegidos y/o defendidos contra daños, uso o modificación no autorizados o explotación]. (p.4)

De igual manera, en el referido modelo se brinda la definición sobre competencia que se utilizará:

> Cluster of related knowledge, skills, and abilities that affects a major part of one's job (a role or responsibility), that correlates with performance on the job, that can be measured against well-accepted standards, and that can be improved through training, development, and experience. [Conjunto de conocimientos, destrezas y habilidades relacionados que afectan una parte importante del trabajo de una persona (una función o responsabilidad), que se correlacionan con el desempeño en el trabajo, que se pueden medir frente a estándares bien aceptados y que se pueden mejorar a través de la capacitación, desarrollo y experiencia.] (p.2)

El modelo desglosa las competencias profesionales en cinco niveles (véase Gráfico N° 01), en el cual los tres primeros corresponden a las "competencias fundamentales" que debe tener un trabajador, y los dos últimos a las "competencias específicas de la industria", este apartado se encuentra a su vez compuesto por dos niveles, en donde el nivel cuatro denominado "Competencias técnicas de toda la industria" es el que abarca las competencias en ciberseguridad.

Las competencias en ciberseguridad en el nivel cuatro, se agrupan en cinco categorías según las actividades que se requieran en la industria, los cuales se detallan a continuación:

a) **Tecnología en ciberseguridad:** Engloban a las competencias que se consideran necesarias para comprender el propósito y función de las tecnologías de ciberseguridad, que incluyen herramientas y sistemas.
b) **Aseguramiento de la información:** Engloban las competencias que se consideran necesarias para proteger la confidencialidad, integridad y disponibilidad de la información.
c) **Gestión de riesgos:** Conjunto de competencias que se consideran necesarias para minimizar el riesgo en el ciberespacio y prevenir incidentes de ciberseguridad.
d) **Detección de incidentes:** Conjunto de competencias necesarias para identificar amenazas o incidentes.

Los apartados que se acaban de describir engloban decenas de competencias que requieren diversos grados de conocimiento en materia informática y ciberseguridad, en ese sentido resulta evidente que según el perfil y posición del trabajador resultará más relevante algunas competencias que otras.

3.2.1.6. Competencias en ciberseguridad del operador jurídico. El operador jurídico es definido de manera general como todo aquel individuo que como parte de su desempeño laboral se ocupa de crear, interpretar o aplicar el derecho (Poder Judicial de Costa Rica, 2021), en ese sentido la Real Academia de la Lengua Española (2021) lo define como “Persona o entidad que interviene en la creación, en la interpretación y aplicación de las normas jurídicas, o en el control de su cumplimiento” (p. 01), entendiéndose por definición que el operador jurídico no será siempre necesariamente un abogado, no obstante en el ámbito laboral el término usualmente es empleado para referirse a los profesionales del derecho independientemente de la función que cumplen ya sea como abogados litigantes, magistrados, autoridades, juristas, etc.

El operador jurídico como parte de su formación profesional en derecho adquiere todo un conjunto de competencias que son definidas por la institución

educativa en donde se imparte su enseñanza, por lo que por ejemplo si se repasa la currícula de universidades a nivel mundial veremos que las competencias impartidas pueden variar entre sí, no obstante, autores como Sanromán & Morales (2021) señalan de forma concisa cuáles serían las competencias fundamentales o básicas en la carrera de derecho:Por su parte, las competencias profesionales fundamentales en la formación de los abogados son la interpretación, la sistematización, la integración, la argumentación y la aplicación, así como saber reflexionar, identificar, elegir, dominar e integrar los problemas sociales interpretando los principios, las teorías, las normas y los axiomas, para poder comprender la disciplina del derecho. (p. 9)

Además de las competencias propias de carrera profesional en derecho, en la actualidad los centros de estudios incorporan de manera casi unánime el aprendizaje de competencias en informática básica, en donde el educando debe de aprender a conocer los fundamentos principales para el aprovechamiento de las tecnologías de la información y las comunicaciones, no obstante se debe de recordar que el derecho también ha incursionado en la informática, por lo que estas competencias pueden ir acompañadas por competencias en derecho informático y por ende e informática jurídica también; sobre esto último, de acuerdo con Vilca (2017, pág. 9), las competencias más esenciales que aquí encontraremos serían las siguientes:

- La aplicación de las fuentes jurídicas del derecho informático.
- La aplicación conceptos jurídicos de derecho informático.
- La aplicación del ordenamiento jurídico del derecho informático.
- La resolución de problemas en el ámbito derecho informático.
- La aplicación de la informática jurídica y las Tecnologías de la Información y las comunicaciones en el desempeño profesional.

En este punto se podría decir que si el operador jurídico cuenta con las competencias antes descritas, estaría preparado para afrontar con solvencia este nuevo escenario global dominado por la informática y las nuevas tecnologías, sin embargo como se ha repasado en el capítulo anterior la informática necesariamente conlleva la existencia de riesgos y amenazas, en consecuencia resulta inevitable que el operador jurídico deba de afrontar esta problemática, para lo cual entonces deberá de contar con

las competencias profesionales pertinentes, las mismas que se encontrarán definidas partiendo del campo de la ciberseguridad, que por definición se ocupa desde un sentido práctico de la gestión de los riesgos y amenazas de la información en el ciberespacio.

En ese sentido, para poder definir las competencias en ciberseguridad que requiere el operador jurídico deberemos partir nuevamente del Cibersecurity Competency Model [Modelo de Competencias en Ciberseguridad], que como ya se ha mencionado es el texto más completo y ordenado que enumera las principales competencias en ciberseguridad que se requieren en el ámbito laboral, pero en donde discriminaremos las competencias que requiere el profesional del derecho partiendo la propia naturaleza de la profesión, separando todas aquellas competencias que requieren una alta especialización técnica, ya que dichas competencias generalmente serán mas requeridas en perfiles profesionales como de los ingenieros y/o técnicos en informática. A continuación, desarrollaremos cada una de las competencias en ciberseguridad que requiere el operador jurídico, describiéndolas y desglosando cada una de las capacidades requeridas para alcanzarlas.

a) **Reconoce tecnologías en ciberseguridad:** Desde un ámbito laboral general consiste en que el operador jurídico pueda reconocer aquellas tecnologías de software y de hardware que le permitirán asegurar la disponibilidad, integridad, autenticidad y confidencialidad de la información, lo cual resulta importante ya que permite al operador jurídico debe mantenerse a la vanguarda de los últimos avances tecnológicos, tener noción sobro su conveniencia en cuanto a su aplicación y/o implementación, valorar en cierta medida su funcionamiento y principalmente reflexionar si así podrá prevenir riesgos y amenazas informáticas. Desde el ámbito de la administración de justicia dicha competencia implica también que el operador jurídico se encuentre debidamente informado de las tecnologías que se vienen aplicando para proteger la información dentro de los procesos judiciales por parte de instituciones como el Poder Judicial, Ministerio Público, Policía Nacional, etc. En ese sentido, para alcanzar esta competencia se pueden delimitar las siguientes:

- Identifica tecnologías en ciberseguridad, que implica que el operador jurídico sea capaz de identificar dentro de una amplia gama de tecnologías en informática, a aquellas que se encuentren relacionadas con la seguridad de la información.
- Identifica problemas, riesgos y vulnerabilidades de tecnologías en ciberseguridad, que implica que el operador jurídico identifica las posibles falencias que puedan presentas las tecnologías en ciberseguridad que se hayan implementado.
- Identifica aplicaciones de tecnologías en ciberseguridad, que implica que el operador jurídico, una vez identificó las tecnologías y consciente de los posibles problemas, riesgos o vulnerabilidades que presentan, sabe identificar las aplicaciones que se las puede dar según sus propios requerimientos profesionales.

b) Aplica procedimientos en ciberseguridad: La presente competencia se encuentra referida a la aplicación de procedimientos en ciberseguridad, partiendo de la premisa que ante la existencia de riesgos y amenazas en el ciberespacio se elaboran procedimientos para su gestión, lo que implica tener definidos los pasos a seguir en caso se produjera algún incidente, y aunque esta elaboración puede contener un alto nivel de tecnicidad, su aplicación tiene un carácter general, ya que con ello se garantiza la seguridad de la información. Desde el ámbito de la administración de justicia, los procedimientos en ciberseguridad están siendo plasmados en reglamentos y protocolos de carácter obligatorio y bajo responsabilidad de los funcionarios y servidores públicos. En ese sentido, para alcanzar esta competencia se pueden delimitar las siguientes:

- Realiza copias de seguridad de datos informáticos, que implica que el operador jurídico realiza procedimientos de respaldo de datos informáticos mediante la realización de copias de seguridad, un procedimiento que debe de ser realizado periódicamente y en donde se debe de valorar mucho el almacenamiento en donde se resguardará dichas copias.
- Identifica límites de acceso y uso de datos y tecnologías informáticas, que implica que el operador jurídico identifica en base a los procedimientos de ciberseguridad, quiénes pueden acceder a determinados datos, usarlos, así

como las tecnologías a utilizar, lo cual se realiza con el fin de evitar accesos no autorizados a determinada información e identificar cuando ello se transgrede.

- Aplica protocolos de seguridad de datos de datos y tecnologías informáticas, que implica que el operador jurídico sabe cómo aplicar los protocolos establecidos por la organización en donde se desempeñe, los mismo que son elaborados por expertos en el área.

c) Identifica incidentes en ciberseguridad: Consiste que, ante un incidente de ciberseguridad, el operador jurídico puede identificar su ocurrencia y así reportar lo ocurrido ante el área especializada de la organización a fin de sé que tomen las medidas pertinentes, coadyubando de esta manera a que se produzca una intervención del incidente rápida y oportuna. Desde el ámbito de la administración de justicia es importante anotar que esta competencia es importante para poder identificar incidentes en donde se haya producido accesos no autorizados a documentos reservados, a sistemas informáticos, etc. En ese sentido, para alcanzar esta competencia se pueden delimitar las siguientes:

- Identifica la clasificación de incidentes en ciberseguridad, que implica que el operador jurídico conoce la clasificación que el área especializada haya realizado, no obstante, si en caso se carece de esta, el operador jurídico esta en la capacidad al menos de forma general en clasificar los incidentes informáticos según su gravedad, nivel de sofisticación o impacto en los activos de información que se consideren importantes.
- Identifica las características de incidentes en ciberseguridad, que implica que el operador jurídico es capaz de tener noción sobre las características o rasgos más fundamentales de los incidentes de ciberseguridad.
- Identifica los riesgos, amenazas y relevancia jurídica de incidentes en ciberseguridad, que implica que ante la ocurrencia de un incidente que el operador jurídico ya pudo reconocer, identifica los riesgos y amenazas que implica, en especial su relevancia jurídica a fin de poder establecer responsabilidades administrativas, civiles y penales según sea el caso.

d) Responde a incidentes en ciberseguridad: Consiste que ante la ocurrencia de un incidente de ciberseguridad que ya fue plenamente identificado, el operador

jurídico sabe qué medidas de respuestas se deben de tomar a fin de que el daño o perjuicio ocasionado no se siga extendiendo más. Es importante resaltar que las acciones de respuesta del operador jurídico serán principalmente para mitigar el daño, dejando la parte de tratamiento y resolución del problema al equipo especializado. En el ámbito de la administración de justicia, aunque en las instituciones públicas se cuenten con equipos especializados en informática, que el operador jurídico conozca tomar acciones de respuesta rápida resultan de mucha ayuda. En ese sentido, para alcanzar esta competencia se pueden delimitar las siguientes:

- Identifica roles y responsabilidades en incidentes en ciberseguridad, que implica que el operador jurídico identifica a quién se le debe de atribuir la responsabilidad por la ocurrencia de un incidente, con apoyo esencial del área especializada que coadyubará a realizar dicha labor, y en cuyo análisis se deberá de considerar el rol que cumplen cada uno los responsables.
- Identifica el marco jurídico aplicable en incidentes de ciberseguridad, que implica que el operador jurídico como conocedor del derecho conoces cuales son las normas aplicables luego de la ocurrencia de un incidente de ciberseguridad, ello como parte del análisis de las posibles responsabilidades civiles, penales o administrativas que resulten aplicables.
- Aplica la informática forense en la investigación de incidentes en ciberseguridad, que implica que el operador jurídico conoce de forma generales cuales son los procedimientos en informática forense a seguir ante la ocurrencia de un incidente de ciberseguridad, los mismo que por su propia naturaleza facilitarán mucho su investigación.

3.2.2 Investigación penal de ciberdelitos

Los ciberdelitos a nivel mundial constituyen un motivo de preocupación debido a su variada complejidad y alcance, por este motivo es que muchos países se han ocupado de tipificarlos dentro de su normativa penal a fin de que puedan ser debidamente investigados y sancionados. La investigación de los ciberdelitos tiene como principal característica la sofisticación que los revistes, por ello se requieren de

muchas condiciones para garantizar en buena medida que dicha labor se llevará a cabo de forma eficiente:

- La primera condición es contar con un marco jurídico que se adapte a la investigación de este tipo de delitos.
- La segunda condición es contar con personal debidamente capacitado, que tenga noción acerca del ciberespacio, la ciberdelincuencia y el derecho penal informático.
- La tercera condición es contar con las herramientas tecnologías adecuadas que faciliten la investigación, las mismas que deberán estar en constante actualización debido a la evolución vertiginosa de los ciberdelitos y las modalidades para su comisión.

3.2.2.1 Ciberdelitos. Conceptualmente si los delitos que tienen como cualidad principal es el desarrollarse desde o través del ciberespacio se les denomina cybercrimes, término en inglés que de acuerdo con el diccionario de Cambridge (2021) se define como "crime or illegal activity that is done using the internet " [delito o actividad ilegal que se hace usando internet] (p. 1), de igual forma cuando se hace una amplia revisión bibliográfica, se advierte que comúnmente también se los denomina delitos informáticos, que según el Diccionario Panhispánico de la Real Academia Española (2021) se definen como "Infracción penal cometida utilizando un medio o un instrumento informático." (p. 1), es cierto que también se les puede llamar de otras maneras como delitos cibernéticos, de internet, de alta tecnología, de las telecomunicaciones, telemáticos, etc., no obstante, si se revisa la legislación de diversos países se advertirá que estos se decantan por los dos términos antes mencionados, aunque a criterio del investigador, el término más práctico en español sea el de ciberdelitos, al ser una traducción literal del término cybercrimes definido anteriormente.

Ahora bien, estando a las definiciones que se tienen sobre los ciberdelitos desde una cuestión puramente terminológica, ello resulta insuficiente para tener una comprensión de qué son exactamente, por este motivo, a fin de poder tener una idea

mas completa, se puede ir revisando en primer orden como es que los conceptúan las principales agencias que se dedican a la investigación de este tipo de delitos:

- Según el Federal Bureau of Investigation – FBI (2021) de los Estados Unidos de América los conceptúa de la siguiente forma "Cyber crimes are defined as a crime that involves a computer and a network" [Los ciberdelitos se definen como un delito que involucra una computadora y una red] (p. 1).
- Según la Organización International de Policía Criminal – INTERPOL (2017) a los ciberdelitos "puros" los conceptúa como "crimes against computers and information systems where the aim is to gain unauthorized access to a device or deny access to a legitimate user" [delitos contra las computadoras y los sistemas de información donde el objetivo es obtener acceso no autorizado a un dispositivo o denegar el acceso a un usuario legítimo] (p. 4), vale anotar que dicha distinción de "puros" es en razón de que también reconocen a los "cyber-enabled crimes" que vendrían a ser todos aquellos otros delitos cuyo alcance se ve amplificado mediante la utilización de computadoras y sistemas de información.
- La Agencia de la Unión Europea para la Cooperación Policial – EUROPO (2021) aunque no brinda un concepto concreto de los ciberdelitos si resalta que se están volviendo más agresivos y confrontacionales, indicando que ello se ve en las diferentes formas de ciberdelitos, incluyendo aquellos de alta tecnología, violaciones de datos y extorsión sexual (p.01).

Dentro de la doctrina jurídica existen también múltiples conceptos sobre los ciberdelitos, a continuación, repasaremos los que consideramos más relevantes:

- Según Téllez (2008) los ciberdelitos o delitos informáticos como él los denomina pueden tener un concepto atípico y típico:

  > En ese orden de ideas, según sea el caso, los delitos informáticos son "actitudes ilícitas que tienen las computadoras como instrumento o fin" (concepto atípico" o las "conductas típicas, antijurídicas y culpables que tienen a las computadoras como instrumento o fin" (concepto típico) (p.187).

- Según De Urbano (como se cita en Quevedo , 2017) respecto de los ciberdelitos los conceptua de la siguiente forma “Cuando se habla de ciberdelito se hace referencia a un tipo de delito, ya sea tradicional o propio de la sociedad de la información, propiciado por las tecnologías que ésta aporta” (p.60).
- Según Casabona (como se cita en Diaz, 2009) los ciberdelitos son descritos desde su óptica de la siguiente forma:

  El conjunto de conductas relativas al acceso, apropiación, intercambio y puesta a disposición de información en redes telemáticas, las cuales constituyen su entorno comisivo, perpetradas sin el consentimiento o autorización exigibles o utilizando información de contenido ilícito, pudiendo afectar a bienes jurídicos diversos de naturaleza individual o supraindividual (p.11).

- Según Villavicencio (2014) los delitos informáticos se pueden conceptualizar como “Aquellas conductas dirigidas a burlar los sistemas de dispositivos de seguridad, esto es, invasiones a computadoras, correos o sistemas de datas mediante una clave de acceso; conductas típicas que únicamente pueden ser cometidas a través de la tecnología” (p.49).

Aunque se pueden encontrar muchos mas conceptos, los presentados son formulados a partir de una revisión por parte de los autores de conceptos pasados, ello por la preocupación que se tiene a nivel doctrinario de que no se pueda formular un concepto convincente sobre ciberdelitos, aunque si coincidan respecto a sus características que repasaremos en el siguiente punto.

3.2.2.2 Características de los ciberdelitos. Los ciberdelitos tienen características que los diferencian de otros delitos, a continuación, repasaremos cada una de estas:

a) **No requieren de presencia física:** para su comisión la mayoría de las modalidades de ciberdelitos no requieren que el sujeto activo se movilice físicamente para cometer el delito, por el contrario, según el nivel de desarrollo de sus competencias en informática podrá prescindir de la presencialidad, y

desplegar su conducta a distancia a través del uso de redes de sistemas y ordenadores, como es el caso de INTERNET.

b) **Son transfronterizos:** En los ciberdelitos el sujeto activo puede realizar la comisión del ilícito sin tener como limitante las fronteras que existen entre los países.
c) **Requieren competencias en informática:** En los ciberdelitos el sujeto activo requiere contar con conocimientos y habilidades mínimas en informática para desplegar su accionar, según el nivel de estas competencias la sofisticación en la modalidad del delito será mayor.
d) **Sus efectos son casi inmediatos:** Los ciberdelitos una vez cometidos tienen efectos inmediatos, pues los acciones y/o procesos que se llevan a cabo en el ciberespacio tienen como cualidad principal el desarrollarse en tiempos muy cortos de unos pocos segundos, o incluso mucho menos.
e) **Pueden ser de alcance masivo:** Los ciberdelitos tienen una característica aterradora y es lo relacionado a su alcance, desde sus inicios los mayores incidentes delictivos se caracterizaron por afectar a decenas de miles de personas, siendo que este alcance con el pasar de los años se ha incrementado al punto en que los mayores incidentes de la actualidad afectan a decenas de millones de personas.
f) **Son difíciles de investigar:** Los ciberdelitos presentan retos al momento de su investigación pues la anonimidad del ciberespacio proporciona un escenario ideal para cometer actos delictivos pues se oculta eficientemente la identidad del autor.
g) **Se renuevan constantemente:** Los ciberdelitos evolucionan a cada momento respecto a las modalidades de su comisión, básicamente lo hacen a la par de los nuevos avances tecnológicos dada la facilidad que se tiene ahora para acceder a estos. Esta característica impone un esfuerzo extra para todos los gobiernos, pues deberán de revisar y actualizar (de ser necesario) su marco jurídico en lo que a ello respecta.
h) **Pueden ocasionar perjuicios a gran escala:** Los ciberdelitos pueden ocasionar perjuicios económicos, sociales y de seguridad a escala masiva, en

donde pueden perjudicar desde personas, empresas y hasta gobiernos amenazando así la seguridad interna de diversos países.

3.2.2.3 Clasificación de los ciberdelitos. De la revisión bibliográfica se identifica que existen diversas formas de clasificarlos, entre las clasificaciones más importantes encontramos las siguientes:

- Según Téllez (2008) los ciberdelitos se pueden clasificar como instrumento o medio y como fin u objetivo, por ello en el primer caso las conductas delictivas usan como medio a la informática para ser cometidas, por lo que aquí encontraremos a delitos comunes pero realizados a través del ciberespacio como es el caso de la falsificación de documentos, el fraude informático, etc., de otro lado en el segundo caso, las conductas delictivas tienen como objetivo el afectar dispositivos informáticos (p.190).
- Según las Naciones Unidas (como se cita en Téllez, 2008), también proporcionan una clasificación, en ese sentido se los divide en fraudes cometidos mediante la manipulación de ordenadores (que incluye conductas como la sustracción de datos, manipulación de programas, etc), daños o modificaciones de programas informáticos o de los datos (que incluye el uso de malware, sabotaje informático, etc) y finalmente las falsificaciones informáticas (que incluiría la alteración de documentos informáticos, y la reproducción total o parcial de archivos de uso comercial).
- Según (Rodriguez, América Latina, ¿debe crear un sistema de normas armonizadas para el cibercrimen?, 2013) del Convenio de Budapest también se puede advertir una agrupación de los ciberdelitos:

  Delitos contra la confidencialidad, integridad y disponibilidad de datos y sistemas informáticos; delitos por su contenido tales como la pornografía infantil y xenofobia; delitos relacionados con la informática como la falsificación y fraude; y delitos relacionados con las infracciones a los derechos de propiedad" (p.08).

3.2.2.4 Normativa internacional en ciberdelitos. A nivel internacional la principal norma sobre ciberdelitos es el Convenio de Ciberdelincuencia también conocido como el Convenio de Budapest (2001), dicho documento que data del año 2001 y que tuvo como firmantes a países de la Unión Europea, así como de Estados Unidos, Canadá, Japón y Sudáfrica tiene como propósito servir como una guía para la persecución de los ciberdelitos, como también el facilitar la cooperación entre todos los países firmantes, ya que como se recordará los ciberdelitos tienen como característica el ser transfronterizos.

De la revisión del Convenio de Budapest (2001) se puede resaltar que este se encuentra estructurado en dos secciones, cuatro capítulos, con un total de cuarenta y ocho artículos. A continuación, repasaremos los puntos más resaltantes que son de nuestro interés:

- En su primer capítulo se proporciona las definiciones de datos informáticos, sistemas informáticos, proveedor de servicios y datos relativos al tráfico, en donde vale hacer la aclaración que la distinción de este último hace referencia a los datos relacionados con una comunicación hecha a través de sistemas informáticos.
- El segundo capítulo se divide en una sección referida desde el derecho penal sustantivo y otra desde el derecho procesal; en ese sentido, en la primera sección se enumeran toda una lista de conductas que sugieren se deben de tipificar como ciberdelitos, las mismas que son agrupadas mediante títulos como: delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos (acceso ilícito, interceptación ilícita, ataque a la integridad de los datos o del sistema y abuso de dispositivos), delitos informáticos (falsificación informática y fraude informático), delitos relacionados con el contenido (pornografía infantil), y delitos relacionados con infracciones a la propiedad intelectual y de derechos afines. De la segunda sección encontraremos que también se organiza en títulos, en la cual se aborda la cuestión relativa al tratamiento de los datos informáticos, desde su conservación, orden de presentación, registro y confiscación, así como su obtención en tiempo real.

