UNIVERSIDAD PERUANA DE LAS AMÉRICAS

ESCUELA PROFESIONAL DE DERECHO

TRABAJO DE INVESTIGACIÓN

"IMPORTANCIA DE LA EVIDENCIA DIGITAL EN LA RESOLUCIÓN DE CASOS DE LA LEY DE DELITOS INFORMÁTICOS - LEY N° 30096 Y MODIFICATORIAS CON LA LEY Nº 30171 EN LA DIVISIÓN DE ALTA TECNOLOGÍA PNP, LIMA, 2022"

PARA OPTAR EL TITULO PROFESIONAL DE ABOGADO

AUTOR:

RAMÍREZ CABRERA, ALAIN HEBERT

(CODIGO ORCID: 0000-0002-6517-5704)

ASESOR:

Mg. PEREZ LOPEZ, JORGE ADALBERTO

(CODIGO ORCID: 0000-0002-4695-389X)

LÍNEAS DE INVESTIGACIÓN: DERECHO PENAL, CIVIL Y CORPORATIVO

LIMA, PERÚ

FEBRERO, 2022

DEDICATORIA

A Dios todopoderoso que ha puesto en mi vida los momentos perfectos que me han permitido concluir mis estudios universitarios y haber alcanzado los conocimientos doctrinarios del derecho, a mis adorables padres, a mi abnegada esposa Diana que nunca me dejó caer en los momentos más difíciles, su brazo ha sido el soporte moral más grande durante mis estudios y finalmente a mis hijos Olga, Rosa y Alain, que su sola existencia ha trascendido en lo más profundo de mi alma y han sido de gran motivación durante mi formación profesional.

AGRADECIMIENTO

Agradezco a mi asesor por brindarme una brillante orientación en el logro y construcción del presente estudio, sus aportes y recomendaciones fueron de gran ayuda para alcanzar los objetivos deseados. Igualmente, las consideraciones a mis docentes que supieron sembrar los conocimientos doctrinarios del derecho sus experiencias han sido de mucha utilidad.

Finalmente, a mis grandes amigos y compañeros de universidad que han sido el soporte moral y de motivación desde el inicio y término de mi vida universitaria, a ellos que siempre estuvieron presentes su lealtad tiene un valor infinito.

RESUMEN

El estudio que se presenta tuvo como meta académica conocer la relación que existe en cuanto a la importancia de la evidencia digital en la resolución de casos de delitos informáticos en la División de Alta Tecnología de la Policía Nacional del Perú (Divindat PNP), Lima, 2022. La elaboración del trabajo fluye en un escenario donde la tecnología viene avanzando exponencialmente en todo el mundo, situación que ha obligado a las personas a cambiar sus hábitos y normas de convivencia como normalmente los hacía, esta misma necesidad ha hecho que aquellas informaciones que se encontraban dentro del vínculo personal tenga que exponerse a través de componentes tecnológicos como el celular, las tablets, computadoras, entre otras y con el uso de plataformas de internet se comparta en las redes y otros sistemas de comunicación, este escenario es aprovechado por ciberdelincuentes para acceder a los sistemas informáticos y apropiarse de estos datos, beneficiarse de ellos, lucrarse y; posteriormente los agraviados se ven en la obligación de interponer sus denuncias por delitos informáticos. Consecuentemente al analizarse la problemática se ha logrado determinar un elevado nexo de la evidencia digital en la resolución de casos de delitos informáticos en la Divindat PNP, Lima, 2022. El proyecto de indagación permite ofrecer un importante aporte académico en la búsqueda de informaciones y archivos relacionados a las variables evidencia digital y delitos informáticos, de igual manera los datos obtenidos, fueron en base a tesis de grado, fuentes de internet y revistas indexadas, los cuales han ofrecido grandes aportes doctrinarios y el surgimiento de nuevas líneas de investigación.

Palabras claves: delitos informáticos, evidencia digital, valor probatorio

ABSTRACT

The study that is presented had as an academic goal, to know the relationship that exists regarding the importance of digital evidence in the resolution of computer crime cases in the High Technology Division of the National Police of Peru (Divindat PNP), Lima , 2022. The elaboration of the work flows in a scenario where technology has been advancing exponentially throughout the world, a situation that has forced people to change their habits and rules of coexistence as they normally did, this same need has made that information that were within the personal bond have to be exposed through technological components such as cell phones, tablets, computers, among others and with the use of internet platforms to be shared on networks and other communication systems, this scenario is used by cybercriminals to access computer systems and appropriate this data, benefit from it, profit from it and; Subsequently, the aggrieved are obliged to file their complaints for computer crimes. Consequently, when analyzing the problem, it has been possible to determine a high nexus of digital evidence in the resolution of computer crime cases in the Divindat PNP, Lima, 2022. The research project allows us to offer an important academic contribution in the search for information and files Related to the variables digital evidence and computer crimes, in the same way the data obtained were based on thesis, internet sources and indexed journals, which have offered great doctrinal contributions and the emergence of new lines of research.

Keywords: computer crimes, digital evidence, probative value

TABLA DE CONTENIDO

INTRODUCCIÓN

El estudio que se ha tratado emerge dentro del contexto de los delitos informáticos y de las diversas modalidades que existen en cuanto a su comisión y lo importante que es poder identificar las características propias para lograr establecer en qué momento se materializa el delito, el estudio tiene como principal objetivo conocer de qué manera la evidencia digital contribuye y aporta en la resolución de casos de la Ley Nº 30096 y sus modificatorias con la Ley Nº 30171 en la Divindat PNP, Lima, 2022.

Los “ciberdelitos” actualmente representan un grave problema que se viene replicando en distintos países de mundo, estos delitos constituyen actos que lesionan a todo el sistema jurídico peruano y que es ejecutado por personas inescrupulosas que mediante la utilización de la informática y otras tecnologías y; a través de una plataforma de internet afectan a los sistemas de información y sus contenidos, aunado a esta situación se encuentra el avance de la tecnología global que ha permitido que los ciberdelincuentes amplíen sus zonas de operaciones.

