FACULTAD DE DERECHO

ESCUELA PROFESIONAL DE DERECHO

"LOS FACTORES PRINCIPALES QUE IMPIDEN LA APLICACIÓN DE LA LEY N°30171- LIMA NORTE EN EL AÑO 2016"

TESIS PARA OBTENER EL TITULO PROFESIONAL DE ABOGADO

AUTOR:

COTRINA YUCRA, SANTIAGO RICARDO JUAN

ASESORES:

ASESOR TEMÁTICO: MG. ACETO, LUCA

ASESOR METODOLOGICO: MG. CHÁVEZ RODRIGUEZ, GILBERTO

LÍNEA DE INVESTIGACIÓN:

DERECHO PENAL

LIMA – PERÚ

2018

UCV UNIVERSIDAD CÉSAR VALLEJO	ACTA DE APROBACIÓN DE LA TESIS	Código : F06-PP-PR-02.02 Versión : 09 Fecha : 23-03-2018 Página : 1 de 1

El Jurado encargado de evaluar la tesis presentada por don (ña) SANTIAGO RICARDO JUAN COLINA YUCRA
cuyo título es: "LOS FACTORES PRINCIPALES QUE IMPIDEN LA APLICACION DE LA LEY Nº 30171 - LIMA NORTE EN EL AÑO 2017"

Reunido en la fecha, escuchó la sustentación y la resolución de preguntas por el estudiante, otorgándole el calificativo de: 16 (número) DIECISEIS (letras).

Lugar y fecha: LIMA 09/12/2018

PRESIDENTE
VILLEGAS CABRERA, ERICK

SECRETARIO
TRUJILLO PAJUELO, MICHAEL

VOCAL
LUCA ACETO.

Elaboró	Dirección de Investigación	Revisó	Responsable de SGC	Aprobó	Vicerrectorado de Investigación

Dedicatoria

Dedico este trabajo de investigación a mis abuelos y madre por su apoyo incondicional, por cada día transcurrido brindarme el aliento y la fortaleza que necesitaba, a mi familia, amigos y compañeros de la facultad que me inspiraron a crecer y querer ser mejor cada día a nivel profesional y personal, así como a cada palabra de aliento que recibí de todos a quien amo.

Agradecimiento

Agradezco el esfuerzo constante de mis asesores a lo largo de todo este tiempo que ha transcurrido, el apoyo incondicional de mi mejor amiga para poder enfrentar este largo camino y poder lograr convertirme en un gran profesional, a mi familia y amigos que de muchas maneras hicieron lo posible para que esté momento llegase, agradezco todo el esfuerzo y los sacrificios de todos a quien amo, gracias.

Declaración Jurada de Autenticidad

Yo, Santiago Ricardo Juan Cotrina Yucra con DNI N° 76404576, a efectos de cumplir con las disposiciones vigentes consideradas en el Reglamento de Grados y Títulos de la Universidad César Vallejo, declaro bajo juramento que:

1. La presente tesis es de mi autoría.

2. He respetado las normas internacionales de cita y referencias para las fuentes consultadas. Por lo tanto, la presente tesis no ha sido plagiada, ni total ni parcialmente.

3. La presente tesis no ha sido auto-plagiada, es decir, no ha sido publicada ni presentada con anterioridad para obtener grado o título profesional alguno.

4. Los datos presentados en los resultados son reales, no han sido falseados, duplicados, ni copiados. Por tanto, los resultados que se presentan en esta tesis se constituirán como aportes a la realidad investigada.

En tal sentido, de identificarse fraude, auto-plagio, piratería o falsificación, asumo la responsabilidad y las consecuencias que de mi accionar deviniera, sometiéndome a las disposiciones contenidas en las normas académicas de la Universidad César Vallejo.

Lima, Julio de 2018.

Santiago Ricardo Juan Cotrina Yucra

DNI N.° 76404576

Presentación

Señores del jurado:

Hago ante ustedes presente la tesis titulada: “Los factores principales que impiden la aplicación de la Ley N°30171- Lima Norte en el año 2016”, teniendo como objetivo el de obtener el título profesional de abogado, a través de la cual se logrará contribuir a determinar cuáles son los factores que impiden la correcta aplicación de la Ley N°30171.