- El tercer capítulo se encuentra referido a la cooperación internacional entre los diversos países que suscribieron el convenio, y en donde de igual forma se organiza mediante títulos cuestiones como los principios generales relativos a la cooperación internacional, de la extradición, de la asistencia mutua y sus procedimientos en ausencia de acuerdos internacionales que resulten aplicables, entre otros.

3.2.2.5 Los ciberdelitos en el derecho penal peruano. En el Perú la inclusión de los ciberdelitos en la normativa penal es relativamente reciente (desde hace poco más de 20 años), pues tuvo como su primer antecedente la Ley 37309, del 17 de julio de 2020, con la que se incorporó en el Código Penal los artículos 207-A (sobre la interferencia, acceso o copia ilícita contenida en bases de datos, 207 – C (sobre la alteración, daño o destrucción de base de datos), y 207 – D (sobre el tráfico ilegal de datos), no obstante, a pesar de la tipificación de estas conductas los índices de criminalidad continuaron creciendo (conforme la tendencia global) y más importante resultaron insuficientes para penalizar las nuevas modalidades de ciberdelitos que se vienen desarrollando, por lo cual todos estos artículos fueron derogados por el congreso de la república, para ser reemplazados mediante una ley especial que permitiría actualizar la normativa penal y abordar de forma integral los ciberdelitos, refiriéndonos a Ley N° 30096 Ley de Delitos Informáticos, la misma que estuvo inspirada en el Convenio de Budaspet, el cual en ese momento el Perú aún no había suscrito.

La Ley N° 30096 fue un importante avance para el derecho penal peruano, al ser un paso contundente para permitiría abordar de forma eficiente el problema de la ciberdelincuencia, en ese sentido su artículo 1 señala que el objetivo es prevenir y sancionar las conductas que afecten sistemas y datos informáticos. No obstante, esta ley fue motivo de crítica por algunas inconsistencias que hacían confusa su aplicación, ya que por ejemplo criminalizaba conductas que no eran penalmente relevantes.

Frente a las críticas hechas a la Ley N° 30096, se promulgó su modificatoria a través de la Ley N° 30171, con la cual se realizó las correcciones pertinentes que se

mantienen hasta la actualidad. Siendo así queda entonces repasar uno a uno los ciberdelitos que se encuentran vigentes en la normativa penal peruana.

3.2.2.5.1 Acceso ilícito a un sistema informático (Art. 3). Es un delito de acción que sanciona el acceso en todo o en parte, sin la debida autorización, a un sistema informático, con la condicionante de que dicha acción se realice vulnerando las medidas de protección que fueron implementadas para impedir dicho acceso, lo cual se sanciona con pena privativa de la libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días multa, asimismo se aplica la misma pena si dicho acceso es excediendo lo autorizado.

Según Villavicencio (2014) en este delito se castiga la violación de la confidencialidad, la misma que se realiza mediante el acceso no autorizado a un sistema informático (p.49), que según el Convenio de Budapest (2001) es todo dispositivo o conjunto de dispositivos que se encuentran interconectados y que tiene como función el tratamiento automatizado de la información.

El verbo rector en este delito es el "acceder" que de acuerdo con la Real Academia Española (2022) tiene entre sus acepciones el entrar a un lugar o pasar a él, en ese sentido, un sistema informático constituye ese "lugar" al cual se accede, el mismo que como se ha mencionado se encuentra constituido por elementos físicos (hardware) y virtuales (software). Asimismo, cuando abordamos la relativo al verbo "acceder" se debe de tener en cuenta que la forma lícita para ingresar a un sistema informático es mediante datos de identificación configurados dentro del sistema, los cuales son dotados de atributos y condiciones de uso (constituyendo en si misma una medida de seguridad informática), no obstante para la configuración de este tipo penal se le acompaña otro verbo rector como es el de "vulneración" de medidas de seguridad, el cual según la Real Academia Española (2022) tiene entre sus acepciones la transgresión, quebrantamiento, violación de una ley o precepto, siendo que en este caso hablaríamos de una vulneración si se accede al sistema informático sin el uso de datos identificación (aprovechando brechas de seguridad o mediante software malicioso) o transgrediendo su uso (utilización indebida de datos de identificación) con lo cual se estaría configurando este delito.

3.2.2.5.2 Atentado a la integridad de datos informáticos (Art. 4). Es un delito de acción que sanciona si de forma deliberada e ilegítima se daña, introduce, borra, deteriora, altera, suprime o se hacen inaccesibles datos informáticos, lo cual se castiga con una pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días multa.

De la revisión de este tipo penal, queda claro que se trata de un delito doloso en el cual concurren dos requisitos para su comisión, la deliberación y la ilegitimidad, los cuales sirven de filtro para evitar criminalizar conductas que no son penalmente relevantes, esto en razón de que cada uno de los verbos rectores que en seguida se señalan (dañar, introducir, borrar, deteriorar, alterar, suprimir, o hacer inaccesible datos informáticos) pueden resultar de acciones fortuitas que no tienen siempre esa intencionalidad, como por ejemplo en casos de impericia, en donde el individuo desconociendo el uso de determinado dispositivo o sistema informático compromete la información contenida en los mismo, mediante cualquiera de los verbos rectores antes mencionados.

También es importante mencionar que, dentro de este tipo penal, podemos encuadrar diversas modalidades de ciberdelitos, en especial en aquellos donde media la utilización de malware, como ocurre con los virus, gusanos y troyanos informáticos, que son programas informáticos desarrollados con fines maliciosos, caracterizados principalmente por dañar, introducir dañar, introducir, borrar, deteriorar, alterar y suprimir datos informáticos, o como en el caso del rasomware en donde hacen inaccesibles dichos datos con la condicionante de pagar un rescate.

3.2.2.5.3 Atentado a la integridad de sistemas informático (Art.4). Es un delito de acción que sanciona si deliberada e ilegítimamente se inutiliza de forma parcial o total un sistema informático, se impide el acceso a este, entorpece o imposibilita su funcionamiento o la prestación de sus servicios, lo cual se castiga con una pena de privativa de libertad no menor de tres años ni mayor de seis años y con ochenta a ciento veinte días multa.

Este tipo penal doloso, en el cual también se aplican los requisitos de deliberación y la ilegitimidad, que sirven de filtro de otras conductas que afecten sistemas informáticos, considera también en su redacción a cuatro verbos rectores (inutilizar, impedir, entorpecer, imposibilitar) que son distintos a los considerados en el delito de atentado contra la integridad de datos informáticos, pero donde algunos guardan cierta semejanza, como ocurre en el inutilizar datos o sistemas informáticos lo cual es materialmente factible, lo mismo ocurre con el impedir su acceso, sin embargo ello no ocurre con el entorpecer su funcionamiento o la prestación de sus servicios, ya que el primer verbo hace alusión a la cualidad de procesar datos de los sistemas informáticos, y el segundo verbo a la posibilidad de prestar mediante la implementación y utilización de sistemas informáticos.

Respecto de las modalidades, existen diversas formas de afectar a los sistemas informáticos, ya sean acciones de sabotaje interno (por parte del propio personal), o ataques informáticos externos (en donde media el uso de malware), en cualquier caso, el denominador común es que para su comisión requieren de competencias en informática a un nivel intermedio u avanzado, a efectos de comprender como funciona el sistema informático y poder así planificar su vulneración.

3.2.2.5.4. Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos (Art. 5). Es un delito de acción que sanciona al que a través de INTERNET u otro medio análogo, se contacta con un(a) menor de catorce años para solicitarle u obtener material pornográfico, o para llevar a cabo actividades sexuales con él, lo cual es castigado con una pena privativa de libertad no menor de cuatro años ni mayor de ocho y con inhabilitación, según los numerales 1, 2 y 4 del Código Penal.

En este delito, se delimita el entorno sobre el cual es cometido, siendo que tanto el INTERNET como cualquier otro medio análogo que se menciona en el tipo penal están comprendidos dentro de lo que se conoce como ciberespacio, asimismo en cuanto a la víctima se delimita la edad en menores de catorce años, entendiéndose dicha precisión por la condición vulnerable de los menores en ese rango de edad. Es importante mencionar que dentro de este delito se estipula una circunstancia atenuante en relación a la víctima, en el cual si tiene entre catorce y dieciocho años de edad, la

pena será no menor de tres ni mayor de seis años (manteniéndose la inhabilitación según a los numerales 1, 2 y 4 del artículo 36 del Código Penal)

De otro lado en este tipo penal el verbo rector es el "contactar", que de acuerdo con la RAE (2022) se define como "establecer contacto o comunicación con alguien", dicho contacto que realiza el sujeto dolosamente debe de tener cualquiera de los propósitos señalados en el tipo penal, como es el solicitar u obtener material pornográfico, y el de llevar a cabo actividades sexuales, por lo que este tipo penal claramente hace alusión a lo que en el ciberespacio se denomina como "grooming", el cual de acuerdo a la Plataforma Digital Única del Estado Peruano (2021) es un término que se utiliza para referirse a las proposiciones sexuales hechas por parte de sujetos adultos a niños, niñas y adolescentes, todo ello con fines de explotación y abuso sexual.

3.2.2.5.5. Interceptación de datos informáticos (Art. 7). Es un delito de acción, que en su primer párrafo castiga a quien deliberada e ilegítimamente intercepta datos informáticos en transmisiones no públicas, dirigidos a un sistema informático, originados en un sistema informático o efectuado dentro del mismo, incluyendo las emisiones electromagnéticas provenientes de un sistema informático que transporte dichos datos informáticos, se reprime con pena privativa de libertad no menor de tres ni mayor de seis años.

Sobre este delito, nos encontramos frente a un delito doloso, ya que la deliberación e ilegitimidad son establecidos como requisitos para calificar una conducta en este tipo penal (y evitar así criminalizar conductas que no tienen relevancia penal ya que la interceptación de datos informáticos es una acción común en informática). De otro lado, en este primer párrafo se advierte hasta tres presupuestos para la comisión de este delito:

- Interceptación de datos informáticos en transmisiones no públicas dirigidos a un sistema informático.
- Interceptación de datos informáticos en transmisiones no públicas originados en un sistema informático.

- Interceptación de datos informáticos en transmisiones no públicas efectuadas dentro de un sistema informático.
- Interceptación de emisiones electromagnéticas provenientes de un sistema informático que transporten datos informáticos.

De los mencionados presupuestos, queda claro que este tipo penal es casi un calco de lo estipulado el artículo 3 del Convenio de Budapest (2001) sobre la interceptación ilícita, siendo que el propósito de esta norma es sancionar cualquier forma de interceptación de datos informáticos en el ciberespacio, que cumplan con los requisitos de deliberación e ilegitimidad antes mencionados.

En cuanto a circunstancias de atenuación y agravantes, debemos de mencionar que este tipo penal en su segundo, tercer y cuarto párrafo solo contempla agravantes:

- Si el delito recae sobre información secreta, reservada o confidencial en conformidad a la Ley 27806 Ley de Transparencia y Acceso a la Información Pública, le pena a aplicar será no menor de cinco ni mayor de ocho años.
- Si el delito compromete la defensa, seguridad o soberanía nacionales, la pena es no menor de ocho ni mayor de diez años.
- Si el agente comete el delito como integrante de una organización criminal, la pena se incrementa hasta en un tercio por encima del máximo legal previsto en los supuestos anteriores.

En cada uno de estos supuestos, se advierte que la severidad del castigo esta en función de la relevancia que tengan los datos informáticos, en donde a mayor importancia o sensibilidad mayor es la pena, lo cual aplica tanto para el primer y segundo presupuesto, siendo que, en el caso del tercer supuesto, la agravante está dirigida a la condición del agente debido a la problemática social de la criminalidad organizada, la misma que tiene un impacto negativo mucho mayor en la sociedad en comparación a individuos que actúan en solitario o complicidad, siendo además que en los grandes incidentes recientes de ciberdelincuencia en el mundo estuvieron involucradas organizaciones de criminalidad organizada de alcance internacional.

3.2.2.5.6. Fraude informático (Art. 8). Este delito de acción se castiga al que deliberada e ilegítimamente procura para sí o para otro un provecho ilícito en perjuicio de tercero mediante el diseño, introducción, alteración, borrado, supresión, clonación de datos informáticos o cualquier interferencia o manipulación en el funcionamiento de un sistema informático, lo cual se reprime con una pena privativa de libertad no menor de tres ni mayor de ocho años y con sesenta a ciento veinte días-multa.

Este tipo penal doloso, contempla como condición de que el agente procure para si mismo u otro un provecho ilícito, lo cual sirve como elemento diferenciador del delito de atentar contra datos informáticos, debido a que en ambos comparten el verbo rector de "introducción".

En este delito, el tipo penal contempla cinco verbos rectores respecto a los datos informáticos (diseño, introducción, alteración, borrado, supresión, clonación), y dos respecto de los sistemas informáticos (interferencia, manipulación), dicha diferenciación se entiende fue elaborada considerando la naturaleza diferente que tienen los datos y sistemas informáticos, de igual modo se infiere que los verbos fueron comprendidos en base a las modalidades conocidas de fraude informático (phishing, pharming, vishing, smishing, etc).

En cuanto a circunstancias atenuantes y agravantes, este tipo penal contempla una única circunstancia agravante que consiste cuando la comisión del delito afecte patrimonio del Estado destinado a fines asistenciales o a programas de apoyo social, en cuyo caso la pena será privativa de libertad no menor de cinco ni mayor de diez años y de ochenta a ciento cuarenta días-multa; claramente esta circunstancia agravante se encuentra inspirada en la especial atención que le dan los ciberdelincuentes a los operarios y/o beneficiarios de programas de apoyo social.

3.2.2.5.7. Abuso de mecanismos y dispositivos informáticos (Art. 10). Este delito de acción, contempla el sancionar a quien deliberada e ilegítimamente fabrica, diseña, desarrolla, vende, facilita, distribuye, importa u obtiene para su utilización, uno o más mecanismos, programas informáticos, dispositivos, contraseñas, códigos de acceso o cualquier otro dato informático, específicamente diseñados para la comisión

de delitos informáticos (previstos en la ley y su modificatoria), o el que ofrece o presta servicio que contribuya a ese propósito, lo cual es reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días-multa.

Es un delito doloso, que contempla para su comisión la deliberación e ilegitimidad, conteniendo en su redacción hasta diez verbos rectores (fabricar, diseñar, desarrollar, vender, facilitar, distribuir, importar, obtener, ofrecer, prestar), en el cual ocho de ellos se relacionan a mecanismos, programas informáticos, dispositivos, contraseñas, códigos de acceso o cualquier otro dato informático, con la precisión de que estos deben de haber sido diseñados específicamente para la comisión de ciberdelitos, mientras que los dos verbos rectores restantes se abocan en quienes ofrecen sus servicios para cometerlos, en ese sentido es importante precisar que este delito esta inspirado en dar sanción a quienes con sus conocimientos en informática son los que proveen las herramientas necesarias para la comisión de un ciberdelito (por ejemplo los "crackers" con sus conocimientos diseñan malware que será utilizado para cometer ciberdelitos), u ofrecen sus servicios en ese mismo sentido (por ejemplo en la "Deep Web" diversos individuos ofrecen sus servicios en programación de malware para la comisión de ciberdelitos).

3.2.2.6 La investigación de los ciberdelitos en el Perú. Conforme a lo desarrollado en los puntos precedentes, el Perú cuenta con un marco normativo penal que persigue y castiga los ciberdelitos, el cual como se mencionó se encuentra contenido en una ley especial de Delitos Informático (Ley N° 30096) y su modificatoria (Ley N° 30171), en ese sentido es pertinente abordar entonces cómo es que se investigan los ciberdelitos en el Perú, partiendo desde el campo procesalista, en el cual se debe de repasar cómo es que se encuentra dividido el proceso penal peruano, cuál es el papel que asumen cada una de las instituciones que intervienen, y un repaso los principales métodos y técnicas investigativas que son aplicables para la investigación de este tipo de delitos.

***3.2.2.6.1 Sobre el Proceso Penal Peruano*.** El Perú cuenta con un Código Procesal Penal vigente desde el año 2004, que tiene como principal característica el haber reformado el proceso penal ordinario que constaba únicamente de dos etapas (la

instrucción y el juicio oral), por un nuevo proceso penal que consta de tres etapas, y que se resumen de forma sintética a continuación:

- La investigación preparatoria, que se caracteriza principalmente por el rol protagónico que desempeña el fiscal como director de la investigación de un hecho presuntamente delictivo (Art. 60 inciso 2 del Código Procesal Penal), ello a fin de lograr su esclarecimiento y determinar entre otras cosas su delictuosidad, circunstancias que rodearon su perpetración, partícipes del hecho, etc. En esta etapa tiene un rol importante la Policía Nacional, la cual según el mencionado código se ocupa de prestar apoyo durante la investigación, ello bajo la conducción del fiscal y mediante la realización de diligencias que se estimen pertinentes (Art. 68 del Código Procesal Penal). Es importante indicar que la investigación preparatoria consta a su vez de dos partes, la investigación preliminar, que tiene como finalidad realizar actos urgentes e inaplazables, a fin de determinar la delictuosidad de un hecho y su esclarecimiento (Art. 330 del Código Procesal Penal), y la investigación preparatoria en sí misma, que se fundamenta en el descubrimiento de todo un conjunto de indicios reveladores respecto de la existencia de un delito que motivan a que el fiscal disponga la realización de más diligencias que permitan aclarar aún lo ocurrido (Art. 336 del Código Procesal Penal), esto con miras de acusar a los presuntos responsables por la clara comisión de un delito o solicitar el sobreseimiento de la investigación debido a la ocurrencia de cualquier de los presupuestos ya establecidos.

- La etapa intermedia, es una etapa que inicia formalmente con la conclusión de la investigación preparatoria, en la cual el fiscal luego de haber realizado la correspondiente investigación, y habiéndose agotado todos los plazos, comunica su finalización porque considera que tiene debidamente esclarecidos los hechos materia de investigación, identificando las circunstancias precedentes, concomitantes y posteriores, los partícipes, tipificando las conductas desplegadas, y por sobre todo el tener reunidos los elementos de convicción suficientes que le permitan fundamentar un requerimiento, sea de acusación o de sobreseimiento, ante el juez de investigación preparatoria, el cual ahora se ocupará de revisar dichos requerimientos y previa audiencia resolver si proceden, así como las pruebas que se ofrecen.

- **Juicio oral**: Finalizada la evaluación del requerimiento fiscal de acusación por parte del juez de investigación preparatoria, y dictado el auto de enjuiciamiento, se ingresa a la etapa de juicio oral, que es considerada como la principal dentro del desarrollo del proceso penal ordinario, y que consiste fundamentalmente en una audiencia en oral y pública, en la cual las partes en merito al principio de contradicción debaten cada uno de los fundamentos que el fiscal plasmó en su requerimiento de acusación, ello a fin de que el juez penal decida absolver o condenar al acusado, plasmando ello en una sentencia.

3.2.2.6.2 Sobre la investigación de ciberdelitos dentro de un proceso penal. Partiendo de lo repasado en el punto anterior, la investigación de los ciberdelitos puede iniciar de oficio o con la denuncia interpuesta por cualquier persona ante la autoridad respectiva, las cuales pueden ser recepcionadas en el Ministerio o en la Policía Nacional del Perú.

Hecha la denuncia de un presunto delictivo (relacionado a ciberdelitos), si fue hecha ante el Ministerio Público, será asignada a un fiscal para su investigación, el cual en cumplimiento de sus funciones deberá realizar la respectiva calificación jurídica, a fin de identificar preliminarmente si realmente estamos ante un hecho en el que se evidencie la presunta comisión de un ciberdelito, de igual modo, si es ante la Policía Nacional del Perú, dicha denuncia dará lugar a la elaboración de un informe policial que esencialmente contendrá los datos del (los) denunciante (s) y denunciado (s), actas, manifestaciones, pericias, u otros actos de investigación que bajo la dirección del fiscal se hayan realizado y que permitirán el esclarecimiento de los hechos, excepto la calificación jurídica (que le corresponde al fiscal), dicho informe posteriormente es remitido al fiscal a fin de que continue con la investigación. En ese sentido, es importante mencionar que en el caso de ciberdelitos no siempre las denuncias recabadas expresaran con precisión la identidad de los presuntos responsables, lo cual no debe causar extrañeza ya que una de las características de los ciberdelitos es precisamente la facilidad que se tiene de poder ocultar las identidades de quienes los cometen en el ciberespacio.

Una vez que el fiscal, que tomó conocimiento del presunto hecho delictivo, concluye que el hecho califica con alguno (os) de los tipos penales contenidos en la normativa penal de ciberdelitos (entiéndase la Ley N° 30096 y su modificatoria), deberá dar por iniciada la primera etapa del proceso penal ordinario, con la disposición de las diligencias preliminares, que como ya se ha mencionado consistirá en realización de toda una serie de diligencias y actos de investigación que permitan esclarecer los hechos. En el caso de los ciberdelitos, de acuerdo con las circunstancias del hecho y la presunta modalidad delictiva aplicada, el fiscal dispondrá según considere necesario, la realización de pericias y diligencias que requerirán de personal especializado, para lo cual hasta la fecha implica recurrir a la unidad especializada en la investigación de ciberdelitos (DIVINDAT) de la Policía Nacional del Perú; en cualquier caso, el fiscal afrontará la investigación de hechos que no poseen una alta la complejidad técnica como para motivar acudir a peritos especializados (por ejemplo en casos donde el ciberdelincuente no es tan habilidoso por lo que resulta sencillo analizar su accionar delictivo), como también estar frente a delitos de alta complejidad técnica que necesiten si o si de peritos informáticos (como por ejemplo aquellos casos en los cuales el ciberdelincuente cuidadosamente oculta su identidad y combina en su accionar delictivo la utilización de herramientas de hardware y de software).

De otro lado, en caso el fiscal reuniera suficientes elementos de convicción dentro del plazo de ley (incluyendo la prórroga), deberá pronunciarse, ya sea archivando el caso o formalizándolo, siendo que, si decidiera formalizar la investigación, será principalmente porque ha hallado elementos de convicción suficientes que sustentan dicha disposición, no obstante, también puede ocurrir el caso se archive por cualquiera de los supuestos que el Código Penal establece.

3.2.2.7 Los procedimientos en la investigación de ciberdelitos. Los ciberdelitos pueden ser investigados desde el ámbito privado o como parte de un proceso penal, el primer caso ocurre cuando en una organización frente la ocurrencia de un incidente de este tipo, se inicia una investigación a fin de determinar causas, establecer responsabilidades y planificar la respuesta al mismo, mientras que en el segundo caso, frente a la noticia criminal de la ocurrencia de este tipo de conductas

delictuosas, los estados y organizaciones supranacionales (INTERPOL) inicia una investigación a fin de hallar a los responsables y aplicarles la pena que corresponda, siendo que en el Perú, como se ha repasado, se ocupa de esta función el Ministerio Público.

Independientemente de quién o en donde se realicen las investigaciones, el manejo de la evidencia es uno de los pilares fundamentales para la investigación de ciberdelitos, que por su naturaleza diferenciadora frente a otros tipos delitos, requieren de consideraciones especiales, siendo así es importante iniciar la investigación identificando bien el espacio, tiempo y lugar con el que se cometió el ilícito, ya que no es lo mismo iniciar una investigación teniendo plenamente identificado el espacio físico en el cual se realizó (incluyendo los dispositivos electrónicos utilizados), que iniciarla contando únicamente con evidencias contenidas en el ciberespacio, en donde todo lo demás se encuentra pendiente de determinar. No obstante, regresando al primer escenario hipotético, lo que ocupa ahora es recabar dicha evidencia, para ello se debe tener como primera consideración el identificar cada uno de los dispositivos informáticos que se encuentren en la escena (en especial computadoras, discos duro, etc), los cuales de encontrarse encendidos, se procederá a recabar la evidencia que se considere pertinente (debido a que los datos que se generan temporalmente en el dispositivo luego desaparecen), o de encontrarse apagados se procederá con su recolección y lacrado (a fin de que puedan ser sometidos a las pericias que correspondan posteriormente).