Particularmente en el Perú, en los últimos años y añadido la grave situación sanitaria a nivel mundial por la presencia del coronavirus 19 (Covid 19), que ha obligado a la sociedad a desarrollar sus actividades económicas, financieras, bancarias, laborales y sociales a través del uso de computadoras y del internet, ha provocado el incremento desmedido de denuncias por este tipo de delitos, por lo que ha conllevado que los operadores de justicia enfrenten con medios legales a los autores y/o responsables de la comisión de estos ilícitos penales, dicha labor implica la formación y capacitación en nuevas herramientas tecnológicas que permitan fortalecer la lucha contra los ciberdelincuentes y dentro de estos actores se encuentra la Divindat PNP, que actualmente viene desarrollando una ardua labor pese a la escases de recursos humanos y tecnológicos; por su parte el Estado Peruano como política pública para darle frente a esta nueva ola criminal tecnológica ha visto por conveniente promulgar la Ley

Nº 30096 – Ley de Delitos Informáticos y sus modificatorias con la Ley Nº 30171, dentro de la estructura de la citada norma podemos encontrar las diversas modalidades cada una de ellas con sus respectivas características.

En cuanto a la importancia de la evidencia digital se señala que esta constituye toda información generada, transmitida y archivada en dispositivos de tipo electrónico y que puedan utilizarse durante los procesos judiciales como medio de prueba, teniendo como principal característica que esta tiene que haberse registrado y producido en el mismo lugar de la intervención y que dicha información nos permita conocer la inalterabilidad de los dispositivos originales por lo que los registros deben corresponder al mismo momento en que fueron recogidos.

1. PROBLEMA DE INVESTIGACIÓN

1.1 Descripción de la Realidad Problemática

En estos tiempos nuevos el crecimiento de la ciencia y otras tecnologías han provocado que las personas y empresas tengan que asumir nuevos retos en su vida implementando el recurso de lo digital, ya que ante la gran cantidad de información valiosa que se produce, registra y circula en los medios digitales los delitos y denuncias informáticas se han elevado en todo el mundo. En este contexto según datos del Sistema de Registro de Denuncias de Investigación Criminal de la PNP (SIRDIC PNP) y de la Divindat PNP, el año 2020 a nivel nacional se presentaron (9,787) denuncias por delitos informáticos y hasta octubre del año 2021 se presentaron en nuestro país (12,827) denuncias por este mismo tipo de ilícitos lo que representa un incremento significativo de denuncias.

Por otro lado, en el escenario internacional en el país del Ecuador se ha conocido que los operadores de justicia presentan un elevado desconocimiento respecto a la informática y otras tecnologías, situación que ha generado que la evidencia digital como instrumento probatorio en los procesos penales sean de muy bajo nivel; igualmente, se asocia a esta situación la ausencia de una norma legal adecuada para combatir estos delitos, lo que está provocando la inaplicabilidad de procedimientos apropiados para las investigaciones, dichas falencias vienen dando lugar a la impunidad de los ciberdelincuentes; por lo que, se hace necesario que los peritos encargados de recoger la evidencia digital tengan que ampliar sus conocimientos en informática y otros medios tecnológicos (Bolaños y Gómez, 2015).

Ante el aumento excesivo de denuncias por Delitos Informáticos está claro que los aparatos tecnológicos como celulares, CPU, Laptops y otros, constituyen una fuente valiosa de donde se pueden obtener amplia y variada información de tal forma que estos datos debidamente recogidos y almacenados por peritos informáticos en

otros componentes tecnológicos de registro se constituyan en importantes medios probatorios que le permitan a los operadores de justicia tomar decisiones más apropiadas frente a los hechos delictivos informáticos (Gómez 2020).

Igualmente por los argumentos expuestos y considerando los actuales escenarios es de mucha vitalidad identificar y conocer como la evidencia digital influye en la resolución de los Delitos Informáticos – Ley N° 30096 y sus modificatorias con la Ley N° 30171 en la Divindat PNP, de tal manera que nos permita contextualizar y evaluar su importancia y también considerar la presencia del Covid 19, donde las personas utilizan con mucha frecuencia diferentes equipos tecnológicos y consecuentemente existe un alto tráfico de informaciones, situación muy bien aprovechada por delincuentes informáticos para la comisión de sus ilícitos.

1.1.1 Formulación del Problema General

- ¿De qué manera la importancia de la evidencia digital influye en la resolución de casos de Delitos Informáticos - Ley Nº 30096 y sus modificatorias con la Ley Nº 30171 en la Divindat PNP, Lima, 2022?

1.1.2 Problemas Específicos

- ¿De qué manera la importancia de la evidencia digital influye en la resolución de casos de delitos contra datos y sistemas informáticos, en la Divindat PNP, Lima, 2022?
- ¿De qué manera la importancia de la evidencia digital influye en la resolución de casos de delitos informáticos contra el patrimonio, en la Divindat PNP, Lima, 2022?
- ¿De qué manera la importancia de la evidencia digital influye en la resolución de casos de delitos informáticos contra la fe pública, en la Divindat PNP, Lima, 2022?

1.2 Objetivos de la Investigación

Objetivo general

- Determinar la influencia de la importancia de la evidencia digital en la resolución de casos de delitos informáticos - Ley Nº 30096 y sus modificatorias con la Ley Nº 30171 en la Divindat PNP, Lima, 2022.

Objetivos específicos

- Determinar la influencia de la importancia de la evidencia digital en la resolución de casos de delitos contra datos y sistemas informáticos, en la Divindat PNP, Lima, 2022.
- Determinar la influencia de la importancia de la evidencia digital en la resolución de casos de delitos informáticos contra el patrimonio, en la Divindat PNP, Lima, 2022.
- Determinar la influencia de la importancia de la evidencia digital en la resolución de casos de delitos informáticos contra la fe pública, en la Divindat PNP, Lima, 2022.

1.3 Justificación e Importancia

Referente al punto de vista práctico, el estudio será muy valioso y trascendental ya que, nos dará un contexto bien desarrollado en cuanto a las variables que se buscó investigar como son la evidencia digital y delitos informáticos – Ley N° 30096 y sus modificatorias con la Ley N° 30171; asimismo, servirá como base doctrinaria al repositorio de la universidad y del propio país, toda vez que, no se han encontrado muchos estudios que nos permita conocer cuál es la influencia de la evidencia digital en la resolución de casos de delitos informáticos. Por tal motivo, se ha logrado identificar y estudiar la relación que existe entre las dos variables (independiente y dependiente), permitiendo conocer resultados óptimos y favorables.

En cuanto al punto de vista teórico, el trabajo ha sido estructurado con informaciones bien sostenidas en cada variable de investigación, de igual forma se ha logrado trabajar con amplia doctrina sobre herramientas de la información y TIC, así como de conceptos jurídicos relacionados a los delitos informáticos los mismos que han sido obtenidos de fuentes abiertas debidamente verificadas como son los repositorios académicos, revistas calificadas, libros, documentos públicos y archivos los cuales han tenido una función muy importante para poder analizar y/o evaluar las informaciones, por lo que, consecuentemente con los datos recolectados han ayudado a enriquecer y dar una mejor perspectiva a la investigación realizada; igualmente esta será de mucha utilidad para otras investigaciones o como un instrumento de consulta a futuro.