De esta manera siguiendo con el Reglamento de Grados y Títulos de la Universidad Cesar Vallejo, la presente investigación se organiza de la siguiente manera: en la parte introductoria se consignan la aproximación temática, trabajos previos o antecedentes, teorías relacionadas al tema o marco teórico y la formulación del problema; estando aquí, el problema de investigación, los objetivos tanto general como los específicos y los supuestos jurídicos; compuesto por el supuesto general y los específicos. En la segunda parte se aborda el marco metodológico en el que se sustenta el trabajo de investigación desarrollada que en esta investigación vendría a ser de enfoque cualitativo, de tipo de estudio orientado a la comprensión con un diseño de estudio fenomenológico, determinado la población y muestra, caracterización a los sujetos de estudio, manifestando las técnicas e instrumentos de recolección de datos, indicando los métodos de análisis de datos y resaltando los aspectos éticos. Continuando con detallar los resultados que permitirán conducir a la conclusión y recomendación, todo ello con el respaldo de las referencias y evidencias contenidas en los anexos del presente trabajo de investigación.

El autor.

INDICE

INDICE DE TABLAS

RESUMEN

La presente tesis tiene como objetivo general analizar cuáles son los factores principales que impiden la aplicación de la Ley N° 30171 en el sector Lima Norte en el año 2016, por ello se ha tomado como base para el desarrollo de la presente tesis, el sector de Lima Norte, tomándose en cuenta la experiencia de especialistas en el tema y de la oficina de División de Investigación de Delitos de Alta Tecnología (DIVINDAT). Asimismo, la presente tesis es de enfoque cualitativo, con tipo de estudio: básica pura, con un diseño de estudio fenomenológico y un nivel o alcance de investigación descriptiva. Además, cabe mencionar que las técnicas de recolección de datos fueron: la entrevista, realizada a 10 abogados expertos en derecho penal y especialistas de la División de Investigación de Delitos de Alta Tecnología, que de aquí en adelante se menciona por sus siglas DIVINDAT, y el análisis documental referente a los factores que impiden la aplicación de la Ley N° 30171, y los instrumentos de recolección de datos fueron: la guía de entrevista, la ficha de análisis documental.

La conclusión a la que se llegó en la presente tesis fue que la ley de delitos informáticos no se ha logrado aplicar correctamente, por falta de indumentaria, capacitaciones a los entes encargados, cooperación operativa por parte de los órganos estatales y falta de adhesión al Convenio de Budapest.

Las palabras clave: Ciberdelincuencia, delito informático,

ABSTRACT

The present thesis has as general objective. Analize which are the principals factors that obstruct the application of the law Nº30171 in Lima Norte sector in the year, 2016 for this, it has been taken, how population for development, of the present thesis, the sector of Lima-Norte, taken as a sample to the subject specialists and the crime investigation (DIVINDAT). Likewise, the present thesis is of qualitative aproach with type of study: pure basic, with a design of phenomenological study and a level or scope of descriptive research. Also, we must to mention that the technics of datas collection were: the interview realize to 10 experts lawyers in criminal law and specialists of the crime investigation division office of high investigation that from now on is mentioned by it's acronyms DIVINDAT and the analysis refering to the factors that impede the application of the law Nº30171, and the instruments of data collection were; the interview guide, the documentary analysis.

The conclusion reached in the present thesis was that the law of cumputer crimes has not been succesfully applied due to lack of instruments, training, operational cooperation by the state organs and lack of adherence to the Budapest Convention.

Keywords: Cybercrime, computer crime.

I. INTRODUCCIÓN

En tiempos actuales, de existir algún detonante que hubiese originado un cambio en el mundo este sería el "Internet", un magnífico descubrimiento que nace a mediados del siglo XX y es la obra representante de esta época contemporánea. El internet facilitó de forma notoria y significante los vínculos de índole social, como también de forma más amplia todo vínculo u trasferencia de datas. No obstante, incluso de forma más considerable, alteró irreversiblemente nuestro *modus vivendi* (modo de vida) y la forma cómo nos aproximamos a los demás.