Luego de recolectadas las evidencias, se las somete a un peritaje, con el cual se tratará de obtener pruebas mediante la aplicación de métodos y técnicas forenses (combinando la utilización de software y hardware creado para tal fin), que incluyen la creación de copias de seguridad sobre las cuales se realizará el análisis (se clonan los datos contenidos en los diferentes dispositivos que se hayan recabado y se someten a exámenes de informática forense).

Finalizado el análisis forense, la parte final corresponde al almacenamiento de las evidencias recabadas.

3.2.2.8 La ciberseguridad en el proceso penal de investigación de ciberdelitos. El proceso penal en la actualidad se ha beneficiado de los avances de la informático, esto debido a que las entidades que se ocupan de la administración de justicia o la persecución del delito (entiéndase Poder Judicial, Ministerio Público, Policía Nacional) han venido implementando los últimos avances tecnológicos, principalmente con la utilización de sistemas informáticos, los mismo que tienen como principal propósito el incrementar la eficiencia y rapidez en las actividades que se realizan, consecuencia de ello es que muchas de estas instituciones cuenten de forma general con portales web que incorporan sistemas informáticos para beneficio de usuarios externos (como litigantes , abogados, etc), como también de sistemas que automatizan procesos y son para el beneficio de los trabajadores; no obstante, como se ha expuesto en el primer capítulo de esta investigación, la utilización de la informática conlleva beneficios pero también riesgos de todo tipo, por tanto, si los procesos penales actualmente se benefician de las ventajas que trae la tecnología, también son vulnerables a riesgos en materia informática que los pueden afectar en diferente medida.

Desde el plano teórico, se tiene que la mejor forma de confrontar los riesgos informáticos es a través de la aplicación de la ciberseguridad, algo que desde las oficinas con competencia en la gestión de los sistemas informáticos entienden bien, en ese sentido de forma gradual han ido aplicando medidas para mitigar los riesgos o prevenirlos, ya sea desarrollando o adquiriendo programadas de software más seguros, como también de componentes de hardware más eficientes y seguros, no obstante todo ello resulta insuficiente si no se hace manera organizada y ordenada, lo cual se logra aplicando los novedosos marcos en ciberseguridad, que en conformidad a estándares internacionales aseguran una mejor gestión de la seguridad de la información en el tiempo.

En base a este razonamiento, considerando que dentro de los procesos penales existe la presencia de riesgos informáticos, tanto más ocurre en los referidos a ciberdelitos, que por su naturaleza tienen mucha de su evidencia y material probatorio en el ciberespacio que se encuentra en constante riesgo; siendo así, conviene recordar

que el proceso penal se encuentra compuesto por tres etapas bien definidas, en las cuales la aplicación de la las prácticas en ciberseguridad tanto por el personal técnico especializado como por los operadores de justicia resulta necesaria, pues para fundamentar este punto debemos partir de que durante la investigación preparatoria, las prácticas en ciberseguridad no solo permitirán asegurar las evidencias recabadas, sino también su aseguramiento para que sean útiles en un eventual juicio, lo mismo ocurre durante la investigación preparatoria, en la cual si bien es cierto se caracteriza por ser posterior a la etapa de investigación, tiene como caracteriza la realización de audiencias en donde se manipula en alguna forma las evidencias recabadas (que sustentan el requerimiento acusatorio o de sobreseimiento), finalmente frente a la etapa de juicio oral está justificada las prácticas en ciberseguridad, ya que se caracteriza por la actuación del material probatorio reunido por el fiscal para sustentar su pedido de sanción a los responsables, como parte del ejercicio de su función persecutora del delito.

3.2. Bases conceptuales

Informática: Comprende el estudio del tratamiento automatizado de la información, que incluye su procesamiento, almacenamiento y transferencia, mediante la utilización de componentes de software y de hardware.

Datos informáticos: Secuencia de representaciones simbólicas (que incluyen números, caracteres u otros tipos de símbolos) que se codifican en un determinado formato para que puedan ser ingresados dentro de un dispositivo informático, a fin de que puedan ser procesados y visualizados.

Sistemas informáticos: Comprendido como aquel conjunto de herramientas de software y hardware previamente elegidos, interconectados y preparados para funcionar de forma conjunta a fin de alcanzar un determinado conjunto de objetivos y propósitos

Competencias profesionales: Reúnen a todo el conjunto de conocimientos, destrezas y habilidades, aplicados en el ámbito profesional para la realización de una determinada labor.

Ciberseguridad: Entendida como el conjunto de prácticas que permiten proteger la información que se encuentra contenida en el ciberespacio.

Ciberdelito: Conjunto de conductas, típicas, antijurídicas y culpables que afectan datos y sistemas informáticos.

Ciberespacio: Entendido como aquel espacio virtual (no físico) construido partiendo de la interconexión de un conjunto de redes de tecnológicas que conforman infraestructuras de sistemas de información, el cual se caracteriza principalmente por conformar un entorno en el cual interactúan personas, servicios de software y servicios de internet, todo ello a través de dispositivos tecnológicos y redes que se conectan a la misma.

CAPÍTULO IV
MARCO METODOLÓGICO

4.1 Ámbito

En la presente investigación, el ámbito fue delimitado espacialmente en el distrito fiscal de Huánuco, el cual se encuentra circunscrito en el departamento de Huánuco en el Perú, según el portal web del Ministerio Público (2020, p. 1) dicho distrito fiscal a la fecha cuenta con fiscalías corporativas penales, fiscalías civiles y de familia, fiscalías especializadas (medio ambiente, trata de personas, violencia contra la mujer e integrantes del grupo familiar), una división médico legal, una unidad de atención de víctimas y testigos, un servicio de administración, entre otros.

4.2 Población y muestra

4.2.1 Descripción de la población

Partiendo de que el ámbito es el departamento de Huánuco, la población se encontró comprendida por operadores jurídicos que intervienen en la investigación de ciberdelitos, que en conformidad a lo establecido en la normativa procesal penal vigente, incluye a jueces, fiscales y abogados,

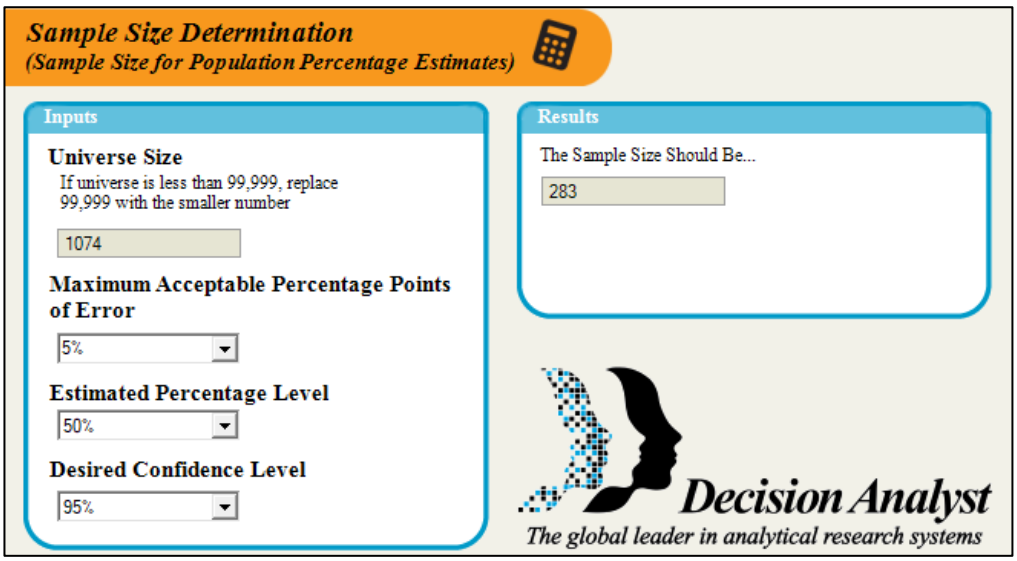
4.2.2 Muestra y método de muestreo

Conforme lo explicado por Hernández et al (2014), sobre los estudios transeccionales en los cuales se debe seleccionar una muestra, se procedió en primer orden en desglosar la unidad de análisis mencionada, que para el presente estudio son los operadores jurídicos, en tres subgrupos que conformaran juntos la muestra y que se indican a continuación:

- Fiscales que laboran en las fiscalías provinciales penales
- Jueces de investigación preparatoria.
- Abogados habilitados para ejercer la abogacía.

Esta división se justifica debido a que en el proceso penal, y como lo explica el Instituto de Ciencias Hegel (2019, p. 01), son varios los actores que intervienen en su desarrollo (jueces, fiscales, policías, personal administrativo, etc), pero de los cuales solo estos tres subgrupos entran de la definición de operadores jurídicos.

Seguidamente, definida la muestra, el método de muestreo aplicado fue el del muestreo estratificado, para lo cual se calculó primero el tamaño de la muestra general, con apoyo del software STATS 2.0 (2021, p. 01) , en el cual se precisó los valores del universo, el máximo porcentaje de error aceptable, el nivel de porcentaje estimado y el nivel de confianza:



Por tanto, ingresado los datos al software se obtuvo que la muestra total estaría conformada por 283 operadores jurídicos, no obstante, atendiendo a que esta se encuentra dividida en subgrupos, se realizó el cálculo correspondiente.

Tabla 5

Cálculo de la muestra de estudio

Subgrupos	Operadores jurídicos que intervienen en los procesos de investigación de delitos informáticos	Población total	Muestra (fh)=0.2635
1	Fiscales que laboran en las fiscalías provinciales penales corporativas y mixtas.	165	43
2	Jueces de investigación preparatoria.	9	2
3	Abogados habilitados para ejercer la abogacía.	900	237
Muestra general=283		1074	283

Nota. Elaboración propia.

De este cuadro se desprende que para este estudio se calculó que la muestra total antes mencionada la conforman 43 fiscales, 2 jueces de investigación preparatoria y 237 abogados habilitados para ejercer la abogacía.

4.3 Nivel y tipo de estudio

4.3.1 Nivel de estudio

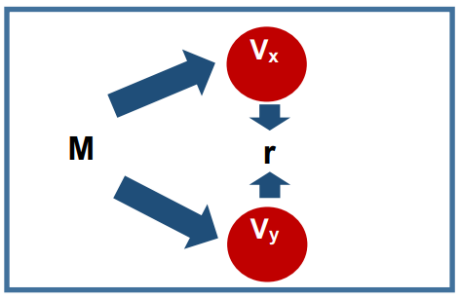
El nivel de la presente investigación fue explicativo, el cual que conforme a Carrasco (2017, p.42) se ocupa de indagar la relación recíproca y concatenada de hechos de la realidad, buscando dar una explicación objetiva real y científica a aquello que se desconoce.

4.3.2 Tipo de estudio

El presente estudio fue una investigación básica, pues conforme lo explica Carrasco (2017, p.43) se buscará ampliar y profundizar el caudal de conocimientos científicos existentes acerca de la realidad.

4.4 Diseño de investigación

En cuanto al diseño de investigación que se utilizó, fue el correlacional transeccional, el cual es un diseño de tipo no experimental que se emplea principalmente para describir las relaciones entre dos o más variables en un momento determinado, lo cual implica que solo se limitará a establecer relaciones entre variables sin precisar algún sentido de causalidad o de análisis de relaciones causales (Hernández et al, 2014, p.258).



Donde:

M : La muestra corresponde a los operadores jurídicos que intervienen dentro de la investigación de delitos informáticos.

Vx: Corresponde a las competencias en ciberseguridad.

Vy: Corresponde a la investigación de delitos informáticos.

r : Es el coeficiente de correlación.

4.5 Técnicas e instrumentos

En la presente investigación se utilizó la técnica de la encuesta, y como instrumento se utilizó el cuestionario, el cual según lo explicado por García (2021, p. 2) consiste en un conjunto de preguntas escritas o ítems que están relacionadas con los indicadores de la investigación, y por ende con las hipótesis y las variables.

Por tanto, la presente investigación consideró la formulación de un conjunto de preguntas cerradas, que según QuestionPro (2021, p. 1) son aquellas en las cuales se pide al encuestado que elija entre respuestas planteadas, las mismas que estuvieron contenidas en una escala ordinal de categorías que fueron previamente delimitadas.

4.6 Procedimiento

Para el desarrollo de la investigación se ha determinado el siguiente procedimiento a realizar aprovechando las tecnologías de la información y las comunicaciones:

4.6.1 Elaboración del instrumento

Definición y codificación de los ítems del instrumento, en consonancia con los indicadores de la investigación, el mismo que será elaborado a través del programa Microsoft Word, el cual según el propio sitio web de Microsoft (2021, p. 1) es un software de procesamiento de texto reconocido mundialmente.

4.6.2 Validación y confiabilidad del instrumento

Luego de elaborarse el instrumento, este se somete a una validación de expertos que validarán su confiabilidad en base a los criterios de: Relevancia, coherencia, suficiencia y claridad, tal y como lo explica Supo (2021, p. 52). Para tal efecto, se utilizará el Anexo 10 titulado "Validación de Instrumento" aprobado por la Escuela de Posgrado de la Universidad Nacional Hermilio Valdizán para que cinco expertos evalúen el instrumento.

4.6.3 Virtualización del del instrumento

Validado el instrumento se procedió a su digitalización, que siguiendo el concepto brindado por Kyocera (2020, p, 1) consiste en convertir dichos datos a un formato digital, a fin de que pueda ser completando por los encuestados a través de internet, para dicho fin se ha seleccionado la aplicación Microsoft Forms, programa perteneciente a la empresa Microsoft (2021, p. 1) que brinda suficiente seguridad y confiabilidad de que se puedan recabar, almacenar y transportar virtualmente los datos de la aplicación del instrumento.

4.6.4 Aplicación del instrumento

Se habilitó desde la plataforma Microsoft Forms el cuestionario virtual para que los operadores jurídicos considerados dentro de la muestra puedan completarlo, proceso que fue permanentemente monitoreado por el investigador para asegurar el registro de las respuestas.

4.6.5 Exportación de los datos recabados

Finalizada la fase de aplicación del instrumento, se procedió a exportar la integridad de los datos recabados del programa Microsoft Forms al programa Microsoft Excel en el formato de hoja de cálculo para su posterior tabulación y análisis, en ese sentido recordemos que conforme lo explica el Proyecto Descartes (Proyecto Descartes, 2020), es en esta etapa en la cual se harán las representaciones gráficas correspondientes.

4.7 Aspectos éticos

Para la realización del presente estudio se contó con el consentimiento informado de los participantes a quienes se les aplicará el instrumento de investigación, de igual forma en el caso de aquellos que laboren en instituciones públicas se contará con también con la autorización expresa de la autoridad competente, pues los datos a recabar serán estrictamente académicos y serán utilizados solo con fines de investigación.

CAPÍTULO V
RESULTADOS Y DISCUSIÓN

5.1 Análisis Descriptivo

Tabla 6

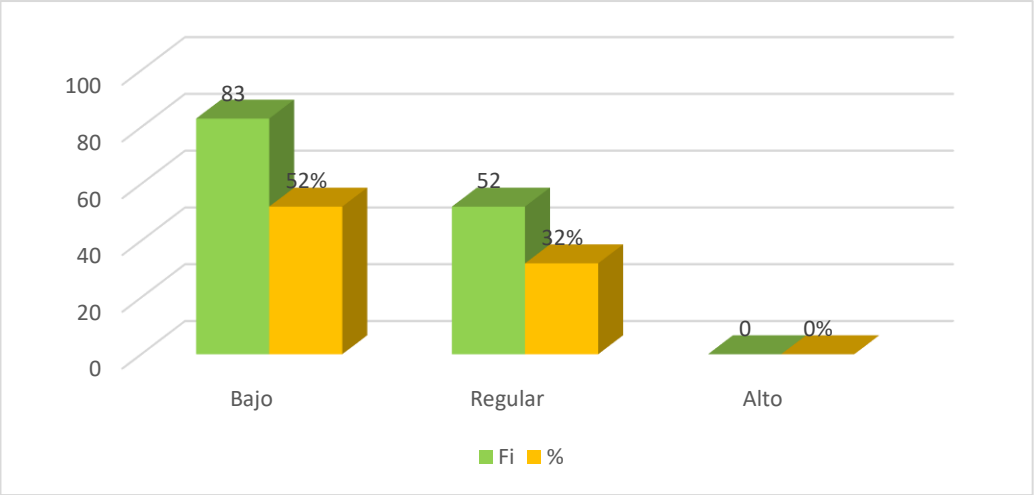
Niveles predominantes de las competencias en ciberseguridad del operador jurídico del distrito fiscal de Huánuco durante el periodo 2020

Niveles predominantes de las competencias en ciberseguridad del operador jurídico	**Abogados**		**Fiscales**		**Jueces**	
	Fi	**%**	**Fi**	**%**	**Fi**	**%**
Bajo (0-20)	83	52%	12	7%	6	4%
Regular (21-40)	52	32%	8	5%	0	0%
Alto (41-60)	0	0%	0	0%	0	0%
Total	**135**	**84%**	**20**	**12%**	**6**	**4%**

Nota. Resultados de la aplicación de los instrumentos de investigación

Figura 1

Niveles predominantes de las competencias en ciberseguridad del operador jurídico en los abogados del distrito fiscal de Huánuco durante el periodo 2020

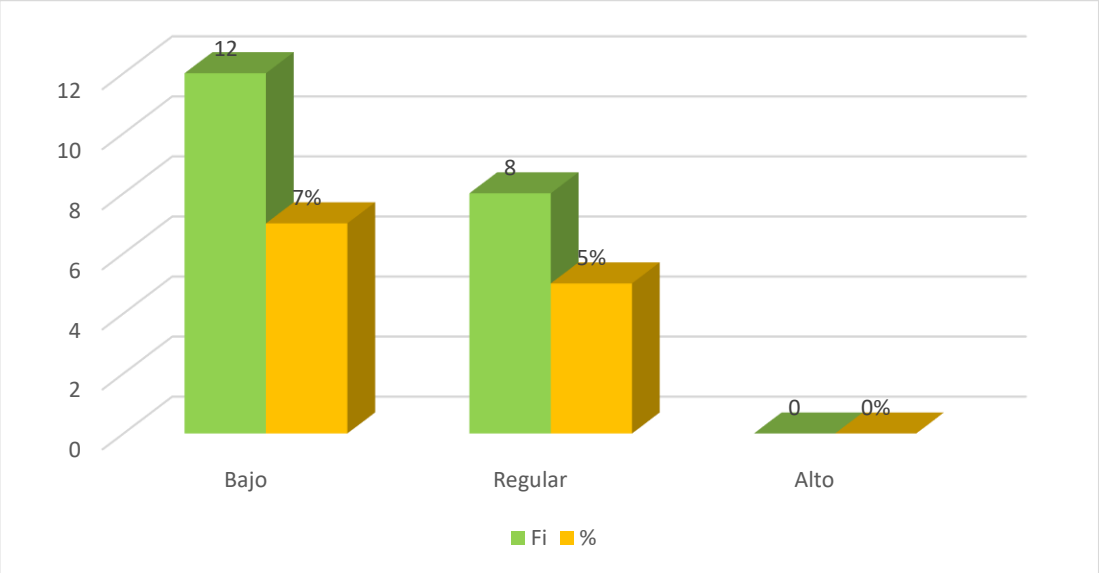


Nota. Resultados de la aplicación del instrumento de investigación

En la figura 1, se evidencia que el 52% de los abogados presentan un bajo nivel respecto a las competencias en ciberseguridad como el reconocimiento de tecnologías en ciberseguridad; así como la identificación, aplicación de procedimientos y respuesta ante las incidencias en ciberseguridad. Mientras que un 32% de los abogados evidencian un nivel regular respecto a las competencias en ciberseguridad. Entre tanto ningún abogado presenta un nivel alto.

Figura 2

Niveles predominantes de las competencias en ciberseguridad del operador jurídico en los fiscales del distrito fiscal de Huánuco durante el periodo 2020

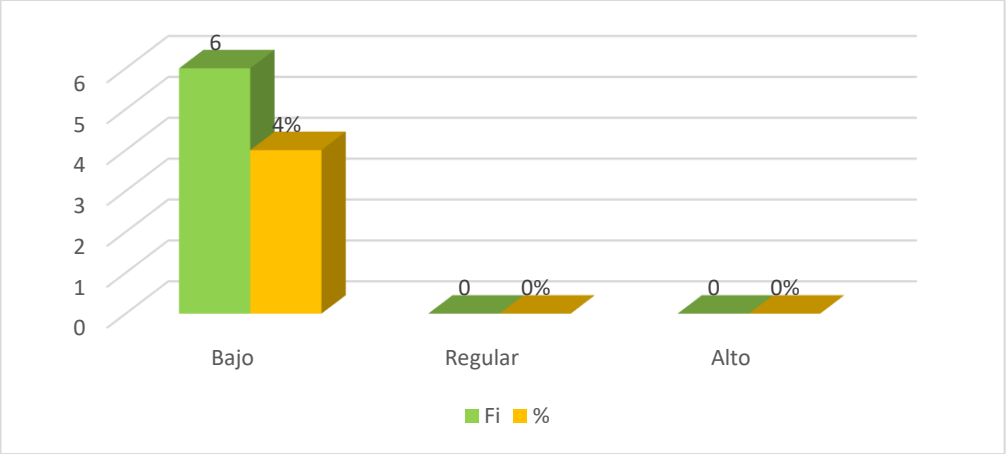


Nota. Resultados de la aplicación del instrumento de investigación

En la figura 2, se evidencia que el 7% de los fiscales presentan un bajo nivel respecto a las competencias en ciberseguridad como el reconocimiento de tecnologías en ciberseguridad; así como la identificación, aplicación de procedimientos y respuesta ante las incidencias en ciberseguridad. Mientras que un 5% de los fiscales evidencian un nivel regular respecto a las competencias en ciberseguridad. Entre tanto ningún fiscal presenta un nivel alto.

Figura 3

Niveles predominantes de las competencias en ciberseguridad del operador jurídico en los jueces del distrito fiscal de Huánuco durante el periodo 2020



Nota. Resultados de la aplicación del instrumento de investigación

En la figura 3, se evidencia que el 4% de los jueces presentan un bajo nivel respecto a las competencias en ciberseguridad como el reconocimiento de tecnologías en ciberseguridad; así como la identificación, aplicación de procedimientos y respuesta ante las incidencias en ciberseguridad. Mientras que ningún juez presenta un nivel regular o alto respecto a las competencias en ciberseguridad.