Desde el punto de vista metodológico, en el trabajo realizado se ha visto por conveniente usar aquellos medios de estudio necesarios, los mismos que, van a contribuir ampliamente para obtener los mejores resultados; este proceso metodológico va a contextualizar en todas sus formas al problema de investigación; de igual manera nos va a permitir identificar la relación que existe entre las dos variables, así como evidenciar como se vincula la evidencia digital con los Delitos Informáticos – Ley N° 30096 y sus modificatorias con la Ley N° 30171 y mostrar las reacciones que se van a generar cuando estas dos variables (Dependiente e Independiente) se junten.

2. MARCO TEÓRICO

2.1 Antecedentes

Internacionales

En cuanto a la experiencia extranjera el autor Tovar y Amariles (2015), realizó un trabajo de investigación el cual tuvo como principal meta identificar la existencia de medidas de prevención por parte del Estado Colombiano destinados a evitar que sus habitantes sean potenciales víctimas por delitos informáticos así como buscó establecer y reconocer cuales eran las líneas de acción que se están empleando para enfrentar y frenar a estos ilícitos, la investigación fue de tipo descriptiva de análisis jurisprudencial, obteniéndose como resultado que la modalidad que con mayor frecuencia ocurre en torno a los delitos informáticos son la sustracción de datos a través de equipos tecnológicos, la violación de sistemas de cómputo con datos personales y el ingreso irregular a componentes informáticos; igualmente, el estudio ha permitido conocer que existen una diversidad de formas de actuar (tipologías) en cuanto a estos ilícitos por lo que consecuentemente los procedimientos y metodologías de investigación que se van a emplear en su lucha son diferentes y obviamente ello implica que el recojo de las evidencias digitales se realicen en atención a sus propias características y/o modalidades, en cuanto a los resultados que se logren alcanzar estos dependerán del expertiz del perito informático encargado de recolectar y registrar los datos.

Del mismo modo la autora Rodríguez (2018), ha formulado su tesis de maestría cuyo argumento principal de análisis y estudio ha sido lograr organizar y estructurar una lista que muestren las diversas modalidades por delitos informáticos y que estos se hayan generado a través de las plataformas de redes sociales en el país del Ecuador, la investigación fue de tipo exploratorio, descriptivo, de método inductivo deductivo, cuyo resultado ha permitido conocer e identificar cuáles son las características principal en cuanto a su conducta criminal y buscar adecuarla al tipo

de delito cometido, este estudio ha permitido determinar que la legislación ecuatoriana no esta tomando en cuenta en sus procesos y procedimientos a esta clasificación delictiva por lo está constituyendo actualmente un alarmante y grave vacío legal que está conduciendo los procesos judiciales a alguna forma de impunidad para estos criminales; igualmente, la investigación ha permitido conocer que un gran porcentaje de la población ecuatoriana no tienen conocimiento de la existencia de esta clase de delitos así como de las diversas formas de operar por estos delincuentes de la informática.

Nacionales.

Por su parte el investigador Osco (2019) a fin de alcanzar su distinción de magister ha realizado un estudio que ha tenido como línea de investigación lograr e identificar los protocolos, diligencias y actuaciones que ejecutan el personal especializado en el momento de la identificación y registro técnico de la evidencia digital; asimismo, determinar cómo se desarrollan los mecanismos de protección y traslado de estas; igualmente, dentro de este escenario se ha tratado de conocer que medios técnicos se vienen utilizando actualmente para el manejo y tratamiento adecuado de la evidencia digital y la forma como se comportan o actúan en concordancia al marco legal normativo de nuestro país, la metodología de investigación que se ha utilizado en el trabajo ha sido cuantitativa de tipo de básica, de nivel descriptivo, de enfoque cualitativo, de diseño no experimental. Los actores que han participado en el trabajo, todos ellos tienen un vínculo directo en cuanto al tratamiento e investigaciones por delitos cometidos por delincuentes informáticos, cuyo aporte y expertiz ha sido de vital importancia toda vez que ha permitido que se entienda que la evidencia digital como medio de prueba en los procesos judiciales por si sola no representan un medio contundente para poder demostrar un delito y quien lo ha perpetrado, si es que esta no tiene una adecuada descripción y procesamiento en la norma legal que la regula, del mismo modo, el tratado contextualiza que personal

de las instituciones involucradas no se encuentran debidamente formados y actualizados en nuevas herramientas tanto en lo procedimental como en lo tecnológico para la manipulación de la evidencia digital, situación que genera mucha incertidumbre y en algunos casos impunidad.

En la misma línea de investigación el autor Espinoza (2017) en su estudio realizado el objeto central ha sido contextualizar doctrinariamente la noción de "Derecho Penal informático" y como esta se encuentra desarrollada dentro del sistema legal peruano desde el punto de vista penal; asimismo, se vincula a esta situación como es que los actores que realizan investigaciones en torno a estos delitos desarrollan sus protocolos y procedimientos para su lucha eficaz. La metodología utilizada en el trabajo ha sido cuantitativa; igualmente, como producto de la labor académica realizada se encuentran el hecho de haber generado nuevos conocimientos doctrinarios respecto al "Derecho Penal Informático" y las normas de carácter legal donde tiene su aplicación, cuyos fundamentos y conceptos básicos serán de mucha utilidad para las investigaciones futuras por ciberdelitos.

2.2 Bases Teóricas

2.2.1 Doctrina de Delitos Informáticos

2.2.1.1 Definición de evidencia digital

Para contextualizar la evidencia digital inicialmente tenemos que identificar que todas las informaciones que quedan registradas en los equipos de cómputo (celulares, tablets, CPC, otros) y estos datos asociados a hechos de tipo criminal, mediante el uso de técnicas y equipos especiales serán identificados, registrados y guardados en otros medios tecnológicos más sofisticados, esta actividad es realizada por un perito informático debidamente

calificado y autorizado, es a partir de ese momento que adquiere su naturaleza propia de evidencia digital, el cual con una correcta cadena de custodia será incorporada a un proceso judicial y servirá a los magistrados para una correcta toma de decisiones (Jijena, 2008).