Tabla 7

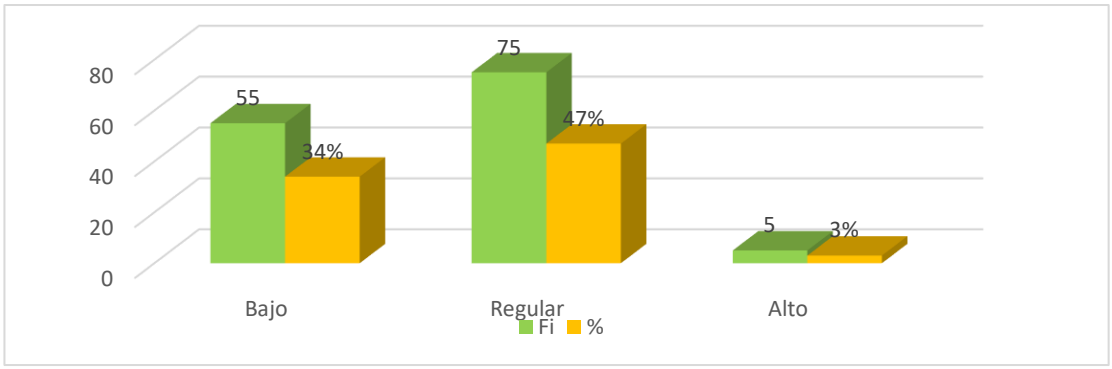
Niveles predominantes de la investigación penal de delitos informáticos del distrito fiscal de Huánuco durante el periodo 2020

Niveles predominantes de la investigación penal de delitos informáticos	**Abogados**		**Fiscales**		**Jueces**	
	Fi	**%**	**Fi**	**%**	**Fi**	**%**
Bajo (0-20)	55	34%	11	7%	5	3%
Regular (21-40)	75	47%	9	5%	1	1%
Alto (41-60)	5	3%	0	0%	0	0%
Total	**135**	**84%**	**20**	**12%**	**6**	**4%**

Nota. Resultados de la aplicación del instrumento de investigación.

Figura 4

Niveles predominantes de la investigación penal de delitos informáticos en los abogados del distrito fiscal de Huánuco durante el periodo 2020

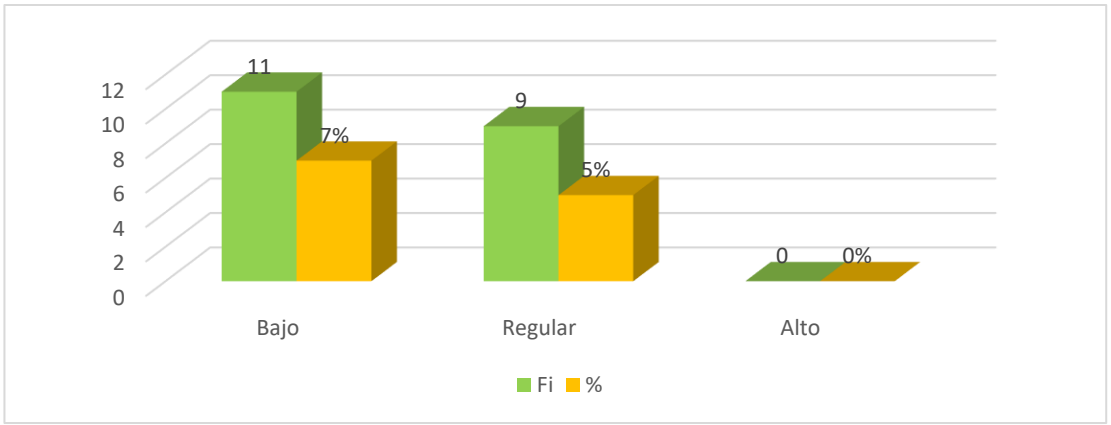


Nota. Resultados de la aplicación del instrumento de investigación

En la figura 4, se evidencia que el 47% de los abogados presentan un nivel regular respecto a la investigación penal de ciberdelitos como la investigación penal de delitos que afectan los datos informáticos, sistemas informáticos y otros bienes jurídicos de relevancia penal mediante la utilización de las tecnologías de la información y las comunicaciones. Mientras que un 34% de los abogados evidencian un nivel bajo respecto a las competencias en ciberseguridad. Entre tanto un 3% de los abogados presenta un nivel alto.

Figura 5

Niveles predominantes de la investigación penal de delitos informáticos en los ficales del distrito fiscal de Huánuco durante el periodo 2020

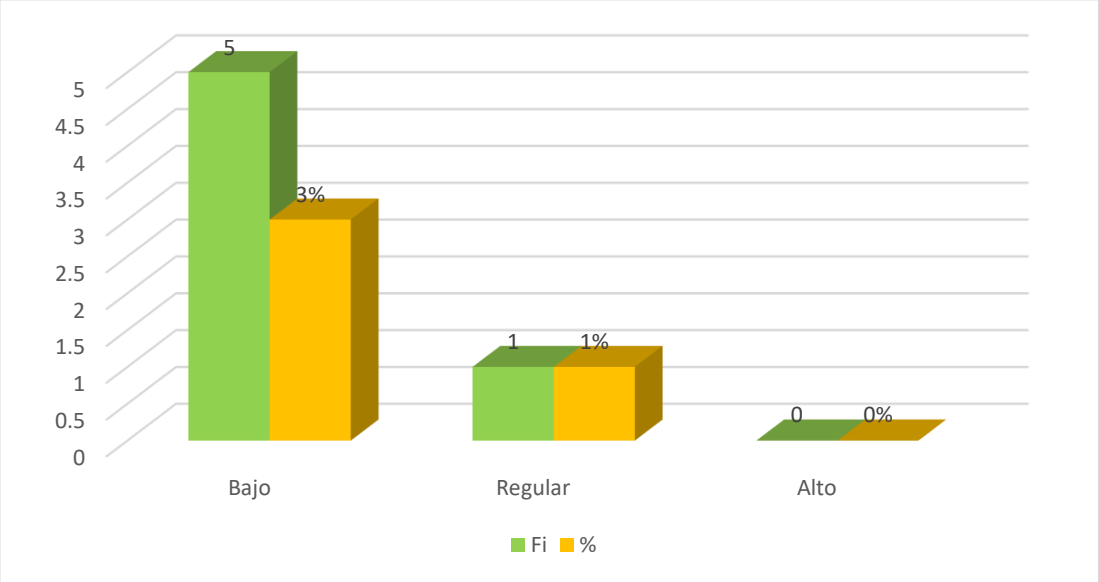


Nota. Resultados de la aplicación del instrumento de investigación

En la figura 5, se evidencia que el 7% de los ficales presentan un nivel bajo respecto a la investigación penal de ciberdelitos como la investigación penal de delitos que afectan los datos informáticos, sistemas informáticos y otros bienes jurídicos de relevancia penal mediante la utilización de las tecnologías de la información y las comunicaciones. Mientras que un 5% de los fiscales evidencian un nivel regular respecto a las competencias en ciberseguridad. Entre tanto, ningún fiscal presenta un nivel alto.

Figura 6

Niveles predominantes de la investigación penal de delitos informáticos en los abogados del distrito fiscal de Huánuco durante el periodo 2020



Nota. Resultados de la aplicación del instrumento de investigación

En la figura 6, se evidencia que el 3% de los jueces presentan un nivel bajo respecto a la investigación penal de ciberdelitos como la investigación penal de delitos que afectan los datos informáticos, sistemas informáticos y otros bienes jurídicos de relevancia penal mediante la utilización de las tecnologías de la información y las comunicaciones. Mientras que un 1% de los jueces evidencian un nivel regular respecto a las competencias en ciberseguridad. Entre tanto, ningún juez presenta un nivel alto.

5.2 Análisis Inferencial y/o contrastación de hipótesis

Tabla 8

Prueba de normalidad

Pruebas de normalidad			
	Kolmogorov-Smirnov[a]		
	Estadístico	gl	Sig.
Competencias en ciberseguridad del operador jurídico	,169	161	,000
Investigación penal de ciberdelitos	,209	161	,000

Nota. Resultados de la aplicación de los instrumentos de investigación

Sobre la tabla 8, acerca de la prueba de normalidad, se observa que los datos de normalidad de Kolmogorov-Smirnov, el cual se utiliza para muestras mayores a 50 (n=161). Se evidencia un p valor de ,000 en las competencias en ciberseguridad del operador jurídico, en tanto en la investigación penal de ciberdelitos se evidencia un p valor de ,000, siendo estos datos menores al nivel de significancia (**α:** 0,05); ello evidenciaría que los datos no tienen una distribución normal, por lo que se utilizara el estadístico de correlación no paramétrico Rho de Spearman.

Tabla 9

Correlación entre las competencias en ciberseguridad del operador jurídico y la investigación penal de delitos informáticos

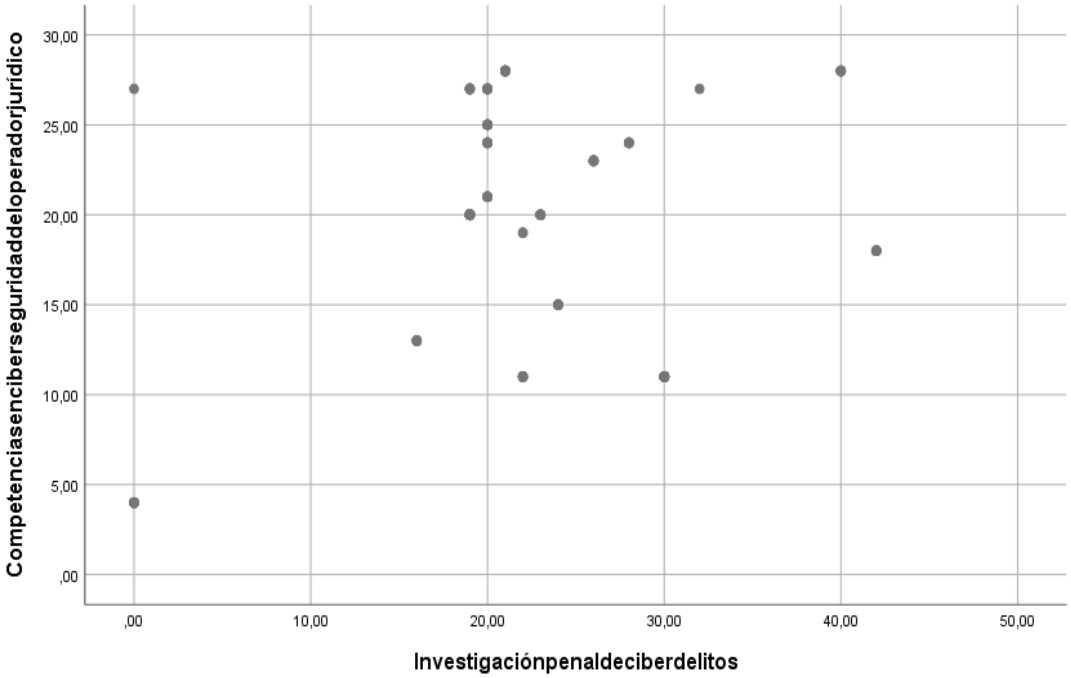
			Investigación penal de ciberdelitos
Rho de Spearman	Competencias en ciberseguridad del operador jurídico	Coeficiente de correlación	-,164*
		Sig. (bilateral)	,038
		N	161

*. La correlación es significativa en el nivel 0,05 (bilateral).

Acerca de la tabla 9, se observa que la correlación de Rho de Spearman es de -,164*, lo cual indicaría que la correlación es negativa muy baja. Así mismo se observa un sig. bilateral (p-valor) de ,038 siendo este menor al **α:** 0.05, lo cual indica que se rechaza la hipótesis nula y se acepta la hipótesis alterna, es decir: Las competencias en ciberseguridad del operador jurídico se relacionan con la investigación penal de delitos informáticos en el distrito fiscal de Huánuco durante el periodo 2020.

Figura 7

Plano cartesiano



Nota. Resultados de la aplicación de los instrumentos de investigación

Acerca de la figura 7, se observa que la correlación es nula. Así mismo que la fuerza de correlación es muy débil pues los datos se encuentran dispersos en el plano cartesiano.

Tabla 10

Correlación entre el reconocimiento de tecnologías para la seguridad de la información por el operador jurídico y la investigación penal de delitos informáticos

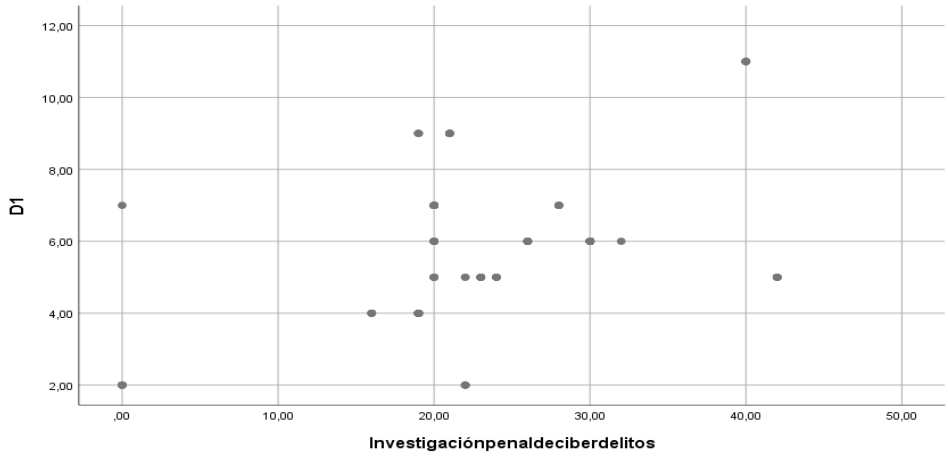
			Investigación penal de ciberdelitos
Rho de Spearman	Reconocimiento de tecnologías para la seguridad de la información por el operador jurídico	Coeficiente de correlación	,457**
		Sig. (bilateral)	,000
		N	161

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

Acerca de la tabla 10, se observa que la correlación de Rho de Spearman es de ,457**, lo cual indicaría que existe una correlación positiva moderada. Así mismo se observa un sig. bilateral (p-valor) de ,000 siendo este menor al **α:** 0.05, lo cual indica que se rechaza la hipótesis nula y se acepta la hipótesis alterna, es decir: El reconocimiento de tecnologías para la seguridad de la información por el operador jurídico se relaciona con la investigación penal de ciberdelitos en el distrito fiscal de Huánuco durante el periodo 2020.

Figura 8

Plano cartesiano



Nota. Resultados de la aplicación de los instrumentos de investigación

Acerca de la figura 8, se observa que la correlación es positiva moderada. Así mismo que la fuerza de correlación es buena pues los datos se encuentran cercanos en el plano cartesiano.

Tabla 11

Correlación entre la aplicación de procedimientos para la seguridad de la información en el ciberespacio por el operador jurídico y la investigación penal de delitos informáticos

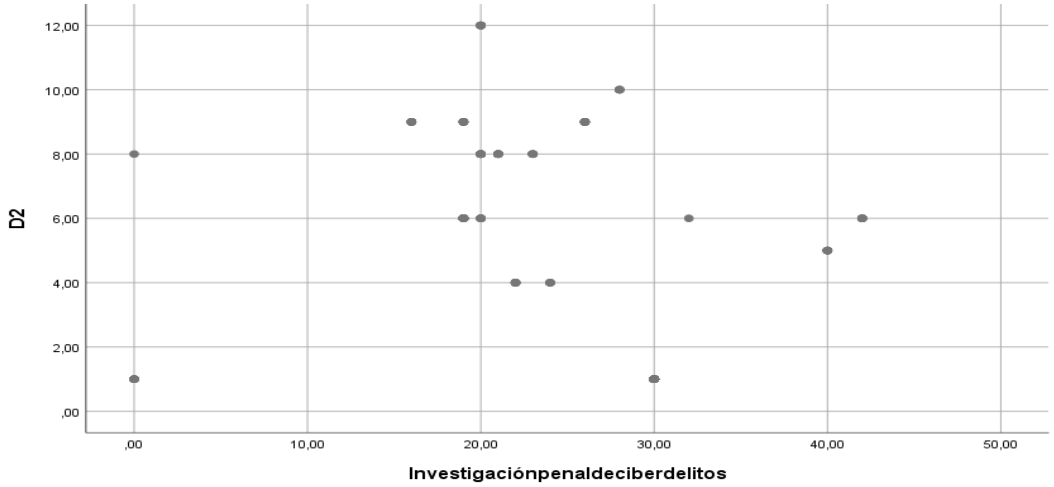
			Investigación penal de ciberdelitos
Rho de Spearman	Aplicación de procedimientos para la seguridad de la información en el ciberespacio por el operador jurídico	Coeficiente de correlación	-,410**
		Sig. (bilateral)	,000
		N	161

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

Acerca de la tabla 11, se observa que la correlación de Rho de Spearman es de -,410**, lo cual indicaría que existe una correlación negativa moderada. Así mismo se observa un sig. bilateral (p-valor) de ,000 siendo este menor al ***α*:** 0.05, lo cual indica que se rechaza la hipótesis nula y se acepta la hipótesis alterna, es decir: La aplicación de procedimientos para la seguridad de la información en el ciberespacio por el operador jurídico se relaciona con la investigación penal de ciberdelitos en el distrito fiscal de Huánuco durante el periodo 2020.

Figura 9

Plano cartesiano



Nota. Resultados de la aplicación de los instrumentos de investigación

Acerca de la figura 9, se observa que la correlación es negativa modera. Así mismo que la fuerza de correlación es buena pues los datos se encuentran cercanos en el plano cartesiano.

Tabla 12

Correlación entre la identificación de incidentes de seguridad de la información en el ciberespacio por el operador jurídico y la investigación penal de delitos informáticos

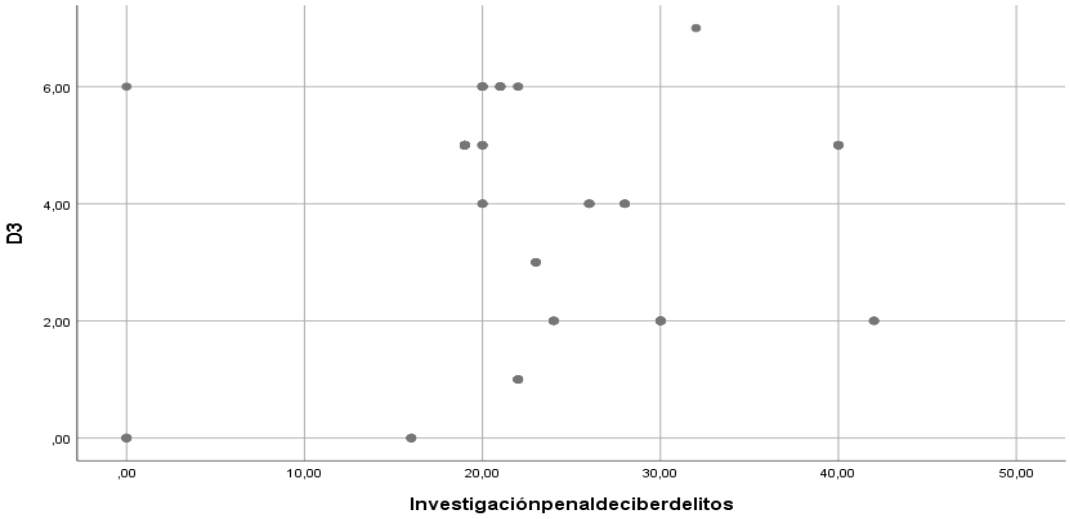
			Investigación penal de ciberdelitos
Rho de Spearman	Identificación de incidentes de seguridad de la información en el ciberespacio por el operador jurídico	Coeficiente de correlación	-,260**
		Sig. (bilateral)	,001
		N	161

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

Acerca de la tabla 12, se observa que la correlación de Rho de Spearman es de -,260**, lo cual indicaría que existe una correlación negativa baja. Así mismo se observa un sig. bilateral (p-valor) de ,001 siendo este menor al **α:** 0.05, lo cual indica que se rechaza la hipótesis nula y se acepta la hipótesis alterna, es decir: La identificación de incidentes de seguridad de la información en el ciberespacio por el operador jurídico se relaciona con la investigación penal de ciberdelitos en el distrito fiscal de Huánuco durante el periodo 2020.

Figura 10

Plano cartesiano



Nota. Resultados de la aplicación de los instrumentos de investigación

Acerca de la figura 10, se observa que la correlación es negativa baja. Así mismo que la fuerza de correlación es débil pues los datos se encuentran dispersos en el plano cartesiano.

Tabla 13

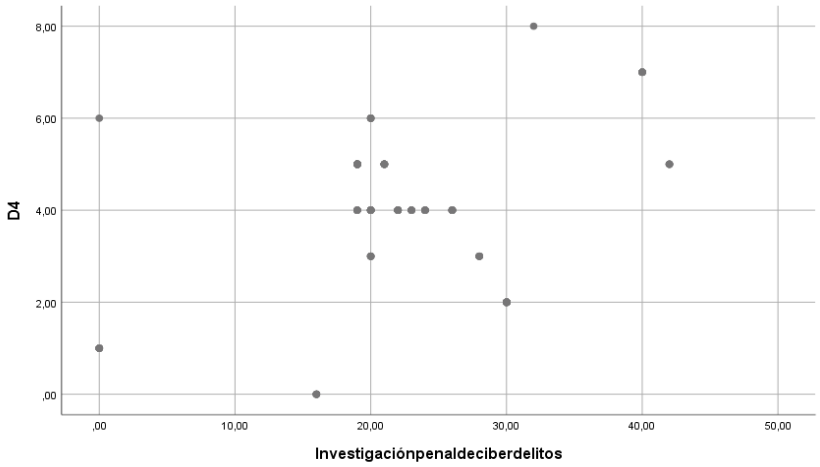
Correlación entre la respuesta a incidentes de seguridad de la información en el ciberespacio por el operador jurídico y la investigación penal de delitos informáticos

			Investigación penal de ciberdelitos
Rho de Spearman	Respuesta a incidentes de seguridad de la información en el ciberespacio por el operador jurídico	Coeficiente de correlación	-,126
		Sig. (bilateral)	,111
		N	161

Acerca de la tabla 13, se observa que la correlación de Rho de Spearman es de -,126**, lo cual indicaría que la correlación es negativa muy baja. Así mismo se observa un sig. bilateral (p-valor) de ,111 siendo este mayor al **α:** 0.05, lo cual indica que se rechaza la hipótesis alterna y se acepta la hipótesis nula, es decir: La respuesta a incidentes de seguridad de la información en el ciberespacio por el operador jurídico no se relaciona con la investigación penal de ciberdelitos en el distrito fiscal de Huánuco durante el periodo 2020.

Figura 11

Plano cartesiano



Nota. Resultados de la aplicación de los instrumentos de investigación

Acerca de la figura 11, se observa que la correlación es nula. Así mismo que la fuerza de correlación es muy débil pues los datos se encuentran dispersos en el plano cartesiano.

5.3 Discusión de Resultados

Conforme lo explican Ñaupas et al (2018) la discusión de los resultados significa analizar su calidad en base a un sentido crítico, autocrítico y con conocimiento de otros estudios que se hayan realizado, en ese sentido se plantean nueve interrogantes que permitirán realizar dicho análisis.

5.3.1 Sobre la confiabilidad de los resultados presentados

En primer orden, habiéndose presentado los resultados, emerge la interrogante sobre su confiabilidad, por lo que a fin de dar una valoración positiva a los datos que se hayan recabado, se debe de tener en consideración que en la preparación del presente estudio, se elaboró un instrumento cuya confiabilidad fue debidamente evaluada, así mismo, se plasmó dicho instrumento de investigación en la plataforma virtual Microsoft Forms, a fin de recabar los datos con ese servicio de la reconocida y mundialmente famosa Microsoft, y de la cual se asegura los fallos en sus sistemas son con menor frecuencia.

De otro lado, es importante también sustentar la confiabilidad en base al hecho de que, para la aplicación del instrumento, el investigador tuvo que solicitar de manera formal a los funcionarios de entidades como el Ministerio Público y Poder Judicial a fin de que autoricen la aplicación del presente instrumento.

En consecuencia, si se solicitó y recabó previa solicitud de permiso a las entidades en donde laboran parte de los operadores jurídicos que forman parte de este estudio, y se aplica un instrumento previamente evaluado apoyado en un servicio informático que asegura una baja posibilidad de fallos, entonces se puede asumir de que los datos recabados son confiables.