2.2.1.2 Admisibilidad y Autenticidad de la Evidencia Digital

En la evidencia digital para que sean admitidas las informaciones que están contenidas en ella, necesariamente tiene que estar correctamente registrada y almacenada electrónicamente de tal manera que los datos incriminados y recuperados deben ser los mismos que fueron ubicados en la zona de investigación, permitiendo a los operadores de justicia identificar directamente a la persona que accedió a los sistemas informáticos y atentó contra los datos de información (Rico, 2003)

Respecto a la autenticidad de la evidencia digital y presentada esta como medio de prueba durante la investigación de casos por Delitos Informáticos se deben considerar dos principios muy fundamentales para su verdadero valor, uno es que esta se encuentre registrada e identificada en el lugar donde ha sido recogida y el otro es que, la evidencia no pueda ser alterada y/o modificada de los equipos técnicos primigenios, mientras que su autenticidad se basa en que estas deben mantener la originalidad tal cual se fueron halladas desde su inicio (Guerrero, 2002).

En este orden de ideas lo más conveniente es que se realicen los procedimientos más adecuados y técnicos considerando que un buen registro y recojo le va a permitir al perito

informático encontrar las informaciones más importantes, de ocurrir lo contrario se obtendrá una evidencia fallida, escasa y en extremos se perderán los datos, por lo que al contaminarse y/o adulterarse la evidencia no será de utilidad a los magistrados durante un proceso judicial; por lo que se hace necesario tener en consideración ciertas reglas y procedimientos que se encuentran desarrollados en la Norma ISO/ IEC 27037, la cual tiene un alcance global y se ha elaborado especialmente para el análisis digital forense, dicha norma establece una serie de principios para el tratamiento técnico de la evidencia digital entre ellos se encuentran la identificación, recolección, adquisición y preservación de los datos; igualmente, ha desarrollado procesos transversales para mantener la originalidad de la evidencia digital además presenta una metodología muy bien reconocida de tal manera que permite garantizar su legalidad y autenticidad en los procesos judiciales (ISO/IEC 27037, 2021)

2.2.1.3 *Confiabilidad y Suficiencia de la Evidencia Digital*

Considerar la confiabilidad de la evidencia digital es entender que las informaciones que fueron recogidas y almacenadas de los equipos informáticos durante el desarrollo del procedimiento judicial estos necesariamente tienen que ser verificables por sí misma, así como que obligatoriamente se van a tener que volver a reproducir y; en cuanto a la suficiencia se debe considerar que a mayor obtención de informaciones será mayor el aporte y de gran ayuda al magistrado al momento de tomar una decisión y poder incriminar con suficientes elementos de convicción a ciberdelincuentes (Guerrero, 2002)

2.2.1.4 Reconocimiento e Identificación de la Evidencia Digital

El proceso de reconocimiento y registro de la Evidencia digital, considera inicialmente el acto de poder conocer e identificar el Hardware de los medios tecnológicos igualmente se tiene que hacer la descripción detallada de los sistemas operativos estructurados así como de las aplicaciones que han sido instaladas en dichos equipos en este actuar es vital trascendencia considerar el hecho de poder ubicar, registrar y recoger aquellas informaciones de mucha importancia para una adecuada conducción en las investigaciones (fotos, mensajes, videos, audios, imágenes, otros), este accionar representa uno de los momentos más trascendentales para la identificación del autor del ilícito penal en descripción. Es en este contexto que el perito informático debe hacer un trabajo muy técnico y profesional para ubicar, consignar y proteger los datos encontrados los cuales en todo momento deben de mantener su originalidad tal cual como fueron encontrados inicialmente, para ello los especialistas utilizan diversas técnicas entre ellas la conocida como copia de “dato a dato” y/o “bit a bit”, dicho procedimiento técnico va a certificar que se trasladen exactamente los mismos datos de su fuente primigenia. Durante los procesos judiciales para la confiabilidad de los sujetos procesales se va a concentrar en que los archivos o la duplicidad de los datos se van a realizar mediante la obtención de valores matemáticos de identificación conocidos técnicamente como HASH, los cuales representan valores numéricos producto de la suma de diversos dígitos obtenidos de los datos que se están copiando y registrando. (Orta, 2020)

2.2.1.5 Dispositivos de Almacenamiento Informático

Los dispositivos de almacenamiento sencillamente son los componentes de tipo electrónico que se usan para leer o poder hacer la grabación de datos en el soporte de almacenamiento que podría hacerse de manera temporal o permanente en este contexto la labor del perito informático es de vital importancia quien debe de preocuparse de que los equipos tecnológicos como celulares, tablets, CPC, otros no se manipulen innecesariamente ni contaminen entonces la evidencia digital según el tipo de registro y/o dinámica de envío de datos utiliza diversos elementos informáticos como la memoria de almacenamiento, memoria de tipo RAM y memoria tráfico de redes, el primero de ellos es la más utilizada actualmente esta corresponde a los discos duros, memorias, CD, DVD, otros, estos pueden almacenar una gran cantidad de información por lo que en ocasiones es muy complejo su peritaje, el segundo corresponde a la obtención de datos desde que el dispositivo fue encendido por última vez y solo se puede trabajar cuando esta encendido y finalmente el tercero corresponde a las informaciones que se pueden recolectar de las redes o el internet aquí encontramos los servicios de envío de contenidos y almacenamientos en la nube (Novak y Gonzales, 2018).

2.2.1.6 Dispositivos Portátiles

Estos corresponden a componentes que se pueden mover o transportar con mucha facilidad, entre estos dispositivos tenemos a las tablets y smartphones los cuales en la actualidad durante los procesos de investigación de delitos informáticos constituyen una fuente de vital importancia en la identificación de rastros digitales,

para examinar estos dispositivos androids se requiere de un acceso root que le va a permitir al perito informático analizar las informaciones más trascendentales (Rullo , 2015)

2.2.1.7 Dispositivos Periféricos

Los dispositivos periféricos conocidos también como hardware son aquellos elementos que se utilizan para interactuar entre el individuo que usa un servicio y el sistema de cómputo cuya finalidad primordial es atender alguna necesidad para el uso del equipo ya sea introduciendo, obteniendo o almacenando datos, estos medios permiten que exista una comunicación entre la computadora y el medio externo, entre estos tenemos al teclado, monitor, CPU, mouse, otros, con estos componentes se pueden enviar todo tipo de informaciones como textos, números, sonidos, imágenes, gráficos, cuadros, otros (Torres, 2018)

2.2.1.8 Peritaje informático

Está definido como peritaje informático a aquella actividad orientada a la obtención de una prueba digital que sirva a los magistrados en los procesos judiciales para poder tomar decisiones claras y decidir la culpabilidad o inocencia de una persona, esta labor técnica es efectuada por un especialista quien es un entendido con amplia preparación, cualidades y expertiz dentro de las habilidades de estos profesionales se tiene que saber cuál es la forma más adecuada de ingresar y/o acceder a los archivos de hibernación, tablas MFT, archivos de Windows, ventana de eventos, archivos de carpetas Prefetch, papelera de reciclaje, registro de fotos, entre otros. (Alvarez, 2018)

2.2.1.9 Objetividad del Peritaje

Para que un peritaje tena el grado de objetividad tiene necesariamente que cumplir con todos los procedimientos legales que se exigen para su levantamiento adecuado y quien se encargue de realizar este proceso tiene que ser personal debidamente capacitado y especializado en dicha actividad técnica que, permita asegurar en la evidencia digital la credibilidad, la autenticidad y la integridad de la misma, el mecanismo que se usa en nuestro país para la realización de peritajes informáticos está compuesto por etapas entre las cuales se encuentran la identificación, adquisición, aseguramiento, análisis y presentación del informe pericial (Proaño y Gavilanes, 2018)

2.2.1.10 Legalidad, idoneidad e inalterabilidad de la evidencia digital

Para que una evidencia digital sea considerada legal su proceso de recojo y levantamiento debe desarrollarse conforme a los protocolos forenses digitales debidamente reconocidos por la ley, las cuales durante el proceso judicial tendrán que ser revisadas y evaluadas por los magistrados, quien va a determinar su verdadera importancia; en cuanto a la idoneidad de la evidencia se tiene que tomar en cuenta que esta para la acción de la justicia tiene que ser verdaderamente autentica, real y debe mantener un nexo con el hecho ocurrido, además de dar mucha confianza para no dar lugar a suspicacias y finalmente en lo concerniente a la inalterabilidad la evidencia debe seguir ciertas medidas en cuanto a su resguardo y/o protección, la idoneidad y capacidad efectiva de quienes realizan el peritaje, los dispositivos de almacenamiento

tienen que ser óptimos junto a una adecuada cadena de custodia (Mesa, 2014)

2.2.1.11 Definición del delito informático

Se entiende como delito informático a todas aquellas formas de comportamiento criminal que se encuentran dirigidas a afectar los componentes tecnológicos de manejo masivo de archivos y datos, teniendo como principal finalidad apoderarse de estas informaciones y poder obtener de ellos un aprovechamiento ilegal (Villavicencio, 2014).

2.2.1.12 Sujetos del delito

En este tipo de delitos podemos encontrar al sujeto activo quien es la persona que materializa el hecho delictivo informático, para cuyo accionar criminal no necesariamente puede tener el perfil de un malhechor común, estos ciberdelincuentes poseen ciertos conocimientos en informática y manejo tecnológico, mientras que el sujeto pasivo corresponde a la persona afectada por el delito informático. (Gil Albarran, 2007).

2,2,1,13 Tipología

De acuerdo con Lara, Martínez & Viollier (2014), en los diversos estudios que ha efectuado en torno a los delitos de tipo informático ha realizado una clasificación delictiva conforme se detalla:

El acceso a un sistema no autorizado: Según esta clasificación el hecho corresponde a acceder a un componente tecnológico o una plataforma de red sin contar con la debida

autorización afectado su esfera de seguridad y haciéndolo de manera subrepticia e irregular aprovechando el delincuente sus conocimientos en informática.

El daño a los datos o sistemas informáticos: De acuerdo a esta clasificación el delincuente informático luego de haber accedido irregularmente afectando su esfera de protección de un medio tecnológico o campo de redes procede a realizar maliciosamente la destrucción parcial o total de los mismos ocasionando un grave daño o perjuicio.

El sabotaje a medios informáticos: En atención a esta clasificación se pude señalar que la misma se materializa cuando el ciberdelincuente ingresa subrepticiamente vulnerando los medios de seguridad a un componente tecnológico o plataforma de redes con el objetivo de dañarlo y consecuentemente evitar que este continue operando provocando graves daños.

La interceptación no autorizada: con esta clasificación el delincuente tecnológico va a tener como principal conducta la acción de utilizar medios o componentes técnicos con la única finalidad de captar las informaciones que se generen en estas buscando obtener de este algún tipo de beneficio ilegal.

El espionaje informático: esta modalidad tiene una singularidad en cuanto a su materialización ya que la misma va a consistir en el acto en el cual el delincuente informático necesariamente va a acceder irregularmente a algún tipo de información atentando a sus medidas de protección y estos datos

los va a trasladar a la esfera de otros individuos y por cuya revelación va a provocar un perjuicio o daño.

2.2.2 Legislación

Dentro de nuestro sistema jurídico tenemos a la "*Ley de Delitos Informáticos – Ley Nº 30096 y sus modificatorias con la Ley Nº 30171"*, revisado y analizado el contenido de la indicada norma permite inferenciar que esta ha sido aprobada por el Estado Peruano como parte de su política pública en la lucha frontal contra la criminalidad cibernética según el espíritu de la precitada norma busca principalmente consolidar una herramienta normativa que asegure una función preventiva para bienestar común de la sociedad y en el otro extremo la labor punitiva para los que incurran en estos ilícitos, a quienes se puede identificar como delincuentes muy hábiles que aprovechando sus conocimientos en informática y TIC mal intencionadamente manipulan los medios tecnológicos y otros intereses de tipo jurídico que se encuentran relacionados al presente ilícito penal, igualmente la ley describe las modalidades de delitos informáticos cada una de ellas con sus respectivas característica entre estas tenemos aquellos actos contra los componentes informáticos e informaciones.