5.3.2 Limitaciones en la presentación de los resultados

Para la presentación de los resultados, el estudio no estuvo exento de limitaciones, el primero de ellos fue la burocracia estatal, ya que para poder aplicar las encuestas de manera efectiva y satisfactoria fue necesario cursar solicitud tanto al Ministerio Público como al Poder Judicial a fin de que autorizaran la aplicación de dicho instrumento de investigación, no obstante, la respuesta a dicha solicitudes se tardaba, fue necesario reiterarlas a fin de que se les diera la debida atención.

También fue una limitante la brecha digital generacional que se advirtió en los operadores jurídicos encuestados, los mismos tuvieron dificultades para acceder al enlace con el cual se accedía al instrumento de investigación, como también al momento de rellenarlo, un aspecto que aunque previsto fue mas recurrente a lo proyectado, por lo que se tuvo que imprimir en muchos casos el instrumento a fin de que en forma física se pueda recabar los datos.

5.3.3 Efecto de las limitaciones en los resultados

Pese a las limitaciones encontradas, los efectos en los resultados fueron mínimos, ya que se pudo recabar el número suficiente de datos para poder analizarlos y presentarlos resultados satisfactoriamente, no obstante a nivel temporal si hubo un efecto adverso ya que se alteraron los tiempos que se habían cronogramado inicialmente en el proyecto, también es importante recalcar que aunque la cantidad de datos fue suficiente, ello no significa que se haya recabados todos los que se habían proyectado.

5.3.4 Generalización de los resultados en otros contextos similares

Los resultados obtenidos si pueden ser generalizados a otros contextos similares, ya que a nivel espacial se obtuvo información sobre los operadores jurídicos de todo un distrito fiscal, cuyo contexto geográfico, jurídico, social y criminal es similar al de muchos otros distritos fiscales del Perú.

5.3.5 Generalización de los resultados en otros contextos similares

Aunque los resultados pueden ser generalizados a otros contextos, ello no ocurre en cuanto a su aplicación, debido a que el fenómeno de la ciberdelincuencia es variado en el Perú, en donde por las brechas digitales existen distritos fiscales en los cuales existe una mayor o menor incidencia de ciberdelitos, en ese sentido, los resultados de la presente investigación resultarían aplicables solo a aquellos distritos fiscales cuya situación de ciberdelincuencia tenga una magnitud semejante.

5.3.6 Comparación con estudios previos

Respecto de los estudios hallados a nivel internacional:

- En cuanto al estudio realizado por Rodríguez (2021), los resultados mostraron la importancia de que los operadores jurídicos comprendan respecto de los riesgos del ciberespacio y desarrollen competencias profesionales para abordarlos, en especial cuando forman parte de procesos penales en donde se investigan casos de ciberdelitos.
- En cuanto al estudio realizado por Montgomery (2017), los resultados mostraron la importancia de las competencias en ciberseguridad para los operadores jurídicos que laboran en instituciones como el Ministerio Público o Poder Judicial, entidades cuyo esquema organizativo contempla contar con personal que opere y preste asistencia a los sistemas informáticos, como también se ocupen de elaborar los marcos de ciberseguridad que permitan capacitar al personal en la prevención, tratamiento y respuesta ante la ocurrencia de un incidente informático.
- En cuanto al estudio realizado por Lundquist (2016), los resultados obtenidos mostraron que los operadores jurídicos contemplan la aplicación de procedimientos de ciberseguridad, lo cual resulta también aplicable en la informática forense, en especial cuando se trata de recabar evidencia digital.
- En cuanto al estudio realizado por Caamaño & Gil (2020) los resultados obtenidos mostraron que los operadores jurídicos contemplan la aplicación de procedimientos de ciberseguridad.

Respecto de los estudios hallados a nivel nacional:

- En cuanto al estudio realizado por Rossi (2021), los resultados obtenidos mostraron que al año 2020, ya se advierte que el mayor uso de las tecnologías de la información de la información por parte del Estado esta trayendo una mayor concientización en el uso de herramientas de ciberseguridad, aunque ello aún no se sea en la forma y niveles adecuados.
- En cuanto al estudio realizado por Ornachea (2019), los resultados que se obtuvieron mostraron que en efecto los operadores muestran tener cierto grado de conciencia respecto de que el uso del ciberespacio y las facilidades que presenta a la vez que permite reducir brechas, también es una apertura para que los ciberdelincuentes lo aprovechen en un sentido negativo.
- En cuanto al estudio realizado por Huamatingo (2022), los resultados obtenidos mostraron que los operadores jurídicos ya cuentan con cierto conocimiento de que el análisis de las vulnerabilidades digitales incluye la gestión de vulnerabilidades, la metodología para el análisis y la tecnología defensiva.

Respecto de los estudios hallados a nivel local:

- En cuanto al estudio realizado por Sandoval (2020) y los resultados obtenidos mostraron que de forma muy elemental los operadores jurídicos pueden comprender las implicancias de las amenazas internas y externas a las cuales están expuestas sus organizaciones en materia de ciberseguridad.
- En cuanto al estudio realizado por Vilca (2018) y los resultados obtenidos mostraron que en efecto los operadores jurídicos son conscientes en cierta forma de que deben mantenerse constantemente actualizados en cuanto a las nuevas tecnologías, a fin de poder confrontar riesgos en materia de ciberseguridad y sus implicancias en la investigación de los ciberdelitos.

5.3.7 Sobre la comprobación de las hipótesis

El estudio contempló la formulación de una hipótesis general y cuatro hipótesis específicas, de las cuales si partimos de la general tenemos que con un de Rho de Spearman es de -,164 se halló que existe una correlación negativa muy baja entre las competencias en ciberseguridad del operador jurídico y la investigación penal de

delitos informáticos, y al tenerse una sig. bilateral (p-valor) de ,038 siendo este menor al **α:** 0.05, se rechazó la hipótesis nula y se aceptó la hipótesis alterna.

En cuanto a la primera hipótesis específica, con un Rho de Spearman es de ,457 se halló que existe una correlación positiva moderada entre el reconocimiento de tecnologías para la seguridad de la información por el operador jurídico y la investigación penal de delitos informáticos, y al tenerse una sig. bilateral (p-valor) de ,000 siendo este menor al **α:** 0.05, se rechazó la hipótesis nula y se aceptó la hipótesis alterna.

En cuanto a la segunda hipótesis específica, con un Rho de Spearman de -,410 se halló que existe una correlación negativa moderada entre la aplicación de procedimientos para la seguridad de la información en el ciberespacio por el operador jurídico y la investigación penal de delitos informáticos, y al tenerse una sig. bilateral (p-valor) de ,000 siendo este menor al **α:** 0.05, se rechazó la hipótesis nula y se aceptó la hipótesis alterna.

Sobre la tercera hipótesis, con un Rho de Spearman es de -,260 se halló que existe una correlación negativa baja entre la identificación de incidentes de seguridad de la información en el ciberespacio por el operador jurídico y la investigación penal de delitos informáticos, y al tenerse una sig. bilateral (p-valor) de ,001 siendo este menor al **α:** 0.05, se rechazó la hipótesis nula y se aceptó la hipótesis alterna.

Finalmente, respecto de la cuarta hipótesis, con un Rho de Spearman es de -,260, se halló que existe una correlación nula entre la respuesta a incidentes de seguridad de la información en el ciberespacio por el operador jurídico y la investigación penal de delitos informáticos, y al tenerse una sig. bilateral (p-valor) de ,111 siendo este mayor al **α:** 0.05 se rechazó la hipótesis alterna y se aceptó la hipótesis nula.

5.4 Aporte científico de la investigación

La relación del derecho y la informática resulta en la actualidad un tema de mucho interés para el ámbito académico, ya sea porque la informática viene siendo

aplicada ampliamente en las instituciones públicas y privadas a fin de modernizar sus procesos, o porque el derecho al abordar el campo de la informática se ocupa del estudio de nuevos fenómenos sociales como por ejemplo el de la criminalidad (cuando nos abocamos al ámbito del derecho penal). En ese sentido, en este estudio se ha abordado que el nuevo paradigma para los operadores jurídicos en general conlleva el dominio de ciertas competencias profesionales que les permitan desenvolverse en este nuevo contexto, y en el que en muchos casos resultará suficiente con el dominio de competencias profesionales en informática básica, las cuales ya sean impartidas en la educación básica o profesional, permitirán al operador jurídico poder aprovechar en cierta medida las nuevas innovaciones tecnologías, dejando el aspecto técnico para los especialistas en informática.

No obstante, afirmar que un aspecto técnico como es el de la ciberseguridad, es exclusiva de los profesionales especialistas en la materia, resulta discutible, ya que desde el aspecto teórico se ha desarrollado ampliamente que la gestión de riesgos en el ciberespacio es un tema que incumbe a todos los miembros dentro de una organización, lo cual incluye a los operadores jurídicos, que podrían contar competencias en dicha materia también, sin embargo este argumento resulta para muchos difuso y poco claro, y se inclinan más en que el operador jurídico únicamente necesita contar con competencias profesionales básicas en informática.

En base a lo mencionado, es que se puede fundamentar el aporte de la presente investigación, considerando que si bien es cierto resulta polémico afirmar que todo operador jurídico debe contar con competencias en ciberseguridad, tiene más sentido lógico esta afirmación si se aplica en el ámbito del derecho penal, y en específico cuando se trata de ciberdelitos, que se caracterizan principalmente por ese componente técnico que dificulta muchas veces su investigación, en ese sentido de la revisión de los antecedentes y la revisión teórica, ya se había encontrado indicios de que esta correlación existía, no obstante con el presente estudio, aplicando el método científico se ha hallado de que la correlación entre las competencias en ciberseguridad del operador jurídico y la investigación penal de delitos informáticos existe efectivamente, y aunque desde el enfoque estadístico, no se trate de una correlación perfecta, el

resultado obtenido constituye un aporte significativo que puede servir de base para futuras investigaciones que ahonden más en este tema.

CONCLUSIONES

1. Se concluye que las competencias en ciberseguridad del operador jurídico y la investigación penal de ciberdelitos si se correlacionan, y que de acuerdo a los datos recabados sería negativa y muy baja (Rho de Spearman), por lo que en base a este resultado se puede afirmar de que todo operador jurídico, sea en su rol de abogado, juez o fiscal, deberá contar con competencias en ciberseguridad que le permitan abordar los incidentes de seguridad informática que se puedan producir en la investigación de ciberdelitos durante la etapa procesal correspondiente.
2. Se concluye que la competencia profesional en el reconocimiento de tecnologías para la seguridad de la información por el operador jurídico y la investigación penal de ciberdelitos si se correlacionan, y que de acuerdo a los datos recabados sería positiva y moderada (Rho de Spearman), por lo que en base a este resultado se puede afirmar de que todo operador jurídico debe de ser competente en identificar dentro de una investigación penal de ciberdelitos, aquellas tecnologías que permitirán asegurar la información en el ciberespacio, lo cual a su vez le permitirá prevenir futuros incidentes de seguridad informática.
3. Se concluye que la competencia en profesional en la aplicación de procedimientos para la seguridad de la información en el ciberespacio por el operador jurídico y la investigación penal de ciberdelitos si se correlacionan, y que de acuerdo a los datos recabados sería una correlación negativa y moderada (Rho de Spearman), por lo que en base a este resultado se puede afirmar de que pese a que aplicación de dichos procedimientos son generalmente responsabilidad los especialistas en informática que se encuentren a cargo, el operador jurídico debe ser competente en la aplicación de procedimientos para el aseguramiento de la seguridad de la información durante la investigación de ciberdelitos, una cuestión que en base a la revisión teórica realizada, resulta determinante para evitar futuros incidentes de ciberseguridad.
4. Se concluye que la competencia profesional en la identificación de incidentes de seguridad de la información en el ciberespacio por el operador jurídico y la investigación penal de ciberdelitos si se correlacionan, y que de acuerdo a los datos recabados sería una correlación correlación negativa y baja (Rho de Spearman), por lo que en base a este resultado se puede afirmar de que pese a que la

identificación de incidentes de seguridad informática son exclusiva labor del área especializada y/o profesional dentro de cualquier , el operador jurídico debe tener dominio de esta competencia, ya que resultará de mucha ayuda en la prevención de incidentes de ciberseguridad en los cuales sea competente en identificar su ocurrencia, tanto más cuando se trata de la investigación de ciberdelitos, en donde los incidentes podrían ser más recurrentes.

5. Se concluye que la competencia profesional en la respuesta a incidentes de seguridad de la información en el ciberespacio por el operador jurídico y la investigación penal de ciberdelitos no se correlacionan, ya que de acuerdo a los datos recabados sería una correlación nula (Rho de Spearman), lo cual se explicaría en la concepción de que la respuesta a estos incidentes, son una cuestión técnica propia de especialistas en ciberseguridad, en ese sentido, de la revisión teórica no se encuentra mucha evidencia de la forma en que el operador jurídico podría dar respuesta a incidentes de seguridad informática durante la investigación de un ciberdelito, no obstante, es menester mencionar que pese a este resultado, dicha competencia forma parte del perfil laboral de un trabajador técnico y/o profesional de cualquier organización en países desarrollados, por lo que se entiende que pese a su complejidad técnica no es exclusiva de especialistas, y en consecuencia puede (y debería) formar parte del perfil profesional de los operadores jurídicos (más aún si de investigar ciberdelitos se trata).

SUGERENCIAS

1. Partiendo de las conclusiones, se recomienda en primer lugar, ahondar más en la investigación de las variables del estudio realizado, en especial en lo relativo a la ciberseguridad, ya que a la fecha es un tema que se trata aún de forma muy superficial dentro del ámbito del derecho.
2. Se recomienda revisar el marco jurídico actual en seguridad informática a fin identificar qué normas resultan mejorables en relativo a la ciberseguridad, pues, aunque el tema se viene abordando como mayor frecuencia en el Perú, en comparación con otros países, el actual marco jurídico contiene muchas normas que contiene aspectos anticuados que deben actualizarse a fin de alcanzar una mejora.
3. Se recomienda a las universidades peruanas realizar mejoras a las currículas de estudio de las facultades de derecho, a fin de que se contemple no solo la preparación de los futuros operadores jurídicos con competencias en informática, sino también en seguridad informática y ciberseguridad.
4. Se recomienda al Ministerio Público y Poder Judicial dar mayor preponderancia al aspecto de la seguridad informática, esto en razón de que ambas instituciones tienen un rol fundamental en la investigación de ciberdelitos, en ese sentido, no solo se recomienda que las áreas especializadas aborden el tema de la ciberseguridad como parte de su responsabilidad (por ejemplo a través de la elaboración de los marcos de gestión de la ciberseguridad), sino que ese abordaje preste real relevancia a la capacitación del personal que labora en dichas instituciones, a fin de que todas las partes coadyuven en prevenir incidentes de seguridad informática.
5. Se recomienda al Estado peruano abordar con mayor interés todo lo relacionado a la ciberseguridad, ya que a la fecha los reportes internacionales muestran que el Perú aunque ha dado paso importantes en ciberseguridad, como Estado sigue siendo muy vulnerable para la ciberdelincuencia, lo cual puede tener resultados catastróficos.

REFERENCIAS

Acurio, S. (12 de septiembre de 2020). *Delitos Informáticos: Generalidades.* Obtenido de https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf.

Agencia de la Unión Europea para la Cooperación Policial. (12 de diciembre de 2021). *Cybercrime*. Obtenido de https://www.europol.europa.eu/crime-areas-and-statistics/crime-areas/cybercrime

Andina. (23 de enero de 2019). *Perú se suscribe a convenio de Budapest en materia de ciberseguridad y ciberdefensa.* Obtenido de https://andina.pe/agencia/noticia-peru-suscribira-convenio-budapest-materia-ciberseguridad-y-ciberdefensa-740180.aspx

Andina. (4 de septiembre de 2021). *Denuncias por delitos informáticos se incrementaron en 92.9% durante el último año.* Obtenido de https://andina.pe/agencia/noticia-denuncias-delitos-informaticos-se-incrementaron-929-durante-ultimo-ano-908177.aspx

Banco Mundial. (15 de julio de 2021). *Banco Mundial.* Obtenido de https://datos.bancomundial.org/indicator/IT.NET.USER.ZS?end=2019&start=1960&view=chart

BID. (2020). *Reporte Ciberseguridad 2020: riesgos, avances y el camino a seguir en América Latina y el Caribe.* Obtenido de https://publications.iadb.org/es/reporte-ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-america-latina-y-el-caribe

Business Insider . (12 de noviembre de 2020). *Los delitos informáticos ocasionaron en 2019 pérdidas superiores al 1% del PIB mundial, por encima de los 800.000 millones de euros*. Obtenido de https://www.businessinsider.es/impacto-ciberdelitos-ya-superior-1-pib-mundial-768519

Caamaño Fernández, E. E. (2020). *Prevención de riesgos por ciberseguridad desde la auditoria forense: conjugando el talento humano organizacional.* Manizales: NOVUM revista de Ciencias Sociales Aplicadas.

Cambridge Dictionary. (11 de octubre de 2021). *Cybercrime*.

Carrasco, D. (2007). *Metodología de la Investigación Científica.* Lima: Editorial San Marcos E.I.R.L.

CISCO. (03 de mayo de 2021). Obtenido de ¿Qué es la ciberseguridad?: https://www.cisco.com/c/es_mx/products/security/what-is-cybersecurity.html

Council of Europe. (2001). *Convenio sobre la ciberdelincuencia.* Obtenido de https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

Decision Analyst. (20 de mayo de 2021). *Free Statistical Software for Marketing Research.* Obtenido de https://www.decisionanalyst.com/download/

Diaz, H. (2009). *El delito informático.* San Sebastián: Revista Eguzkilore.

El Peruano. (30 de diciembre de 2020). *Crean la Unidad Fiscal Especializada en Ciberdelincuencia del Ministerio Público con competencia nacional y designan y nombran Fiscales en el Distrito Fiscal de Lima.* Obtenido de https://busquedas.elperuano.pe/normaslegales/crean-la-unidad-fiscal-especializada-en-ciberdelincuencia-de-resolucion-no-1503-2020-mp-fn-1916745-1/

Employment and Training Administration. (2021). *Cybersecurity Competency Model.* United States Department of Labor.

Federal Bureau of Investigation. (14 de marzo de 2021). *FBI Cyber Crimes Division Career Information.* Obtenido de https://www.fbitraining.org/cyber-crimes/

Galdeano, C., & Valiente, A. (2010). *Competencias profesionales*. Obtenido de SCIELO: http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0187-

893X2010000100004#:~:text=La%20competencia%20se%20puede%20definir,campo%20de%20su%20actividad%20profesional%22.

García, F. (21 de agosto de 2021). *El cuestionario.* Obtenido de http://www.estadistica.mat.uson.mx/Material/elcuestionario.pdf

Hernandez, S., Fernández, C., & Baptista, L. (2014). *Metodología de la Investigación.* México D.F.: Editorial McGraw-Hill/Interamericana Editores S.A.

Huamantingo, R. (2022). *Modelo para el Análisis de Vulnerabilidades Digitales en una entiedad pública.* Lima: Universidad Cesar Vallejo.

Instituto de Ciencias Hegel. (12 de agosto de 2019). *Código procesal penal peruano: cuándo se aplica, situaciones y actores.* Obtenido de https://hegel.edu.pe/blog/codigo-procesal-penal-peruano-cuando-se-aplica-situaciones-y-actores/

Kaspersky. (02 de marzo de 2021). Obtenido de ¿Qué es la ciberseguridad?: https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security

Kaspersky. (15 de agosto de 2021). *Ciberataques en América Latina crecen un 24% durante los primeros ocho meses de 2021.* Obtenido de https://latam.kaspersky.com/blog/ciberataques-en-america-latina-crecen-un-24-durante-los-primeros-ocho-meses-de-2021/22718/

Kyocera. (1 de diciembre de 2020). *Digitalización empresarial: qué es, ventajas, seguridad y herramientas.* Obtenido de https://www.kyoceradocumentsolutions.es/es/smarter-workspaces/business-challenges/paperless/digitalizacion-en-la-empresa-que-es-ventajas-seguridad-y-herramientas.html

Lundquist, R. (2016). *An Examination of Failed Digital Forensics and the Criminal Justice System.*

Microsoft. (12 de marzo de 2021). *Microsoft Forms.* Obtenido de https://www.microsoft.com/es/microsoft-365/online-surveys-polls-quizzes

Microsoft. (16 de abril de 2021). *Microsoft Word.* Obtenido de https://www.microsoft.com/es-es/microsoft-365/word?activetab=tabs%3afaqheaderregion3

Ministerio Público. (26 de noviembre de 2020). *Distrito Fiscal de Huánuco.* Obtenido de https://www.mpfn.gob.pe/huanuco/

Ministerio Público. (12 de octubre de 2020). *Etapas del proceso.* Obtenido de https://www.mpfn.gob.pe/elfiscal/etapas_proceso/

Ministerio Público. (12 de octubre de 2021). *Actores*. Obtenido de https://www.mpfn.gob.pe/elfiscal/actores/

Montgomery, C. (2017). *New security for a new era: an investigation into law enforcement cybersecurity threats, obstacles, and community applications.* Utica: Faculty of Utica.

Mozilla. (11 de junio de 2021). *MDN Web Docs*. Obtenido de https://developer.mozilla.org/es/docs/Glossary/Arpanet

National Institute of Standards and Technology. (12 de septiembre de 2021). Obtenido de Computer Security Resource Center: https://csrc.nist.gov/glossary/term/cybersecurity

Ñaupas, P., Valdivia, D., Palacios, V., & Romero, D. (2018). *Metodología de la Investigación: Cuantitativa-Cualitativa y Redacción de la Tesis.* México D.F. : Editorial Grijley.

OEA. (2 de diciembre de 2020). *Ciberdelito: 90.000 millones de razones para perseguirlo*. Obtenido de https://www.oas.org/es/centro_noticias/comunicado_prensa.asp?sCodigo=C-

063/16#:~:text=Seg%C3%BAn%20estimaciones%20de%20LACNIC%2C%20el,millones%20de%20d%C3%B3lares%20al%20a%C3%B1o.

Organización Internacional de Normalización. (2020). *Information security, cybersecurity and privacy protection*. Obtenido de https://www.iso.org/standard/72434.html

Ormachea, J. (2019). *Estrategias integradas de ciberseguridad para el fortalecimiento de la seguridad nacional.* Lima: Centro de Altos Estudios Nacionales.

Plataforma digital única del Estado Peruano. (10 de noviembre de 2021). *¿Cómo actuar frente a un caso de grooming?* Obtenido de https://www.gob.pe/12801-como-actuar-frente-a-un-caso-de-grooming

Poder Judicial de Costa Rica. (03 de junio de 2021). *Diccionario usual del Poder Judicial*. Obtenido de https://diccionariousual.poder-judicial.go.cr/index.php/diccionario/44304:operador-a-jur%C3%ADdico-a

Proyecto Descartes. (30 de junio de 2020). *Tabulación de datos.* Obtenido de https://proyectodescartes.org/iCartesiLibri/materiales_didacticos/IntroduccionEstadisticaProbabilidad/3ESO/3TabulacionDatos.html

Question pro. (12 de marzo de 2021). *Preguntas cerradas ¿Cuando utilizarlas?* Obtenido de https://www.questionpro.com/blog/es/preguntas-cerradas/

Quevedo , J. (2017). *Investigación y prueba del ciberdelito.* Barcelona: Universitat de Barcelona.

Real Academía Española. (12 de diciembre de 2021). Obtenido de https://dle.rae.es/inform%C3%A1tico

Real Academia Española. (07 de abril de 2021). *Diccionario Panhispánico del Español Jurídico*. Obtenido de https://dpej.rae.es/

Real Academia Española. (11 de junio de 2022). Obtenido de Real Academia Española.

Rivadeneira, E. (2017). Habilidades conceptuales, procedimentales y actitudinales para la orientación y reflexión pedagógica. *Revista Científica Electrónica de Ciencias Humanas*, 41-55.

Rodriguez Marquez, M. P. (2021). *Ciberseguridad en la justicia digital: recomendaciones para el caso colombiano.* Revista UIS Ingenierías.

Rodriguez, M. (2013). *América Latina, ¿debe crear un sistema de normas armonizadas para el cibercrimen?* Obtenido de http://econ.uchile.cl/uploads/publicacion/9ba7739a0ac26598402dab53c990c58e49fc259a.pdf

Rodriguez, M. (1 de abril de 2020). *Los sujetos procesales en el Código Procesal.* Obtenido de https://revistas.pucp.edu.pe/index.php/derechopucp/article/download/3140/2962/&cd=12&hl=es-419&ct=clnk&gl=pe

Rossi, G. (2021). *"La Seguridad y Defensa en la era de la Cuarta Revolución Industrial: Elementos para una propuesta de estrategia de política exterior para el fortalecimiento de las capacidades del Perú en materia de ciberdefensa y amenazas híbridas".* Lima: Academia Diplomática Javier Perez de Cuellar.

Sandoval, J. (2020). - *Propuesta de diseño de un sistema de gestión de seguridad de la información basado en la NTPISO/IEC 27001 para la Dirección Regional de Trabajo y Promoción del Empleo – Huánuco.* Huánuco: Universidad Nacional Hermilio Valdizan.

Sanromán, R., & Morales, L. (4 de mayo de 2021). La educación por competencias en el campo del derecho. *Boletín mexicano de derecho comparado*. Obtenido de http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0041-86332016000200179#fn20

Supo, J. (13 de septiembre de 2021). *Cómo validar un instrumento.* Obtenido de http://www.cua.uam.mx/pdfs/coplavi/s_p/doc_ng/validacion-de-instrumentos-de-medicion.pdf

Téllez, J. (2008). *Derecho Informático.* México D.F.: Editorial Mc Graw Hill .

The International Criminal Police Organization. (2017). *Global Cibercrime Strategy.* Obtenido de https://www.interpol.int/content/download/5586/file/Summary_CYBER_Strategy_2017_01_EN%20LR.pdf

Vilca, L. (2017). *La formación profesional en derecho informático y la persecución penal de delitos informáticos en el distrito fiscal de Huánuco – 2017.* Huánuco: Universidad Nacional Hermilio Valdizán.

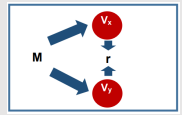
Villavicencio, F. (2014). *Delitos Informáticos.* Lima: Revista Ius Et Veritas.

ANEXO 01

MATRIZ DE CONSISTENCIA

COMPETENCIAS EN CIBERSEGURIDAD DEL OPERADOR JURÍDICO Y LA INVESTIGACIÓN PENAL DE CIBERDELITOS EN EL DISTRITO FISCAL DE HUÁNUCO DURANTE EL PERIODO 2020

PROBLEMA	OBJETIVO	HIPÓTESIS	MARCO TEÓRICO	MATRIZ DE OPERACIONZALIZACIÓN DE VARIABLES				
GENERAL	GENERAL	GENERAL	ANTECEDENTES	VARIABLES		CONCEPTO	DIMENSIONES	INDICADORES ITEMS
PG. ¿Cuál es la relación de las competencias en ciberseguridad del operador jurídico y la investigación penal de delitos informáticos en el distrito fiscal de Huánuco durante el periodo 2020?	OG. Determinar la relación entre las competencias en ciberseguridad del operador jurídico y la investigación penal de delitos informáticos en el distrito fiscal de Huánuco durante el periodo 2020.	HG. Las competencias en ciberseguridad del operador jurídico se relacionan con la investigación penal de delitos informáticos en el distrito fiscal de Huánuco durante el periodo 2020.	Omachea, J. (2020). Estrategias Integradas de Ciberseguridad para el Fortalecimiento de la Seguridad Nacional. Villalba, A. (2015). La ciberseguridad en España 2011 – 2015 una propuesta de modelo de organización. Valenzuela, D. (2018). Ciberseguridad en América Latina y ciberdefensa en Chile.	VARIABLE 1	Competencias en ciberseguridad del operador jurídico	Conjunto de competencias enfocadas en el reconocimiento de tecnologías y aplicación de procedimientos para la seguridad de la información, así como el identificación y respuesta de incidentes de seguridad de la información en entornos informáticos.	Reconocimiento de tecnología para la seguridad de la información en el ciberespacio	Identifica tecnologías en ciberseguridad Identifica problemas, riesgos y vulnerabilidades de tecnologías en ciberseguridad Identifica tecnologías en ciberseguridad
							Aplicación de procedimientos para la seguridad de la información en el ciberespacio	Realiza copias de seguridad de datos informáticos Identifica límites de acceso y uso de datos y tecnologías informáticas Realiza copias de seguridad de datos informáticos
							Identificación de incidentes de seguridad de la información en el ciberespacio	Identifica la clasificación de incidentes en ciberseguridad Identifica las características de incidentes en ciberseguridad Identifica los riesgos, amenazas y relevancia jurídica de incidentes en ciberseguridad
							Respuesta a incidentes de seguridad de la información en el ciberespacio	Identifica roles y responsabilidades en incidentes en ciberseguridad Identifica el marco jurídico aplicable en incidentes de ciberseguridad Aplica la informática forense en la investigación de incidentes en ciberseguridad.
ESPECÍFICO	ESPECÍFICO	ESPECÍFICO	MARCO TEÓRICO	VARIABLE 2	Investigación penal de delitos informáticos	Investigación de delitos que afectan sistemas o datos informáticos u otros bienes jurídicos de relevancia penal mediante la utilización de las de las tecnologías de la información y las comunicaciones	Investigación penal de delitos que afectan datos informáticos	Identifica si la conducta incriminada es delictuosa. Identifica las circunstancias y/o móviles del hecho. Identifica la identidad del autor, participe y víctimas. Identifica la existencia del daño causado.
PE1. ¿Cuál es la relación entre el reconocimiento de tecnología para la seguridad de la información en el ciberespacio y la	OE1. Determinar la relación entre el reconocimiento de tecnología para la seguridad de la información en el ciberespacio y la investigación penal de delitos informáticos.	HE1. El reconocimiento de tecnología para la seguridad de la información en el ciberespacio se relaciona con la investigación penal de delitos informáticos.	T1. Teoría de la formación por competencias. T2. La teoría de la informática. T3. Teoría de la ciberseguridad. T4. La teoría del proceso penal.				Investigación penal de delitos afectan sistemas informáticos	Identifica si la conducta incriminada es delictuosa. Identifica las circunstancias y/o móviles del hecho.

MARCO METODOLÓGICO	
TIPO	Correlacional
ENFOQUE	Cuantitativo
NIVEL	Explicativo
DISEÑO	Descriptivo transeccional
ESQUEMA	 Donde: M : La muestra corresponde a los operadores jurídicos que intervienen dentro de la investigación de delitos informáticos. Vx: Corresponde a las competencias en ciberseguridad. Vy: Corresponde a la investigación penal de delitos informáticos. r : Es el coeficiente de correlación.
POBLACIÓN	Operadores jurídicos que participan en la investigación de ciberdelitos (jueces, fiscales, abogados litigantes).

investigación penal de delitos informáticos? PE2. ¿Cuál es la relación entre la aplicación de procedimientos para la seguridad de la información en el ciberespacio y la investigación penal de delitos informáticos? PE3. ¿Cuál es la relación entre la identificación de incidentes de seguridad de la información en el ciberespacio y la investigación penal de delitos informáticos? PE4. ¿Cuál es la relación entre la respuesta a incidentes de seguridad de la información en el ciberespacio y la investigación penal de delitos informáticos?	OE2. Determinar la relación entre la aplicación de procedimientos para la seguridad de la información en el ciberespacio y la investigación penal de ciberdelitos. OE3. Determinar la relación entre la identificación de incidentes de seguridad de la información en el ciberespacio y la investigación penal de delitos informáticos. OE4. Determinar la relación entre la respuesta a incidentes de seguridad de la información en el ciberespacio y la investigación penal de delitos informáticos	HE2. La aplicación de procedimientos para la seguridad de la información en el ciberespacio se relaciona con la investigación penal de delitos informáticos. HE3. La identificación de incidentes de seguridad de la información en el ciberespacio se relaciona con la investigación penal de delitos informáticos. HE4. La respuesta a incidentes de seguridad de la información en el ciberespacio se relaciona con la investigación penal de delitos informáticos.							
							Investigación penal de delitos que afectan otros bienes jurídicos de relevancia penal mediante la utilización de las tecnologías de la información y las comunicaciones	Identifica la identidad del autor, participe y víctimas.	MUESTRA	Muestra probabilística: 283 operadores jurídicos.
								Identifica la existencia del daño causado.		
								Identifica si la conducta incriminada es delictuosa.	TÉCNICAS	INSTRUMENTOS
								Identifica las circunstancias y/o móviles del hecho. Identifica la identidad del autor, participe y víctimas.	Análisis documental	Matriz de análisis documental
								Identifica las circunstancias y/o móviles del hecho. Identifica la identidad del autor, participe y víctimas.	La encuesta	Cuestionario
								Identifica la existencia del daño causado.	La entrevista	Guía de entrevista virtual

ANEXO 02

CONSENTIMIENTO INFORMADO

ID: _____ **FECHA:**_____

Título de la investigación: Competencias en ciberseguridad del operador jurídico y la investigación penal de ciberdelitos en el distrito fiscal de Huánuco durante el periodo 2020.

Objetivo: Determinar la relación entre las competencias en ciberseguridad del operador jurídico y la investigación penal de ciberdelitos en el distrito fiscal de Huánuco durante el periodo 2020.

Investigador: Leonardo Edgard Vilca Morales

Consentimiento / Participación voluntaria

Acepto participar en el estudio: He leído la información proporcionada, o me ha sido leída. He tenido la oportunidad de preguntar dudas sobre ello y se me ha respondido satisfactoriamente. Consiento voluntariamente participar en este estudio y entiendo que tengo el derecho de retirarme en cualquier momento de la intervención (tratamiento) sin que me afecte de ninguna manera.

Firma del participante : _____ **Huella digital si el caso lo amerita:**

Firma del investigador : _____

Huánuco, 2020.

ANEXO 03

CUESTIONARIO

COMPETENCIAS EN CIBERSEGURIDAD Y LA INVESTIGACIÓN PENAL DE DELITOS INFORMÁTICOS EN EL DISTRITO FISCAL DE HUÁNUCO – 2020

ENCUESTA DIRIGIDA: JUECES, FISCALES, ABOGADOS.

Estimado Sr./Sra., con fines estrictamente académicos se ha elaborado el presente cuestionario, a efectos de que con vuestra valiosa colaboración pueda aportar al desarrollo de la presente investigación científica.
A continuación, sírvase en marcar con un aspa la respuesta que usted crea conveniente.

INSTRUCCIONES:

- ✓ Lea detenidamente cada una de las preguntas y responda con la verdad.
- ✓ Conteste marcando con un aspa (X) la valoración que otorgue a cada una de las interrogantes.
- ✓ No debe dejar de marcar ninguna de las preguntas, en caso de duda, pregunte al evaluador.

DATOS DEL ENCUESTADO

Cargo que ocupa:
JUEZ: ☐ FISCAL: ☐ ABOGADO: ☐

RUBROS	ITEMS	VALORES				
		NUNCA	SI NUNCA	VECES	SI SIEMPRE	EMPRE
		0	1	2	3	4
1	¿Identifica usted problemas, riesgos y vulnerabilidades en las tecnologías de la información y las comunicaciones?					
	¿Identifica usted tecnología informática que le permita brindar seguridad a la información en el ciberespacio?					
	¿Aplica usted tecnología informática para la seguridad de la información en el ciberespacio?					
2	¿Realiza usted copias de seguridad de datos informáticos?					
	¿Identifica usted los límites de acceso y uso de las tecnologías de la información y las comunicaciones en la organización donde labora?					
	¿Aplica usted los protocolos de seguridad de la información en el ciberespacio que establece la organización donde labora?					
3	¿Identifica usted la clasificación de un incidente de seguridad de la información en el ciberespacio?					
	¿Identifica usted las características de un incidente de seguridad de la información en el ciberespacio?					
	¿Identifica usted los riesgos y amenazas con relevancia jurídica de un incidente de seguridad de la información en el ciberespacio?					

4	¿Identifica usted los roles y responsabilidades ante un incidente de seguridad de la información en el ciberespacio?					
	¿Identifica usted el marco jurídico aplicable ante un incidente de seguridad de la información en el ciberespacio?					
	¿Aplica usted procedimientos en informática forense para investigar un incidente de seguridad de la información en el ciberespacio?					
5	Durante la investigación de un hecho en el cual se que afectaron datos informáticos ¿Identificó si la conducta incriminada es delictuosa?					
	Durante la investigación de un hecho en el cual se que afectaron datos informáticos ¿Identificó las circunstancias y/o móviles del hecho?					
	Durante la investigación de un hecho en el cual se que afectaron datos informáticos ¿Identificó la identidad del autor, participe y víctimas?					
	Durante la investigación de un hecho en el cual se que afectaron datos informáticos ¿Identificó la existencia del daño causado?					
6	Durante la investigación de un hecho en la cual se que afectaron sistemas informáticos ¿Identificó si la conducta incriminada es delictuosa?					
	Durante la investigación de un hecho en el cual se que afectaron sistemas informáticos ¿Identificó las circunstancias y/o móviles del hecho?					
	Durante la investigación de un hecho en el cual se que afectaron sistemas informáticos ¿Identificó la identidad del autor, participe y víctimas?					
	Durante la investigación de un hecho en el cual se que afectaron sistemas informáticos ¿Identificó la existencia del daño causado?					
7	Durante la investigación de un hecho en el cual se que afectaron otros bienes jurídicos (distintos a datos y sistemas informáticos) ¿Identificó si la conducta incriminada es delictuosa?					
	Durante la investigación de un hecho en el cual se que afectaron otros bienes jurídicos (distintos a datos y sistemas informáticos) ¿Identificó las circunstancias y/o móviles del hecho?					
	Durante la investigación de un hecho en el cual se que afectaron otros bienes jurídicos (distintos a datos y sistemas informáticos) ¿Identificó la identidad del autor, participe y víctimas?					
	Durante la investigación de un hecho en el cual se que afectaron otros bienes jurídicos (distintos a datos y sistemas informáticos) ¿Identificó la existencia del daño causado?					

La presente encuesta también la puede completar vía online a través del siguiente enlace: **https://cutt.ly/ch2KZw6**

¡MUCHAS GRACIAS POR SU COLABORACIÓN!

ANEXO 04

UNIVERSIDAD NACIONAL HERMILIO VALDIZAN
UNIDAD DE POSGRADO
MAESTRÍA EN DERECHO
MENCIÓN EN CIENCIAS PENALES

FICHA DE VALIDACIÓN POR JUICIO DE EXPERTOS

I.DATOS GENERALES:

Grado académico, Apellidos y nombres del experto	DOCTORA DURAND MOLINA, AMÉRICA FELIPA
Cargo o institución donde labora	ESTUDIO JURÍDICO DURAND E.I.R.L
Nombre del instrumento de evaluación	Cuestionario de encuesta
Autor del instrumento	Leonardo Edgard Vilca Morales

II. ASPECTOS DE VALIDACIÓN: Calificar con 1, 2, 3 ó 4 cada ítem respecto a los criterios de relevancia, coherencia, suficiencia y claridad.

OPERACIONALIZACIÓN DE LA VARIABLE				CRITERIOS DE VALIDACIÓN					
VARIABLES	DIMENSIONES	ITEMS	ITEMS	RELEVANCIA	COHERENCIA	SUFICIENCIA	CLARIDAD	OBSERVACIÓN PROMEDIO PARCIAL	OBSERVACIÓN
Competencias en ciberseguridad Del operador Jurídico	Reconocimiento de tecnología para la seguridad de la información en el ciberespacio	¿Identifica usted problemas, riesgos y vulnerabilidades en las tecnologías de la información y las comunicaciones?	1	4	4	4	4	16	
		¿Identifica usted tecnología informática que le permita brindar seguridad a la información en el ciberespacio?	2	4	4	4	4	16	
		¿Aplica usted tecnología informática para la seguridad de la información en el ciberespacio?	3	4	4	4	4	16	
	Aplicación de procedimientos para la seguridad de la información en el ciberespacio	¿Realiza usted copias de seguridad de datos informáticos?	4	4	4	4	4	16	
		¿Identifica usted los límites de acceso y uso de las tecnologías de la información y las comunicaciones en la organización donde labora?	5	4	4	4	4	16	
		¿Aplica usted los protocolos de seguridad de la información en el ciberespacio que establece la organización donde labora?	6	4	4	4	4	16	
	Identificación de incidentes de seguridad de la información en el ciberespacio	¿Identifica usted la clasificación de un incidente de seguridad de la información en el ciberespacio?	7	4	4	4	4	16	
		¿Identifica usted las características de un incidente de seguridad de la información en el ciberespacio?	8	4	4	4	4	16	
		¿Identifica usted los riesgos y amenazas con relevancia jurídica de un incidente de seguridad de la información en el ciberespacio?	9	4	4	4	4	16	
	Respuesta a incidentes de seguridad de la información en el ciberespacio	¿Identifica usted los roles y responsabilidades ante un incidente de seguridad de la información en el ciberespacio?	10	4	4	4	4	16	
		¿Identifica usted el marco jurídico aplicable ante un incidente de seguridad de la información en el ciberespacio?	11	4	4	4	4	16	
		¿Aplica usted procedimientos en informática forense para investigar un incidente de seguridad de la información en el ciberespacio?	12	4	4	4	4	16	
Investigación penal de delitos informáticos	Investigación penal de delitos que afectan datos informáticos	Durante la investigación de un hecho en el cual se afectaron datos informáticos ¿Identificó si la conducta incriminada es delictuosa?	13	4	4	4	4	16	
		Durante la investigación de un hecho en el cual se afectaron datos informáticos ¿Identificó las circunstancias y/o móviles del hecho?	14	4	4	4	4	16	
		Durante la investigación de un hecho en el cual se afectaron datos informáticos ¿Identificó la identidad del autor, participe y víctimas?	15	4	4	4	4	16	
		Durante la investigación de un hecho en el cual se afectaron datos informáticos ¿Identificó la existencia del daño causado?	16	4	4	4	4	16	

	Investigación penal de delitos afectan sistemas informáticos	Durante la investigación de un hecho en la cual se afectaron sistemas informáticos ¿Identificó si la conducta incriminada es delictuosa?	17	4	4	4	4	16	
		Durante la investigación de un hecho en el cual se afectaron sistemas informáticos ¿Identificó las circunstancias y/o móviles del hecho?	18	4	4	4	4	16	
		Durante la investigación de un hecho en el cual se afectaron sistemas informáticos ¿Identificó la identidad del autor, participe y víctimas?	19	4	4	4	4	16	
		Durante la investigación de un hecho en el cual se afectaron sistemas informáticos ¿Identificó la existencia del daño causado?	20	4	4	4	4	16	
	Investigación penal de delitos que afectan otros bienes jurídicos de relevancia penal mediante la utilización de las tecnologías de la información y las comunicaciones	Durante la investigación de un hecho en el cual se afectaron otros bienes jurídicos mediante el uso de las tecnologías de la información y las comunicaciones ¿Identificó si la conducta incriminada es delictuosa?	21	4	4	4	4	16	
		Durante la investigación de un hecho en el cual se afectaron otros bienes jurídicos mediante el uso de las tecnologías de la información y las comunicaciones ¿Identificó las circunstancias y/o móviles del hecho?	22	4	4	4	4	16	
		Durante la investigación de un hecho en el cual se afectaron otros bienes jurídicos mediante el uso de las tecnologías de la información y las comunicaciones ¿Identificó la identidad del autor, participe y víctimas?	23	4	4	4	4	16	
		Durante la investigación de un hecho en el cual se afectaron otros bienes jurídicos mediante el uso de las tecnologías de la información y las comunicaciones ¿Identificó la existencia del daño causado?	24	4	4	4	4	16	
	PUNTAJE TOTAL							384	
	PUNTAJE EXPRESADA EN EL SISTEMA VIGESIMAL							20	

III.ESCALA DE CALIFICACIÓN: 20/40 x Puntaje Total = 0,5 x Puntaje total

CUALITATIVA		CUANTITATIVA	CUALITATIVA		CUANTITATIVA
E	MUY DEFICIENTE	00 - 05	C	REGULAR	11 - 13
D	DEFICIENTE	06 - 10	B	BUENO	14 - 17
			A	EXCELENTE	18 - 20

IV. OPINIÓN DE APLICACIÓN: (X) VÁLIDO ( ) MEJORAR ( ) NO VALIDO

V. RECOMENDACIONES :

Huánuco..11..de .Noviembre del 2020	22511678		962028104
Lugar y fecha	DNI	Firma del experto	Teléfono

HOJA DE INSTRUCCIONES PARA LA EVALUACIÓN

CATEGORÍA	CALIFICACIÓN	INDICADOR
RELEVANCIA El ítem es esencial o importante, es decir debe ser incluido.	1.No cumple con el criterio	El ítem puede ser eliminado sin que se vea afectada la medición de la dimensión.
	2.Bajo nivel	El ítem tiene una alguna relevancia, pero otro ítem puede estar incluyendo lo que mide este.
	3.Moderado nivel	El ítem es relativamente importante.
	4.Alto nivel	El ítem es muy relevante y debe ser incluido.
COHERENCIA El ítem tiene relación lógica con la dimensión o indicador.	1.No cumple con el criterio	El ítem puede ser eliminado sin que se vea afectada la medición de la dimensión.
	2.Bajo nivel	El ítem tiene una relación tangencial con la dimensión.
	3.Moderado nivel	El ítem tiene relación moderada con la dimensión que está midiendo.
	4.Alto nivel	El ítem tiene relación lógica con la dimensión.
SUFICIENCIA Los ítems que pertenecen a una misma dimensión bastan para obtener la medición de esta	1.No cumple con el criterio	Los ítems no son suficientes para medir la dimensión.
	2.Bajo nivel	Los ítems miden algún aspecto de la dimensión, pero no corresponden con la dimensión total.
	3.Moderado nivel	Se deben incrementar algunos ítems para poder evaluar la dimensión completamente.
	4.Alto nivel	Los ítems son suficientes.
CLARIDAD El ítem se comprende fácilmente, es decir sus sintácticas y semánticas son adecuadas	1.No cumple con el criterio	El ítem no es claro.
	2.Bajo nivel	El ítem requiere bastantes modificaciones o una modificación muy grande en el uso de las palabras que utilizan de acuerdo a su significado o por la ordenación de los mismos.
	3.Moderado nivel	Se requiere una modificación muy específica de algunos términos de ítem.
	4.Alto nivel	El ítem es claro, tiene semántica y sintaxis adecuada.

UNIVERSIDAD NACIONAL HERMILIO VALDIZAN
UNIDAD DE POSGRADO
MAESTRÍA EN DERECHO
MENCIÓN EN CIENCIAS PENALES

FICHA DE VALIDACIÓN POR JUICIO DE EXPERTOS

I.DATOS GENERALES:

Grado académico, Apellidos y nombres del experto	Mg. Jeremías Rojas Velásquez
Cargo o institución donde labora	Docente Universitario
Nombre del instrumento de evaluación	Cuestionario de encuesta
Autor del instrumento	Leonardo Edgard Vilca Morales

II. ASPECTOS DE VALIDACIÓN: Calificar con 1, 2, 3 ó 4 cada ítem respecto a los criterios de relevancia, coherencia, suficiencia y claridad.