2.2.3 Jurisprudencia

Existe en nuestro sistema legal un antecedente jurídico por parte del Tribunal Constitucional peruano que está relacionado a un recurso de agravio constitucional interpuesto contra una sentencia que fuera emitida por la 2da. Sala Penal para Procesos con Reos Libres dependiente de la Corte Superior de Justicia de la jurisdicción de Lima, en la cual su colegiado principal ha resuelto ser improcedente una demanda constitucional de habeas corpus los hechos versan en el extremo de haberse emitido una sentencia aplicando la

Ley Nº 30096 – Ley de Delitos Informáticos cuando esta no se encontraba vigente consecuentemente el caso fue revisado en Pleno del Tribunal Constitucional y en la parte de los fundamentos y análisis del caso el colegiado ha llegado a determinar que el citado dispositivo legal se encontraba vigente, ya que esta fue publicada oficialmente el 23 de octubre del 2013 y el condenado habrían materializado su conducta criminal sustrayendo sistemáticamente dinero de la Caja Municipal de Ahorros y de Crédito de Trujillo con sede en Lima hasta el mes de marzo del 2014, cuando la norma ya estaba en vigencia por lo que finalmente el colegiado ha resuelto declarar infundada la demanda interpuesta la cual ha sido registrada en el Pleno de Sentencia 1100/2020 (Exp. Nº 01189-2019-PHC/TC LIMA)

2.2.4 Tratados de Delitos Informáticos

El 23 de noviembre del 2001 en el contienen Europeo se juntaron diferentes naciones que preocupados por el gran desarrollo de la ciencia y la tecnología a nivel global y consecuentemente la aparición de modalidades por crímenes cibernéticos celebraron el “Convenio Budapest”, el cual surge ante la necesidad de buscar un medio de defensa social de carácter general con la finalidad de cuidar un bien jurídico muy importante como son las informaciones y la intimidad de las personas de cara a los actos de los delincuentes cibernéticos quienes aprovechando sus cocimientos en informática y las plataformas de internet vulneran los campos de protección e ingresan a los competentes tecnológicos afectando a los sistemas y las informaciones, igualmente los países en acuerdo han buscado construir un dispositivo legal que tenga un alcance a nivel mundial que busque reprimir jurídicamente a quienes cometan estos ilícitos penales en sus diferentes modalidades; asimismo, el tratado se presenta como un medio completamente necesario como un mecanismo adecuado para la esfera de seguridad y de protección de

las sistemas e informaciones de todas las personas y de esta manera poder luchar eficientemente contra la cibercriminalidad en el ciberespacio, agilizando las investigaciones con procedimientos idóneos en la ubicación y detención de los presuntos responsables de estos ilícitos con el objeto de ser sancionados penalmente por las autoridades competentes (Budapest, 2021).

2.2.5 Definición de Términos Básicos

- **Autenticidad**

  La autenticidad está referida a la acción de obrar de manera adecuada y clara, mientras que en el campo del derecho está relacionado estrechamente con realizar un determinado proceso de manera legítima y real (Flores, 2014).

- **Confiabilidad**

  La confiabilidad en el campo del derecho corresponde a una característica sumamente importante porque permite poder controlar la eficiencia y efectividad de los procesos, así como de los medios probatorios y/o evidencias que se desarrollan dentro de las actuaciones judiciales (Alcaíno, 2014)

- **Suficiencia**

  En el campo del derecho la suficiencia es una característica que se puede utilizar para evaluar alguna afirmación, se debe considerar que los magistrados al momento de determinar la responsabilidad penal del sujeto activo, los medios probatorios tienen que ser capaces y suficientes que le permitan poder despejar cualquier tipo de suspicacia y/o cuestionamiento (De le Court, 2019).

- **Dispositivos de almacenamiento informático**

  Los dispositivos de almacenamiento informático son los componentes que se encuentran en los equipos de cómputo y que le

permite almacenar y registrar las informaciones, según su clasificación estos pueden ser dispositivos de primer y segundo nivel (Cabral, 2018)

- **Dispositivos portátiles**

  Son equipos electrónicos que se han inventado con la finalidad de agilizar las actividades de los seres humanos, igualmente, tienen como beneficios poder ser trasladados de manera rápida y cómoda, dentro de estos aparatos tenemos a los celulares, laptops y las Tablet (Basantes, 2017).

- **Dispositivos periféricos**

  Se llaman dispositivos periféricos a aquellos componentes externos a un equipo de cómputo y que desempeñan una función entre la interface del usuario y la computadora, estos los podemos identificar en los teclados, mouse, USB, parlantes, etc. (Vásquez, 2015)

- **Objetividad**

  La objetividad en el campo del derecho lo podemos entender como la sensatez o cordura de quien hace una apreciación y no se deja llevar por subjetivismos o la influencia de terceros a una decisión manteniendo en todo momento el principio de imparcialidad (Saldaña, 2009).

- **Legalidad**

  La legalidad la entendemos como un principio rector que le dice a las personas como comportarse de acuerdo a las normas y reglas que impone el Estado, vale decir, que siempre debe de existir un equilibrio entre la actuación de las personas y la normatividad vigente (Calleros, 2014).

- **Idoneidad**

  La idoneidad esta contextualizada como la capacidad profesional que tienen las personas para ocupar responsabilidades de manera correcta y profesional dentro las instituciones (Vial, 2016)

- **Inalterabilidad**

  La inalterabilidad se entiende como el estado o situación de una determinada cosa la cual a través del tiempo debe mantenerse imborrable o inalterable permitiendo encontrarlo tal cual como era al inicio (Albarracín, 2019)

3. CONCLUSIONES

- El desmedido crecimiento y gran auge de muchos campos de la ciencia así como del área de la tecnología a nivel mundial han dado lugar que la sociedad en su conjunto tenga que reestructurar sus hábitos de convivencia y asumir nuevos retos en su vida diaria implementando y digitalizando sus recursos y necesidades, esto es debido principalmente que, ante la gran cantidad de datos e informaciones que circulan en los distintos medios digitales (redes) han provocado que las denuncias por delitos informáticos se incrementen exponencialmente.
- Los delitos informáticos también conocidos técnicamente como “ciberdelitos” actualmente representan un grave problema para la sociedad su accionar es cometido por delincuentes y/o personas inescrupulosas quienes aprovechando de sus múltiples conocimientos respecto a medios informáticos, áreas de las tecnología y a través de las plataformas de internet vienen lucrándose ilegalmente, atentando contra los sistemas informáticos, generando fraude y suplantando identidades, frente a esta dura ola criminal cibernética se asocia también la grave situación sanitaria a nivel global por la presencia del coronavirus 19 (Covid 19) en nuestro país, que ha obligado a las personas y a la sociedad a desarrollar sus actividades económicas, bancarias y financieras a través del uso de computadoras y del internet, esta actividad ha traído como consecuencia el incremento desmedido de denuncias por delitos informáticos según cifras y datos obtenidos de la Divindat PNP.
- La evidencia digital se entiende como toda información producida, transmitida y almacenada en dispositivos electrónicos y que pueda utilizarse en el futuro como medio de prueba, teniendo como principal característica que esta tiene que haberse registrado y generado en el mismo lugar de la intervención y que esta nos permita conocer la inalterabilidad de los dispositivos originales, para que esta evidencia tenga efectividad en los procesos judiciales es de vital interés reconocer el trabajo técnico

que efectúa el perito informático quien formulará el informe pericial de análisis digital forense, este profesional debe conocer necesariamente el acceso a la memoria de todos los sistemas que se van a analizar e investigar.