OPERACIONALIZACIÓN DE LA VARIABLE				CRITERIOS DE VALIDACIÓN					
VARIABLES	DIMENSIONES	ITEMS	ITEMS	RELEVANCIA	COHERENCIA	SUFICIENCIA	CLARIDAD	OBSERVACIÓN PROMEDIO PARCIAL	OBSERVACIÓN
Competencias en ciberseguridad Del operador Jurídico	Reconocimiento de tecnología para la seguridad de la información en el ciberespacio	¿Identifica usted problemas, riesgos y vulnerabilidades en las tecnologías de la información y las comunicaciones?	1	4	4	4	4	16	
		¿Identifica usted tecnología informática que le permita brindar seguridad a la información en el ciberespacio?	2	4	4	4	4	16	
		¿Aplica usted tecnología informática para la seguridad de la información en el ciberespacio?	3	4	4	4	4	16	
	Aplicación de procedimientos para la seguridad de la información en el ciberespacio	¿Realiza usted copias de seguridad de datos informáticos?	4	4	4	4	4	16	
		¿Identifica usted los límites de acceso y uso de las tecnologías de la información y las comunicaciones en la organización donde labora?	5	4	4	4	4	16	
		¿Aplica usted los protocolos de seguridad de la información en el ciberespacio que establece la organización donde labora?	6	4	4	4	4	16	
	Identificación de incidentes de seguridad de la información en el ciberespacio	¿Identifica usted la clasificación de un incidente de seguridad de la información en el ciberespacio?	7	4	4	4	4	16	
		¿Identifica usted las características de un incidente de seguridad de la información en el ciberespacio?	8	4	4	4	4	16	
		¿Identifica usted los riesgos y amenazas con relevancia jurídica de un incidente de seguridad de la información en el ciberespacio?	9	4	4	4	4	16	
	Respuesta a incidentes de seguridad de la información en el ciberespacio	¿Identifica usted los roles y responsabilidades ante un incidente de seguridad de la información en el ciberespacio?	10	4	4	4	4	16	
		¿Identifica usted el marco jurídico aplicable ante un incidente de seguridad de la información en el ciberespacio?	11	4	4	4	4	16	
		¿Aplica usted procedimientos en informática forense para investigar un incidente de seguridad de la información en el ciberespacio?	12	4	4	4	4	16	
Investigación penal de delitos informáticos	Investigación penal de delitos que afectan datos informáticos	Durante la investigación de un hecho en el cual se afectaron datos informáticos ¿Identificó si la conducta incriminada es delictuosa?	13	4	4	4	4	16	
		Durante la investigación de un hecho en el cual se afectaron datos informáticos ¿Identificó las circunstancias y/o móviles del hecho?	14	4	4	4	4	16	
		Durante la investigación de un hecho en el cual se afectaron datos informáticos ¿Identificó la identidad del autor, participe y victimas?	15	4	4	4	4	16	
		Durante la investigación de un hecho en el cual se afectaron datos informáticos ¿Identificó la existencia del daño causado?	16	4	4	4	4	16	

	Investigación penal de delitos afectan sistemas informáticos	Durante la investigación de un hecho en la cual se afectaron sistemas informáticos ¿Identificó si la conducta incriminada es delictuosa?	17	4	4	4	4	16	
		Durante la investigación de un hecho en el cual se afectaron sistemas informáticos ¿Identificó las circunstancias y/o móviles del hecho?	18	4	4	4	4	16	
		Durante la investigación de un hecho en el cual se afectaron sistemas informáticos ¿Identificó la identidad del autor, participe y víctimas?	19	4	4	4	4	16	
		Durante la investigación de un hecho en el cual se afectaron sistemas informáticos ¿Identificó la existencia del daño causado?	20	4	4	4	4	16	
	Investigación penal de delitos que afectan otros bienes jurídicos de relevancia penal mediante la utilización de las tecnologías de la información y las comunicaciones	Durante la investigación de un hecho en el cual se afectaron otros bienes jurídicos mediante el uso de las tecnologías de la información y las comunicaciones ¿Identificó si la conducta incriminada es delictuosa?	21	4	4	4	4	16	
		Durante la investigación de un hecho en el cual se afectaron otros bienes jurídicos mediante el uso de las tecnologías de la información y las comunicaciones ¿Identificó las circunstancias y/o móviles del hecho?	22	4	4	4	4	16	
		Durante la investigación de un hecho en el cual se afectaron otros bienes jurídicos mediante el uso de las tecnologías de la información y las comunicaciones ¿Identificó la identidad del autor, participe y víctimas?	23	4	4	4	4	16	
		Durante la investigación de un hecho en el cual se afectaron otros bienes jurídicos mediante el uso de las tecnologías de la información y las comunicaciones ¿Identificó la existencia del daño causado?	24	4	4	4	4	16	
	PUNTAJE TOTAL							384	
	PUNTAJE EXPRESADA EN EL SISTEMA VIGESIMAL							20	

III.ESCALA DE CALIFICACIÓN: 20/40 x Puntaje Total = 0,5 x Puntaje total

CUALITATIVA		CUANTITATIVA	CUALITATIVA		CUANTITATIVA
E	MUY DEFICIENTE	00 - 05	C	REGULAR	11 - 13
D	DEFICIENTE	06 - 10	B	BUENO	14 - 17
			A	EXCELENTE	18 - 20

IV. OPINIÓN DE APLICACIÓN: (X) **VÁLIDO** ( ) **MEJORAR** ( ) **NO VALIDO**

V. RECOMENDACIONES :

Huánuco 09 de noviembre del 2020	22497958		962689300
Lugar y fecha	**DNI**	**Firma del experto**	**Teléfono**

HOJA DE INSTRUCCIONES PARA LA EVALUACIÓN

CATEGORÍA	CALIFICACIÓN	INDICADOR
RELEVANCIA El ítem es esencial o importante, es decir debe ser incluido.	1.No cumple con el criterio	El ítem puede ser eliminado sin que se vea afectada la medición de la dimensión.
	2.Bajo nivel	El ítem tiene una alguna relevancia, pero otro ítem puede estar incluyendo lo que mide este.
	3.Moderado nivel	El ítem es relativamente importante.
	4.Alto nivel	El ítem es muy relevante y debe ser incluido.
COHERENCIA El ítem tiene relación lógica con la dimensión o indicador.	1.No cumple con el criterio	El ítem puede ser eliminado sin que se vea afectada la medición de la dimensión.
	2.Bajo nivel	El ítem tiene una relación tangencial con la dimensión.
	3.Moderado nivel	El ítem tiene relación moderada con la dimensión que está midiendo.
	4.Alto nivel	El ítem tiene relación lógica con la dimensión.
SUFICIENCIA Los ítems que pertenecen a una misma dimensión bastan para obtener la medición de esta	1.No cumple con el criterio	Los ítems no son suficientes para medir la dimensión.
	2.Bajo nivel	Los ítems miden algún aspecto de la dimensión, pero no corresponden con la dimensión total.
	3.Moderado nivel	Se deben incrementar algunos ítems para poder evaluar la dimensión completamente.
	4.Alto nivel	Los ítems son suficientes.
CLARIDAD El ítem se comprende fácilmente, es decir sus sintácticas y semánticas son adecuadas	1.No cumple con el criterio	El ítem no es claro.
	2.Bajo nivel	El ítem requiere bastantes modificaciones o una modificación muy grande en el uso de las palabras que utilizan de acuerdo a su significado o por la ordenación de los mismos.
	3.Moderado nivel	Se requiere una modificación muy específica de algunos términos de ítem.
	4.Alto nivel	El ítem es claro, tiene semántica y sintaxis adecuada.

UNIVERSIDAD NACIONAL HERMILIO VALDIZAN
UNIDAD DE POSGRADO
MAESTRÍA EN DERECHO
MENCIÓN EN CIENCIAS PENALES

FICHA DE VALIDACIÓN POR JUICIO DE EXPERTOS

I.DATOS GENERALES:

Grado académico, Apellidos y nombres del experto	Dr. SOTIL CORTAVARRÍA, Wilfredo Antonio
Cargo o institución donde labora	Docente Universitario de la UNHEVAL
Nombre del instrumento de evaluación	Cuestionario de encuesta
Autor del instrumento	Leonardo Edgard Vilca Morales

II. ASPECTOS DE VALIDACIÓN: Calificar con 1, 2, 3 ó 4 cada ítem respecto a los criterios de relevancia, coherencia, suficiencia y claridad.

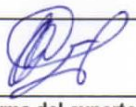
OPERACIONALIZACIÓN DE LA VARIABLE				CRITERIOS DE VALIDACIÓN				OBSERVACIÓN PROMEDIO PARCIAL	OBSERVACIÓN
VARIABLES	DIMENSIONES	ITEMS	ITEMS	RELEVANCIA	COHERENCIA	SUFICIENCIA	CLARIDAD		
Competencias en ciberseguridad Del operador Jurídico	Reconocimiento de tecnología para la seguridad de la información en el ciberespacio	¿Identifica usted problemas, riesgos y vulnerabilidades en las tecnologías de la información y las comunicaciones?	1	4	4	4	4		
		¿Identifica usted tecnología informática que le permita brindar seguridad a la información en el ciberespacio?	2	4	4	3	4		
		¿Aplica usted tecnología informática para la seguridad de la información en el ciberespacio?	3	4	4	4	4		
	Aplicación de procedimientos para la seguridad de la información en el ciberespacio	¿Realiza usted copias de seguridad de datos informáticos?	4	4	4	4	4		
		¿Identifica usted los límites de acceso y uso de las tecnologías de la información y las comunicaciones en la organización donde labora?	5	4	4	4	4		
		¿Aplica usted los protocolos de seguridad de la información en el ciberespacio que establece la organización donde labora?	6	4	3	4	4		
	Identificación de incidentes de seguridad de la información en el ciberespacio	¿Identifica usted la clasificación de un incidente de seguridad de la información en el ciberespacio?	7	4	4	4	4		
		¿Identifica usted las características de un incidente de seguridad de la información en el ciberespacio?	8	4	4	4	4		
		¿Identifica usted los riesgos y amenazas con relevancia jurídica de un incidente de seguridad de la información en el ciberespacio?	9	4	4	4	4		
	Respuesta a incidentes de seguridad de la información en el ciberespacio	¿Identifica usted los roles y responsabilidades ante un incidente de seguridad de la información en el ciberespacio?	10	4	4	3	4		
		¿Identifica usted el marco jurídico aplicable ante un incidente de seguridad de la información en el ciberespacio?	11	4	4	4	4		
		¿Aplica usted procedimientos en informática forense para investigar un incidente de seguridad de la información en el ciberespacio?	12	4	3	4	4		
Investigación penal de delitos informáticos	Investigación penal de delitos que afectan datos informáticos	Durante la investigación de un hecho en el cual se afectaron datos informáticos ¿Identificó si la conducta incriminada es delictuosa?	13	4	4	4	4		
		Durante la investigación de un hecho en el cual se afectaron datos informáticos ¿Identificó las circunstancias y/o móviles del hecho?	14	4	4	4	4		
		Durante la investigación de un hecho en el cual se afectaron datos informáticos ¿Identificó la identidad del autor, participe y víctimas?	15	4	4	4	4		
		Durante la investigación de un hecho en el cual se afectaron datos informáticos ¿Identificó la existencia del daño causado?	16	4	4	4	4		
	Investigación penal de delito	Durante la investigación de un hecho en la cual se afectaron sistemas informáticos ¿Identificó si la conducta incriminada es delictuosa?	17	4	4	4	4		

		Durante la investigación de un hecho en el cual se afectaron sistemas informáticos ¿Identificó las circunstancias y/o móviles del hecho?	18	4	4	4	4		
		Durante la investigación de un hecho en el cual se afectaron sistemas informáticos ¿Identificó la identidad del autor, participe y víctimas?	19	4	4	4	4		
		Durante la investigación de un hecho en el cual se afectaron sistemas informáticos ¿Identificó la existencia del daño causado?	20	4	3	4	4		
	Investigación penal de delitos que afectan otros bienes jurídicos de relevancia penal mediante la utilización de las tecnologías de la información y las comunicaciones	Durante la investigación de un hecho en el cual se afectaron otros bienes jurídicos mediante el uso de las tecnologías de la información y las comunicaciones ¿Identificó si la conducta incriminada es delictuosa?	21	4	4	4	4		
		Durante la investigación de un hecho en el cual se afectaron otros bienes jurídicos mediante el uso de las tecnologías de la información y las comunicaciones ¿Identificó las circunstancias y/o móviles del hecho?	22	4	4	4	4		
		Durante la investigación de un hecho en el cual se afectaron otros bienes jurídicos mediante el uso de las tecnologías de la información y las comunicaciones ¿Identificó la identidad del autor, participe y víctimas?	23	4	4	4	4		
		Durante la investigación de un hecho en el cual se afectaron otros bienes jurídicos mediante el uso de las tecnologías de la información y las comunicaciones ¿Identificó la existencia del daño causado?	24	3	4	4	4		
	PUNTAJE TOTAL								
	PUNTAJE EXPRESADA EN EL SISTEMA VIGESIMAL							18	

III.ESCALA DE CALIFICACIÓN: 20/40 x Puntaje Total = 0,5 x Puntaje total

CUALITATIVA		CUANTITATIVA	CUALITATIVA		CUANTITATIVA
E	MUY DEFICIENTE	00 - 05	C	REGULAR	11 - 13
D	DEFICIENTE	06 - 10	B	BUENO	14 - 17
			A	EXCELENTE	18 - 20

IV. OPINIÓN DE APLICACIÓN: (X) VÁLIDO ( ) MEJORAR ( ) NO VALIDO
V. RECOMENDACIONES :

Huánuco 09 de noviembre del 2020	22417860		962622399
Lugar y fecha	DNI	Firma del experto	Teléfono

HOJA DE INSTRUCCIONES PARA LA EVALUACIÓN

CATEGORÍA	CALIFICACIÓN	INDICADOR
RELEVANCIA El ítem es esencial o importante, es decir debe ser incluido.	1.No cumple con el criterio	El ítem puede ser eliminado sin que se vea afectada la medición de la dimensión.
	2.Bajo nivel	El ítem tiene una alguna relevancia, pero otro ítem puede estar incluyendo lo que mide este.
	3.Moderado nivel	El ítem es relativamente importante.
	4.Alto nivel	El ítem es muy relevante y debe ser incluido.
COHERENCIA El ítem tiene relación lógica con la dimensión o indicador.	1.No cumple con el criterio	El ítem puede ser eliminado sin que se vea afectada la medición de la dimensión.
	2.Bajo nivel	El ítem tiene una relación tangencial con la dimensión.
	3.Moderado nivel	El ítem tiene relación moderada con la dimensión que está midiendo.
	4.Alto nivel	El ítem tiene relación lógica con la dimensión.
SUFICIENCIA Los ítems que pertenecen a una misma dimensión bastan para obtener la medición de esta	1.No cumple con el criterio	Los ítems no son suficientes para medir la dimensión.
	2.Bajo nivel	Los ítems miden algún aspecto de la dimensión, pero no corresponden con la dimensión total.
	3.Moderado nivel	Se deben incrementar algunos ítems para poder evaluar la dimensión completamente.
	4.Alto nivel	Los ítems son suficientes.
CLARIDAD El ítem se comprende fácilmente, es decir sus sintácticas y semánticas son adecuadas	1.No cumple con el criterio	El ítem no es claro.
	2.Bajo nivel	El ítem requiere bastantes modificaciones o una modificación muy grande en el uso de las palabras que utilizan de acuerdo a su significado o por la ordenación de los mismos.
	3.Moderado nivel	Se requiere una modificación muy específica de algunos términos de ítem.
	4.Alto nivel	El ítem es claro, tiene semántica y sintaxis adecuada.

UNIVERSIDAD NACIONAL HERMILIO VALDIZAN
UNIDAD DE POSGRADO
MAESTRÍA EN DERECHO
MENCIÓN EN CIENCIAS PENALES

FICHA DE VALIDACIÓN POR JUICIO DE EXPERTOS

I.DATOS GENERALES:

Grado académico, Apellidos y nombres del experto	Maestro: FLORES SUTTA, WILFREDO
Cargo o institución donde labora	UNIVERSIDAD CATOLICA DE TRUJILLO – ULADECH
Nombre del instrumento de evaluación	Cuestionario de encuesta
Autor del instrumento	Leonardo Edgard Vilca Morales

II. ASPECTOS DE VALIDACIÓN: Calificar con 1, 2, 3 ó 4 cada ítem respecto a los criterios de relevancia, coherencia, suficiencia y claridad.

OPERACIONALIZACIÓN DE LA VARIABLE				CRITERIOS DE VALIDACIÓN					
VARIABLES	DIMENSIONES	ITEMS	ITEMS	RELEVANCIA	COHERENCIA	SUFICIENCIA	CLARIDAD	OBSERVACIÓN PROMEDIO PARCIAL	OBSERVACIÓN
Competencias en ciberseguridad Del operador Jurídico	Reconocimiento de tecnología para la seguridad de la información en el ciberespacio	¿Identifica usted problemas, riesgos y vulnerabilidades en las tecnologías de la información y las comunicaciones?	1	4	4	4	4	16	
		¿Identifica usted tecnología informática que le permita brindar seguridad a la información en el ciberespacio?	2	4	4	4	4	16	
		¿Aplica usted tecnología informática para la seguridad de la información en el ciberespacio?	3	4	4	4	4	16	
	Aplicación de procedimientos para la seguridad de la información en el ciberespacio	¿Realiza usted copias de seguridad de datos informáticos?	4	4	4	4	4	16	
		¿Identifica usted los límites de acceso y uso de las tecnologías de la información y las comunicaciones en la organización donde labora?	5	4	4	4	4	16	
		¿Aplica usted los protocolos de seguridad de la información en el ciberespacio que establece la organización donde labora?	6	4	4	4	4	16	
	Identificación de incidentes de seguridad de la información en el ciberespacio	¿Identifica usted la clasificación de un incidente de seguridad de la información en el ciberespacio?	7	4	4	4	4	16	
		¿Identifica usted las características de un incidente de seguridad de la información en el ciberespacio?	8	4	4	4	4	16	
		¿Identifica usted los riesgos y amenazas con relevancia jurídica de un incidente de seguridad de la información en el ciberespacio?	9	4	4	4	4	16	
	Respuesta a incidentes de seguridad de la información en el ciberespacio	¿Identifica usted los roles y responsabilidades ante un incidente de seguridad de la información en el ciberespacio?	10	4	4	4	4	16	
		¿Identifica usted el marco jurídico aplicable ante un incidente de seguridad de la información en el ciberespacio?	11	4	4	4	4	16	
		¿Aplica usted procedimientos en informática forense para investigar un incidente de seguridad de la información en el ciberespacio?	12	4	4	4	4	16	
Investigación penal de delitos informáticos	Investigación penal de delitos que afectan datos informáticos	Durante la investigación de un hecho en el cual se afectaron datos informáticos ¿Identificó si la conducta incriminada es delictuosa?	13	4	4	4	4	16	
		Durante la investigación de un hecho en el cual se afectaron datos informáticos ¿Identificó las circunstancias y/o móviles del hecho?	14	4	4	4	4	16	
		Durante la investigación de un hecho en el cual se afectaron datos informáticos ¿Identificó la identidad del autor, participe y víctimas?	15	4	4	4	4	16	
		Durante la investigación de un hecho en el cual se afectaron datos informáticos ¿Identificó la existencia del daño causado?	16	4	4	4	4	16	

	Investigación penal de delitos afectan sistemas informáticos	Durante la investigación de un hecho en la cual se afectaron sistemas informáticos ¿Identificó si la conducta incriminada es delictuosa?	17	4	4	4	4	16	
		Durante la investigación de un hecho en el cual se afectaron sistemas informáticos ¿Identificó las circunstancias y/o móviles del hecho?	18	4	4	4	4	16	
		Durante la investigación de un hecho en el cual se afectaron sistemas informáticos ¿Identificó la identidad del autor, participe y víctimas?	19	4	4	4	4	16	
		Durante la investigación de un hecho en el cual se afectaron sistemas informáticos ¿Identificó la existencia del daño causado?	20	4	4	4	4	16	
	Investigación penal de delitos que afectan otros bienes jurídicos de relevancia penal mediante la utilización de las tecnologías de la información y las comunicaciones	Durante la investigación de un hecho en el cual se afectaron otros bienes jurídicos mediante el uso de las tecnologías de la información y las comunicaciones ¿Identificó si la conducta incriminada es delictuosa?	21	4	4	4	4	16	
		Durante la investigación de un hecho en el cual se afectaron otros bienes jurídicos mediante el uso de las tecnologías de la información y las comunicaciones ¿Identificó las circunstancias y/o móviles del hecho?	22	4	4	4	4	16	
		Durante la investigación de un hecho en el cual se afectaron otros bienes jurídicos mediante el uso de las tecnologías de la información y las comunicaciones ¿Identificó la identidad del autor, participe y víctimas?	23	4	4	4	4	16	
		Durante la investigación de un hecho en el cual se afectaron otros bienes jurídicos mediante el uso de las tecnologías de la información y las comunicaciones ¿Identificó la existencia del daño causado?	24	4	4	4	4	16	
	PUNTAJE TOTAL							384	
	PUNTAJE EXPRESADA EN EL SISTEMA VIGESIMAL							20	

III.ESCALA DE CALIFICACIÓN: 20/40 x Puntaje Total = 0,5 x Puntaje total

CUALITATIVA		CUANTITATIVA	CUALITATIVA		CUANTITATIVA
E	MUY DEFICIENTE	00 - 05	C	REGULAR	11 - 13
D	DEFICIENTE	06 - 10	B	BUENO	14 - 17
			A	EXCELENTE	18 - (20)

IV. OPINIÓN DE APLICACIÓN: (X) VÁLIDO ( ) MEJORAR ( ) NO VALIDO

V. RECOMENDACIONES : Se recomienda la aplicación del instrumento

Huánuco.....de ..... del 2020	80172689	ULADECH CATÓLICA Mtro. Wilfredo Flores Sutta DOCENTE TUTOR INVESTIGADOR	962904725
Lugar y fecha	**DNI**	**Firma del experto**	**Teléfono**

HOJA DE INSTRUCCIONES PARA LA EVALUACIÓN

CATEGORÍA	CALIFICACIÓN	INDICADOR
RELEVANCIA El ítem es esencial o importante, es decir debe ser incluido.	1.No cumple con el criterio	El ítem puede ser eliminado sin que se vea afectada la medición de la dimensión.
	2.Bajo nivel	El ítem tiene una alguna relevancia, pero otro ítem puede estar incluyendo lo que mide este.
	3.Moderado nivel	El ítem es relativamente importante.
	4.Alto nivel	El ítem es muy relevante y debe ser incluido.
COHERENCIA El ítem tiene relación lógica con la dimensión o indicador.	1.No cumple con el criterio	El ítem puede ser eliminado sin que se vea afectada la medición de la dimensión.
	2.Bajo nivel	El ítem tiene una relación tangencial con la dimensión.
	3.Moderado nivel	El ítem tiene relación moderada con la dimensión que está midiendo.
	4.Alto nivel	El ítem tiene relación lógica con la dimensión.
SUFICIENCIA Los ítems que pertenecen a una misma dimensión bastan para obtener la medición de esta	1.No cumple con el criterio	Los ítems no son suficientes para medir la dimensión.
	2.Bajo nivel	Los ítems miden algún aspecto de la dimensión, pero no corresponden con la dimensión total.
	3.Moderado nivel	Se deben incrementar algunos ítems para poder evaluar la dimensión completamente.
	4.Alto nivel	Los ítems son suficientes.
CLARIDAD El ítem se comprende fácilmente, es decir sus sintácticas y semánticas son adecuadas	1.No cumple con el criterio	El ítem no es claro.
	2.Bajo nivel	El ítem requiere bastantes modificaciones o una modificación muy grande en el uso de las palabras que utilizan de acuerdo a su significado o por la ordenación de los mismos.
	3.Moderado nivel	Se requiere una modificación muy específica de algunos términos de ítem.
	4.Alto nivel	El ítem es claro, tiene semántica y sintaxis adecuada.