- En la actualidad existe una gran cantidad de denuncias por delitos informáticos lo que consecuentemente ha dado lugar que, los operadores de justicia busquen contrarrestar a estos ciberdelincuentes y para ello es absolutamente necesario que sus principales actores entre estos los fiscales y personal de la Divindat PNP, se actualicen en el uso y aplicación de herramientas modernas y de la TIC, que permitan fortalecer la lucha contra estos delitos que se encuentran tipificados en la Ley Nº 30096 – Ley de Delitos Informáticos y sus modificatorias con la Ley Nº 30171.

4. APORTES DE LA INVESTIGACIÓN

El aporte académico del presente trabajo de investigación se expresa en la manera de valorar e identificar la trascendencia de la “evidencia digital” durante el desarrollo de los procesos penales por la realización de los delitos de tipo informático y para ello la Divindat PNP, tiene una participación directa en cuanto a su prosecución y efectividad ante la justicia, igualmente se tiene que considerar que ante el incremento desmedido de denuncias por este tipo de delitos ocasionado por personas inescrupulosas que debido a sus conocimientos técnicos se aprovechan de esta situación y proceden a lucrarse ilegítimamente atentando contra los sistemas informáticos, generando fraudes y suplantando identidades entonces surge la necesidad de que la sociedad tenga un rol más consciente y proactivo procediendo a proteger todas sus informaciones de carácter personal, bancario o financiero.

Igualmente, ante la grave situación sanitaria a nivel mundial por la presencia del coronavirus 19 (Covid 19), ha obligado a la sociedad en su conjunto a desarrollar sus transacciones económicas, bancarias y financieras a través del uso de computadoras, celulares, Tablet, otros y del internet, situación que viene siendo aprovechada por los “ciberdelincuentes”, quienes han encontrado un mercado criminal muy amplio para sus insanas intenciones, consecuentemente ha dado lugar al incremento excesivo de casos por delitos informáticos tipificados en la Ley Nº 30096 – Ley de Delitos Informáticos y sus modificatorias con la Ley Nº 30171, evidenciándose una amplia falta de conocimiento por parte de las víctimas quienes no toman ningún tipo de protección y/o medidas de seguridad para sus informaciones y datos personales.

5. RECOMENDACIONES

- Como primera recomendación, se señala que el personal especializado responsable de realizar las actividades de peritaje en análisis digital forense sea permanentemente capacitados y preparados en esta labor de tal forma que la evidencia de naturaleza digital recogida con medios tecnológicos en los lugares donde se materializa el crimen asegure su autenticidad, credibilidad e integridad.

- Asimismo, se recomienda a los funcionarios que integran el Ministerio Público y personal policial de la Divindat PNP, que realizan diligencias y actos de investigación en torno a los Delitos Informáticos descritos en la Ley Nº 30096 – Ley de Delitos Informáticos y sus modificatorias con la Ley Nº 30171, sean capacitados y actualizados para enfrentar a los criminales con nuevas herramientas informáticas y en TIC.

- Igualmente, recomendar que los funcionarios del Ministerio Público y personal de la Policía Nacional del Perú desarrollen estrategias en campañas masivas de información a las personas y la sociedad informando la existencia de diversas modalidades en Delitos Informáticos, la actuación de los ciberdelincuentes, así como para el aseguramiento y cuidado permanente de los datos que se encuentran en la esfera intima de las personas y a través de medios informáticos.

- Finalmente recomendar que una comisión multidisciplinaria de alto nivel y que desarrollen actividades en la lucha contra el crimen cibernético se encarguen de la revisión, actualización y mejora continua de la Ley Nº 30096 – Ley de Delitos Informáticos considerando que actualmente y con la presencia del coronavirus 19

(Covid 19) se han incrementado otras modalidades y ciberdelitos que no se encuentran en la legislación actual.

6. REFERENCIAS BIBLIOGRÁFICAS

Referencias

ISO / IEC 27037. (2021). *Ciberseguridad.* Obtenido de https://ciberseguridad.com/normativa/espana/iso-iec-27037-evidencia-digital/

Albarracín, A. (2019). *La inalterabilidad del derecho de propiedad del titular registral en la trasferencia de la propiedad inmueble y el tráfico ilegal de bienes inmuebles.* Tesis, Universidad Nacional del Antiplano. Obtenido de http://repositorio.unap.edu.pe/bitstream/handle/UNAP/13890/Angela_Magaly_Albarracin_Machicado.pdf?sequence=1&isAllowed=y

Alcaíno , E. (2014). La confiabilidad como estándar para evaluar la calidad de los reconocimientos de imputados. *Política criminal, 9*(18), 564-613. doi:https://dx.doi.org/10.4067/S0718-33992014000200009

Alvarez Porras, J. A., Lopez Guzman, U. M., & Gutierrez Portela , F. (2018). Presente y futro de la evidencia infirmatica:analisis frente a las competencias del auditor. *Revista sinergia, 4*, 108-129. Obtenido de http://sinergia.colmayor.edu.co/ojs/index.php/Revistasinergia/article/view/60/38

Basantes , A., Naranjo, M., Gallegos, M., & Benítez, N. (2017). Los dispositivos móviles en el proceso de aprendizaje de la facultad de educación ciencia y tecnología de la Universidad Técnica del Norte de Ecuador. *10*(2), 79-87. Obtenido de https://www.redalyc.org/articulo.oa?id=373550473009

Bolaños Burgos, F., & Gómez Giacoman, C. (2015). Estudio cualitativo de la relación de las leyes y la pericia informática en el Ecuador. *Revista electrónica de Computación, Informática, Biomédica y Electrónica*. Obtenido de https://www.redalyc.org/pdf/5122/512251503001.pdf

Cabral, V. (2018). Consdieraciones para el almacenamiento de archivos digitales en la nuve informática en bibliotecas universitarias. *Investigación bibliotecológica, 32*(74), 55-75. doi:https://doi.org/10.22201/iibi.24488321xe.2018.74.57909

Calleros, M. (2014). Cultura de la legalidad: porqué y para qué en la educación media superior. *IE Revista de Investigación Educativa de la REDIECH, 5*(8), 29-35. Obtenido de https://www.redalyc.org/articulo.oa?id=521651962005

Convenio sobre la ciberdelincuencia (2001), obtenido de https://static.legis.pe/wp-content/uploads/2019/09/Convenio-sobre-la-Ciberdelincuencia-Legis.pe_.pdf

De le Court, A. (2019). Principio de suficiencia y prestaciones mínimas de Seguridad Social: una revisión desde el derecho al mínimode existencia alemán. *Revista de derecho (Valdivia), XXXII*(2), 165-184. Obtenido de http://revistas.uach.cl/index.php/revider/article/view/5951/7063

Espinoza Coila, M. (2017). *Derecho Penal Informàtico:Deslegitimaciòn del poder punitivo en la sociedad de control.* [Tesis de titulo,Universidad Nacional del Antiplano]. Obtenido dehttp://repositorio.unap.edu.pe/bitstream/handle/UNAP/6309/Espinoza_Coila_Michael.pdf?sequence=1&isAllowed=y

Flores, J. G. (2014). Por un derecho electoral al servicio de la democracia, México, UNAM. *Estudios Políticos, 9*(31), 191-194. Obtenido de https://www.redalyc.org/articulo.oa?id=426439552010

Flores, J. G. (2014). Por un derecho electoral al servicio de la democracia, México, UNAM. *Estudios Políticos, 9*(31), 191-194. Obtenido de https://www.redalyc.org/articulo.oa?id=426439552010

Gil Albarran, G. (2007). Derecho Informàtico. Megabyte. Obtenido de http://sbiblio.uandina.edu.pe/cgi-bin/koha/opac-detail.pl?biblionumber=1359

Gómez, D. (2020). Implicaciones jurídicas de la evidencia digital en el proceso judicial colombiano. *Redalyc, 15*(30), 220-240. Obtenido de https://www.redalyc.org/articulo.oa?id=585764837011

Guerrero Mateus , M. F. (2002). La Ciberdelincuencia: la ley patriotica y los efectos globales en las regulaciones nacionales y en particular en el caso colombiano. *tesis de grado*. Repositorio Universidad de los Andes. Obtenido de https://repositorio.uniandes.edu.co/handle/1992/47382?show=full

Ley de Delitos Infornáticos Nº 30096 y sus moficicatorias con la Ley Nº 30171. Obtenido de https://spijweb.minjus.gob.pe/

Mesa Elneser, A. M. (2014). La evidencia digital eximente de violacion a la proteccion del dato personal a partir de la utorregulacion. *Revista Academia y Derecho, 10*(6), 1-38. Obtenido de http://190.143.117.169/ojs/index.php/derecho/article/view/3

Novak, M., Grier, J., & Gonzales, D. (2018). Department of Justice. "New Approaches to Digital Evidence Acquisition and Analysis" (EE.UU.). *National Institute of Justice Journal*. Obtenido de https://nij.ojp.gov/topics/articles/new-approaches-digital-evidence-acquisition-and-analysis

Orta Martinez, R. (2020). Informatica forense como medio de pruebas. *DragonJar*. Obtenido de https://www.dragonjar.org/informatica-forense-como-medio-de-pruebas.xhtml#:~:text=Reconocimiento%3A%20El%20reconocimiento%20de%20la%20Evidencia%20Digital%20incluye,sistemas%20operativos%20y%20aplicaciones%20instaladas%20en%20los%20mismos.

Osco Escobedo, M. (2019). *La admisibilidad y el valor probatorio de la evidencia digital en el Sistema Jurídico Peruano 2018.* Tesis de maestria,Universidad Cèsar Vallejo. Obtenido de https://repositorioslatinoamericanos.uchile.cl/handle/2250/2997329

Proaño Escalante , R. A., & Gavilanes Molina, A. F. (2018). Strategy for responding to computer incidents of insecurity set Ecuatorian Law. *Enfoque UTE*. Obtenido de http://scielo.senescyt.gob.ec/scielo.php?script=sci_arttext&pid=S1390-65422018000100090

Rico Carrillo, M. (2003). La función procesal probatoria del documento electronico. *Derecho de internet & Telecomunicaciones*. Obtenido de http://biblioteca.ugc.edu.co/cgi-bin/koha/opac-detail.pl?biblionumber=247221

Rodriguez Cevallos, C. D. (2018). Metodologia de Clasificacion de delitos informaticos en redes sociales tipificacion segun las leyes del ecuador determinacion de vacios legales y el proceso para propuesta de ley. *Tesis de Maestria*. Repositorio Universidad Internacional SEK. Obtenido de https://repositorio.uisek.edu.ec/bitstream/123456789/3220/1/CAROL%20DE%20LAS%20MERCEDES%20RODR%c3%8dGUEZ.pdf

Rullo Albo , J. (2015). Analisis Forense en dispositivos Android. *Reunir unir*. Obtenido de https://reunir.unir.net/bitstream/handle/123456789/2835/rullo%20albo.pdf?sequence=1&isAllowed=y

Saldaña, J. (2009). Reseña de Objetividad jurídica e interpretación del derecho. *Boletín Mexicano de Derecho Comparado, XLII*(126), 1577-1586. Obtenido de https://www.redalyc.org/articulo.oa?id=42715770013

Torres, M. E. (2018). Informatica forense: el camino de la Evidencia Digital. *Ciencia y Tecnica Administrativa*. Obtenido de http://www.cyta.com.ar/biblioteca/bddoc/bdlibros/informatica_forence.htm

Tovar, C. F., & Amariles Bedoya, K. (2015). Mitigacion de riesgo de delitos informaticos en el contexto empresarial. *Tesis de grado*. Repositorio UNiversidad Tecnologica de Pereira. Obtenido de

http://repositorio.utp.edu.co/dspace/bitstream/handle/11059/5164/0058T736.pdf?sequence=1&isAllowed=y

Tribunal Constitucional, pleno sentencia 1100/2020 del T.C Obtenido del https://tc.gob.pe/jurisprudencia/2020/01189-2019-HC.pdf

Vázquez, S. E. (2015). Tecnologías de almacenamiento de información en el ambiente digital. *Revista e-Ciencias de la Información, 5*(2), 1-18. Obtenido de https://www.redalyc.org/articulo.oa?id=476847248008

Vial, M. (2016). Algunas reflexiones sobre la idoneidad de las normas regulatorias de los regímenes matrimoniales del Derecho Internacional Privado chileno. *Ius et Praxis, 22*(1), 165-185. Obtenido de https://www.redalyc.org/articulo.oa?id=19746570006

Villavicencio Terreros, F. (2014). Delitos Informàticos. *Ius Et Veritas, 24*(49), 284-304. Obtenido de https://revistas.pucp.edu.pe/index.php/iusetveritas/article/view/13630