UNIVERSIDAD NACIONAL HERMILIO VALDIZAN
UNIDAD DE POSGRADO
MAESTRÍA EN DERECHO
MENCIÓN EN CIENCIAS PENALES

FICHA DE VALIDACIÓN POR JUICIO DE EXPERTOS

I.DATOS GENERALES:

Grado académico, Apellidos y nombres del experto	Doctor en Ciencias de la Educación. ECHEVARRÍA RODRÍGUEZ, Haiber Policarpo
Cargo o institución donde labora	UNHEVAL
Nombre del instrumento de evaluación	Cuestionario de encuesta
Autor del instrumento	Leonardo Edgard Vilca Morales

II. ASPECTOS DE VALIDACIÓN: Calificar con 1, 2, 3 o 4 cada ítem respecto a los criterios de relevancia, coherencia, suficiencia y claridad.

OPERACIONALIZACIÓN DE LA VARIABLE				CRITERIOS DE VALIDACIÓN					
VARIABLES	DIMENSIONES	ITEMS	ITEMS	RELEVANCIA	COHERENCIA	SUFICIENCIA	CLARIDAD	OBSERVACIÓN PROMEDIO PARCIAL	OBSERVACIÓN
Competencias en ciberseguridad Del operador Jurídico	Reconocimiento de tecnología para la seguridad de la información en el ciberespacio	¿Identifica usted problemas, riesgos y vulnerabilidades en las tecnologías de la información y las comunicaciones?	1	4	4	4	4	16	
		¿Identifica usted tecnología informática que le permita brindar seguridad a la información en el ciberespacio?	2	4	4	4	4	16	
		¿Aplica usted tecnología informática para la seguridad de la información en el ciberespacio?	3	4	4	4	4	16	
	Aplicación de procedimientos para la seguridad de la información en el ciberespacio	¿Realiza usted copias de seguridad de datos informáticos?	4	4	4	4	4	16	
		¿Identifica usted los límites de acceso y uso de las tecnologías de la información y las comunicaciones en la organización donde labora?	5	4	4	4	4	16	
		¿Aplica usted los protocolos de seguridad de la información en el ciberespacio que establece la organización donde labora?	6	4	4	4	4	16	
	Identificación de incidentes de seguridad de la información en el ciberespacio	¿Identifica usted la clasificación de un incidente de seguridad de la información en el ciberespacio?	7	4	4	4	4	16	
		¿Identifica usted las características de un incidente de seguridad de la información en el ciberespacio?	8	4	4	4	4	16	
		¿Identifica usted los riesgos y amenazas con relevancia jurídica de un incidente de seguridad de la información en el ciberespacio?	9	4	4	4	4	16	
	Respuesta a incidentes de seguridad de la información en el ciberespacio	¿Identifica usted los roles y responsabilidades ante un incidente de seguridad de la información en el ciberespacio?	10	4	4	4	4	16	
		¿Identifica usted el marco jurídico aplicable ante un incidente de seguridad de la información en el ciberespacio?	11	4	4	4	4	16	
		¿Aplica usted procedimientos en informática forense para investigar un incidente de seguridad de la información en el ciberespacio?	12	4	4	4	4	16	
Investigación penal de delitos informáticos	Investigación penal de delitos que afectan datos informáticos	Durante la investigación de un hecho en el cual se afectaron datos informáticos ¿Identificó si la conducta incriminada es delictuosa?	13	4	4	4	4	16	
		Durante la investigación de un hecho en el cual se afectaron datos informáticos ¿Identificó las circunstancias y/o móviles del hecho?	14	4	4	4	4	16	
		Durante la investigación de un hecho en el cual se afectaron datos informáticos ¿Identificó la identidad del autor, participe y víctimas?	15	4	4	4	4	16	

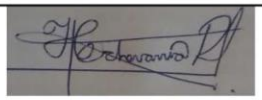
		Durante la investigación de un hecho en el cual se afectaron datos informáticos ¿Identificó la existencia del daño causado?	16	4	4	4	4	16	
	Investigación penal de delitos afectan sistemas informáticos	Durante la investigación de un hecho en la cual se afectaron sistemas informáticos ¿Identificó si la conducta incriminada es delictuosa?	17	4	4	4	4	16	
		Durante la investigación de un hecho en el cual se afectaron sistemas informáticos ¿Identificó las circunstancias y/o móviles del hecho?	18	4	4	4	4	16	
		Durante la investigación de un hecho en el cual se afectaron sistemas informáticos ¿Identificó la identidad del autor, participe y víctimas?	19	4	4	4	4	16	
		Durante la investigación de un hecho en el cual se afectaron sistemas informáticos ¿Identificó la existencia del daño causado?	20	4	4	4	4	16	
	Investigación penal de delitos que afectan otros bienes jurídicos de relevancia penal mediante la utilización de las tecnologías de la información y las comunicaciones	Durante la investigación de un hecho en el cual se afectaron otros bienes jurídicos mediante el uso de las tecnologías de la información y las comunicaciones ¿Identificó si la conducta incriminada es delictuosa?	21	4	4	4	4	16	
		Durante la investigación de un hecho en el cual se afectaron otros bienes jurídicos mediante el uso de las tecnologías de la información y las comunicaciones ¿Identificó las circunstancias y/o móviles del hecho?	22	4	4	4	4	16	
		Durante la investigación de un hecho en el cual se afectaron otros bienes jurídicos mediante el uso de las tecnologías de la información y las comunicaciones ¿Identificó la identidad del autor, participe y víctimas?	23	4	4	4	4	16	
		Durante la investigación de un hecho en el cual se afectaron otros bienes jurídicos mediante el uso de las tecnologías de la información y las comunicaciones ¿Identificó la existencia del daño causado?	24	4	4	4	4	16	
	PUNTAJE TOTAL							384	
	PUNTAJE EXPRESADA EN EL SISTEMA VIGESIMAL							20	

III.ESCALA DE CALIFICACIÓN: 20/40 x Puntaje Total = 0,5 x Puntaje total

CUALITATIVA		CUANTITATIVA	CUALITATIVA		CUANTITATIVA
E	MUY DEFICIENTE	00 - 05	C	REGULAR	11 - 13
D	DEFICIENTE	06 - 10	B	BUENO	14 - 17
			A	EXCELENTE	18 - (20)

IV. OPINIÓN DE APLICACIÓN: (X) VÁLIDO ( ) MEJORAR ( ) NO VALIDO

V. RECOMENDACIONES :

Huánuco 09 de noviembre del 2020	22669203		985726195
Lugar y fecha	**DNI**	**Firma del experto**	**Teléfono**

HOJA DE INSTRUCCIONES PARA LA EVALUACIÓN

CATEGORÍA	CALIFICACIÓN	INDICADOR
RELEVANCIA El ítem es esencial o importante, es decir debe ser incluido.	1.No cumple con el criterio	El ítem puede ser eliminado sin que se vea afectada la medición de la dimensión.
	2.Bajo nivel	El ítem tiene una alguna relevancia, pero otro ítem puede estar incluyendo lo que mide este.
	3.Moderado nivel	El ítem es relativamente importante.
	4.Alto nivel	El ítem es muy relevante y debe ser incluido.
COHERENCIA El ítem tiene relación lógica con la dimensión o indicador.	1.No cumple con el criterio	El ítem puede ser eliminado sin que se vea afectada la medición de la dimensión.
	2.Bajo nivel	El ítem tiene una relación tangencial con la dimensión.
	3.Moderado nivel	El ítem tiene relación moderada con la dimensión que está midiendo.
	4.Alto nivel	El ítem tiene relación lógica con la dimensión.
SUFICIENCIA Los ítems que pertenecen a una misma dimensión bastan para obtener la medición de esta	1.No cumple con el criterio	Los ítems no son suficientes para medir la dimensión.
	2.Bajo nivel	Los ítems miden algún aspecto de la dimensión, pero no corresponden con la dimensión total.
	3.Moderado nivel	Se deben incrementar algunos ítems para poder evaluar la dimensión completamente.
	4.Alto nivel	Los ítems son suficientes.
CLARIDAD El ítem se comprende fácilmente, es decir sus sintácticas y semánticas son adecuadas	1.No cumple con el criterio	El ítem no es claro.
	2.Bajo nivel	El ítem requiere bastantes modificaciones o una modificación muy grande en el uso de las palabras que utilizan de acuerdo a su significado o por la ordenación de los mismos.
	3.Moderado nivel	Se requiere una modificación muy especifica de algunos términos de ítem.
	4.Alto nivel	El ítem es claro, tiene semántica y sintaxis adecuada.

NOTA BIOGRÁFICA

Leonardo Edgard Vilca Morales nació en el distrito de Amarilis, provincia y departamento de Huánuco, en la República del Perú, el 07 de diciembre de 1994, hijo de la maestra Marilú Morales Calderón y el maestro Edgar Vilca Figueredo, realizó sus estudios educación primaria en la Institución Educativa N° 32575 – Panao, y parte de sus estudios en educación secundaria en la Gran Unidad Escolar Leoncio Prado de Huánuco, los mismos que finalizó en la Institución Educativa Springfield Collegue Huánuco (ahora Springfield School Huánuco). Cursó sus estudios universitarios en la Facultad de Derecho y Ciencias Políticas de la Universidad Nacional Hermilio Valdizán de Huánuco, obteniendo el grado de Bachiller en Derecho. Cuenta con título a nombre de la nación como abogado, y es conciliador extrajudicial especializado en familia acreditado por el Ministerio de Justicia y Derechos Humanos, cuenta además con estudios universitarios en la escuela académico profesional de administración de la Universidad Católica los Ángeles de Chimbote, y estudios de especialización concluidos en derecho informático y ciberseguridad por la Universidad Continental.

ACTA DE DEFENSA DE TESIS DE MAESTRO

En la Plataforma Microsoft Teams de la Escuela de Posgrado, siendo las **13:00h,** del día viernes **21 DE OCTUBRE DE 2022** ante los Jurados de Tesis constituido por los siguientes docentes:

Dr. Amancio Ricardo ROJAS COTRINA	Presidente
Dr. Jose Luis MANDUJANO RUBIN	Secretario
Dr. Leoncio Enrique VASQUEZ SOLIS	Vocal

Asesor (a) de tesis: Dr. Cesar Alfonso NAJAR FARRO (Resolución N° 01140-2020-UNHEVAL/EPG-D)

El aspirante al Grado de Maestro en Derecho, mención en Ciencias Penales, Don Leonardo Edgard VILCA MORALES.

Procedió al acto de Defensa:

Con la exposición de la Tesis titulado: **"COMPETENCIAS EN CIBERSEGURIDAD DEL OPERADOR JURÍDICO Y LA INVESTIGACIÓN PENAL DE CIBERDELITOS EN EL DISTRITO FISCAL DE HUÁNUCO DURANTE EL PERIODO 2020".**

Respondiendo las preguntas formuladas por los miembros del Jurado y público asistente.

Concluido el acto de defensa, cada miembro del Jurado procedió a la evaluación del aspirante al Grado de Maestro, teniendo presente los criterios siguientes:

a) Presentación personal.
b) Exposición: el problema a resolver, hipótesis, objetivos, resultados, conclusiones, los aportes, contribución a la ciencia y/o solución a un problema social y recomendaciones.
c) Grado de convicción y sustento bibliográfico utilizados para las respuestas a las interrogantes del Jurado y público asistente.
d) Dicción y dominio de escenario.

Así mismo, el Jurado plantea a la tesis **las observaciones** siguientes:

.....
.....

Obteniendo en consecuencia el Maestrista la Nota de.....Diecisiete..... (17)
Equivalente a .....Muy bueno....., por lo que se declara .....aprobado.....
(Aprobado o desaprobado)

Los miembros del Jurado firman el presente **ACTA** en señal de conformidad, en Huánuco, siendo las..14:44.. horas de 21 de octubre de 2022.

.....
PRESIDENTE
DNI Nº .....04025628.....

.....
SECRETARIO
DNI Nº .....41879366.....

.....
VOCAL
DNI Nº .....22409006.....

Leyenda:
19 a 20: ExcelenteS
17 a 18: Muy Bueno
14 a 16: Bueno

(Resolución Nº 02922-2022-UNHEVAL/EPG)

UNIVERSIDAD NACIONAL HERMILIO VALDIZÁN

ESCUELA DE POSGRADO

CONSTANCIA DE ORIGINALIDAD

El que suscribe:

Dr. Amancio Ricardo Rojas Cotrina

HACE CONSTAR:

Que, la tesis titulada: ***"COMPETENCIAS EN CIBERSEGURIDAD DEL OPERADOR JURÍDICO Y LA INVESTIGACIÓN PENAL DE CIBERDELITOS EN EL DISTRITO FISCAL DE HUÁNUCO DURANTE EL PERIODO 2020",*** *realizado por el Maestrista en Derecho, mención en Ciencias Penales,* ***Leonardo Edgard VILCA MORALES,*** *cuenta con un* ***índice de similitud del 13%,*** *verificable en el Reporte de Originalidad del software* ***Turnitin****. Luego del análisis se concluye que cada una de las coincidencias detectadas no constituyen plagio; por lo expuesto, la Tesis cumple con todas las normas para el uso de citas y referencias, además de presentar un índice de similitud menor al 20% establecido en el Reglamento General de Grados y Títulos de la Universidad Nacional Hermilio Valdizán.*

Cayhuayna, 28 de setiembre de 2022.

UNIVERSIDAD NACIONAL "HERMILIO VALDIZÁN" ESCUELA DE POSGRADO DIRECTOR HUÁNUCO

Dr. Amancio Ricardo Rojas Cotrina
DIRECTOR DE LA ESCUELA DE POSGRADO

SECC

UNHEVAL UNIVERSIDAD NACIONAL HERMILIO VALDIZÁN | VICERRECTORADO DE INVESTIGACIÓN | DIRECCIÓN DE INVESTIGACIÓN

AUTORIZACIÓN DE PUBLICACIÓN DIGITAL Y DECLARACIÓN JURADA DEL TRABAJO DE INVESTIGACIÓN PARA OPTAR UN GRADO ACADÉMICO O TÍTULO PROFESIONAL

1. Autorización de Publicación: *(Marque con una "X")*

Pregrado		Segunda Especialidad		Posgrado:	Maestría	X	Doctorado	

Pregrado (*tal y como está registrado en **SUNEDU)***

Facultad	
Escuela Profesional	
Carrera Profesional	
Grado que otorga	
Título que otorga	

Segunda especialidad (*tal y como está registrado en **SUNEDU)***

Facultad	
Nombre del programa	
Título que Otorga	

Posgrado (*tal y como está registrado en **SUNEDU)***

Nombre del Programa de estudio	DERECHO, MENCIÓN EN CIENCIAS PENALES
Grado que otorga	MAESTRO EN DERECHO, MENCIÓN EN CIENCIAS PENALES

2. Datos del Autor(es): *(Ingrese todos los **datos** requeridos **completos**)*

Apellidos y Nombres:	LEONARDO EDGARD VILCA MORALES							
Tipo de Documento:	**DNI**	X	**Pasaporte**		**C.E.**		**Nro. de Celular:**	999013464
Nro. de Documento:	71314572						**Correo Electrónico:**	lvmevolution@gmail.com

Apellidos y Nombres:								
Tipo de Documento:	**DNI**		**Pasaporte**		**C.E.**		**Nro. de Celular:**	
Nro. de Documento:							**Correo Electrónico:**	

Apellidos y Nombres:								
Tipo de Documento:	**DNI**		**Pasaporte**		**C.E.**		**Nro. de Celular:**	
Nro. de Documento:							**Correo Electrónico:**	

3. Datos del Asesor: *(Ingrese todos los **datos** requeridos **completos según DNI**, no es necesario indicar el Grado Académico del Asesor)*

¿El Trabajo de Investigación cuenta con un Asesor?: *(marque con una "**X**" en el recuadro del costado, según corresponda)*							**SI**	X	**NO**	
Apellidos y Nombres:	NAJAR FARRO CESAR ALFONSO					**ORCID ID:**	0000-0003-2266-1451			
Tipo de Documento:	**DNI**	X	**Pasaporte**		**C.E.**		**Nro. de documento:**	22513421		

4. Datos del Jurado calificador: *(Ingrese solamente los **Apellidos y Nombres completos según DNI**, no es necesario indicar el Grado Académico del Jurado)*

Presidente:	ROJAS COTRINA AMANCIO RICARDO
Secretario:	MANDUJANO RUBIN JOSE LUIS
Vocal:	VASQUEZ SOLIS LUIS ENRIQUE
Vocal:	
Vocal:	
Accesitario	

UNHEVAL UNIVERSIDAD NACIONAL HERMILIO VALDIZÁN | VICERRECTORADO DE INVESTIGACIÓN | DIRECCIÓN DE INVESTIGACIÓN

5. Declaración Jurada: *(Ingrese todos los **datos** requeridos **completos**)*

a) **Soy Autor (a) (es) del Trabajo de Investigación Titulado:** *(Ingrese el título tal y como está registrado en el **Acta de Sustentación**)*
COMPETENCIAS EN CIBERSEGURIDAD DEL OPERADOR JURÍDICO Y LA INVESTIGACIÓN PENAL DE CIBERDELITOS EN EL DISTRITO FISCAL DE HUÁNUCO DURANTE EL PERIODO 2020
b) **El Trabajo de Investigación fue sustentado para optar el Grado Académico o Título Profesional de:** *(tal y como está registrado en **SUNEDU**)*
MAESTRO EN DERECHO, MENCIÓN EN CIENCIAS PENALES
c) El Trabajo de investigación no contiene plagio (ninguna frase completa o párrafo del documento corresponde a otro autor sin haber sido citado previamente), ni total ni parcial, para lo cual se han respetado las normas internacionales de citas y referencias.
d) El trabajo de investigación presentado no atenta contra derechos de terceros.
e) El trabajo de investigación no ha sido publicado, ni presentado anteriormente para obtener algún Grado Académico o Título profesional.
f) Los datos presentados en los resultados (tablas, gráficos, textos) no han sido falsificados, ni presentados sin citar la fuente.
g) Los archivos digitales que entrego contienen la versión final del documento sustentado y aprobado por el jurado.
h) Por lo expuesto, mediante la presente asumo frente a la Universidad Nacional Hermilio Valdizan (en adelante LA UNIVERSIDAD), cualquier responsabilidad que pudiera derivarse por la autoría, originalidad y veracidad del contenido del Trabajo de Investigación, así como por los derechos de la obra y/o invención presentada. En consecuencia, me hago responsable frente a LA UNIVERSIDAD y frente a terceros de cualquier daño que pudiera ocasionar a LA UNIVERSIDAD o a terceros, por el incumplimiento de lo declarado o que pudiera encontrar causas en la tesis presentada, asumiendo todas las cargas pecuniarias que pudieran derivarse de ello. Asimismo, por la presente me comprometo a asumir además todas las cargas pecuniarias que pudieran derivarse para LA UNIVERSIDAD en favor de terceros con motivo de acciones, reclamaciones o conflictos derivados del incumplimiento de lo declarado o las que encontraren causa en el contenido del trabajo de investigación. De identificarse fraude, piratería, plagio, falsificación o que el trabajo haya sido publicado anteriormente; asumo las consecuencias y sanciones que de mi acción se deriven, sometiéndome a la normatividad vigente de la Universidad Nacional Hermilio Valdizan.

6. Datos del Documento Digital a Publicar: *(Ingrese todos los **datos** requeridos **completos**)*

Ingrese solo el año en el que sustentó su Trabajo de Investigación: *(Verifique la Información en el **Acta de Sustentación**)*						2022	
Modalidad de obtención del Grado Académico o Título Profesional: *(Marque con **X** según Ley Universitaria con la que inició sus estudios)*	**Tesis**	X	**Tesis Formato Artículo**		**Tesis Formato Patente de Invención**		
	Trabajo de Investigación		**Trabajo de Suficiencia Profesional**		**Tesis Formato Libro, revisado por Pares Externos**		
	Trabajo Académico		**Otros** *(especifique modalidad)*				

Palabras Clave: *(solo se requieren 3 palabras)*	CIBERSEGURIDAD	CIBERDELITOS	INVESTIGACION PENAL

Tipo de Acceso: *(Marque con **X** según corresponda)*	**Acceso Abierto**	X	**Condición Cerrada** (*)		
	Con Periodo de Embargo (*)		**Fecha de Fin de Embargo:**		

¿El Trabajo de Investigación, fue realizado en el marco de una Agencia Patrocinadora? *(ya sea por financiamientos de proyectos, esquema financiero, beca, subvención u otras; marcar con una "**X**" en el recuadro del costado según corresponda):*	**SI**		**NO**	X
Información de la Agencia Patrocinadora:				

El trabajo de investigación en digital y físico tienen los mismos registros del presente documento como son: Denominación del programa Académico, Denominación del Grado Académico o Título profesional, Nombres y Apellidos del autor, Asesor y Jurado calificador tal y como figura en el Documento de Identidad, Titulo completo del Trabajo de Investigación y Modalidad de Obtención del Grado Académico o Título Profesional según la Ley Universitaria con la que se inició los estudios.

UNHEVAL UNIVERSIDAD NACIONAL HERMILIO VALDIZÁN | VICERRECTORADO DE INVESTIGACIÓN | DIRECCIÓN DE INVESTIGACIÓN | RI UNHEVAL | DI UNHEVAL

7. **Autorización de Publicación Digital:**

A través de la presente. Autorizo de manera gratuita a la Universidad Nacional Hermilio Valdizán a publicar la versión electrónica de este Trabajo de Investigación en su Biblioteca Virtual, Portal Web, Repositorio Institucional y Base de Datos académica, por plazo indefinido, consintiendo que con dicha autorización cualquier tercero podrá acceder a dichas páginas de manera gratuita pudiendo revisarla, imprimirla o grabarla siempre y cuando se respete la autoría y sea citada correctamente. Se autoriza cambiar el contenido de forma, más no de fondo, para propósitos de estandarización de formatos, como también establecer los metadatos correspondientes.

Firma: 		
Apellidos y Nombres:	VILCA MORALES LEONARDO EDGARD	**Huella Digital**
DNI:	71314572	
Firma:		
Apellidos y Nombres:		**Huella Digital**
DNI:		
Firma:		
Apellidos y Nombres:		**Huella Digital**
DNI:		
Fecha: 30/12/2022		

Nota:

- ✓ No modificar los textos preestablecidos, conservar la estructura del documento.
- ✓ Marque con una **X** en el recuadro que corresponde.
- ✓ Llenar este formato de forma digital, con tipo de letra **calibri, tamaño de fuente 09**, manteniendo la alineación del texto que observa en el modelo, sin errores gramaticales *(recuerde las mayúsculas también se tildan si corresponde)*.
- ✓ La información que escriba en este formato debe coincidir con la información registrada en los demás archivos y/o formatos que presente, tales como: DNI, Acta de Sustentación, Trabajo de Investigación (PDF) y Declaración Jurada.
- ✓ Cada uno de los datos requeridos en este formato, es de carácter obligatorio según corresponda.