En la actualidad no se concibe algún individuo ajeno a esta poderosa corriente, causada por la informática en las actividades diarias de personas y agrupaciones, sobretodo se denota en el avance de un país. Es así que las actividades que han tenido una mayor alteración radical y sucesiva son: los intercambios de carácter comercial, las comunicaciones, los procedimientos industriales, los estudios, la defensa, etcétera.

Todos estos ámbitos necesitan cada día más de un idóneo progreso de la tecnología, junto al desarrollo de la informática y su repercusión en todas las instancias de la vida social, necesitando de una correcta regulación y aplicación normativa, es por ello que ha surgido una serie de conductas ilícitas denominadas de manera genérica "Delitos Informáticos".

Se debe tener como misión el investigar al ilícito desde cualquier aspecto, es una tarea dificultosa, de ello no existe cuestionamiento alguno, sin embargo para poder enfrentar esta rama de ilícitos en el ámbito nacional se adjudica esta labor al Ministerio Público, debido a lo decretado por la constitución y por corroboración legal. Siendo este mismo sentido una disyuntiva descrita en general; dentro de estos últimos tiempos los delitos informáticos han sufrido un incremento de forma exponencial en consideración a la exteriorización del fenómeno que es la globalización, esta no solo carece de beneficios, sino que además ayudo a la multidiversificación y concretización de este tipo de ilícitos.

Sin embargo, es obligatorio tener en cuenta que si es cierto, que la denominada red da una infinita gama de herramientas a las personas para desempeñar sus trabajos diarios, de similar forma es verdadero que dará igual cantidad de oportunidades para transgredir la ley.

1.1. APROXIMACIÓN TEMÁTICA

Hoy en día la tecnología y comunicaciones avanzan a pasos abismales, a comparación de lo que se suscitaba hace unos 30 ó 40 años, cuando se entregaba al mundo un nuevo descubrimiento tecnológico cada cierto periodo de tiempo, hoy en día por ejemplo podemos observar que salen novedades y al otro día, algo mejor, con mejoras adicionales para facilitar la vida del usuario o consumidor, en pocas palabras, el avance tecnológico es una realidad, una corriente a la cual nadie puede ir en contra de esta, lo único que se puede hacer es adaptarse y acoplarse a ella , porque de no hacerlo se entraría en un callejón oscuro de la sociedad, denominada la "ciberdelincuencia" o lo que más comúnmente se conoce, como "delitos informáticos", el cual es un tema que se tocara dentro del presente trabajo de investigación.

En el Perú, encontramos en el centro de Lima, existen centros de comercialización de bases de datos por S/.200. 00 a más, dependiendo la importancia; la clo^{na}ción de tarjetas es muy común, estados de cuenta elevados sin haber hecho uso de la tarjeta de crédito, transferencias fantasmas, pornografía infantil vendida en pleno centro lima; la DIVINDAT encargada de combatir los delitos informáticos a la fecha cuenta con 470 casos sin resolver y quizás más, pero las cifras en total no son reveladas, por miedo a que los empresarios teman invertir en el Perú, entonces uno se pregunta ¿qué sucede con nuestra legislación?

¿Porque hasta ahora esos delitos no han sido castigados?, si ya existen legislaciones que nos amparan ante esos ilícitos, tenemos al Código Penal, la Ley Nº 30096 y su modificatoria la ley Nº 30171, Ley de delitos informáticos, pero según especialistas existen varios problemas para que no se puedan castigar a los culpables de estos delitos, entre ellos están: La falta de especialización a los encargados de sancionar estos ilícitos, falta de la tecnología necesaria para encontrar a los culpables y la ayuda internacional, para conseguir información de manera rápida, y es ahí donde entra a tallar el presente trabajo de investigación será cierto que la falta de especialización, la falta de adhesión a convenios internacionales es lo que está dificultando la aplicación de estas sanciones a los responsables de delitos informáticos.

1.1.1 Antecedentes Internacionales

Ceresole y Oyarzábal (2014) En su trabajo de Investigación titulada "*Los delitos informáticos*" que tuvo como objetivo principal, hallar la forma como el delito informático se confronta en la jurisdicción de Rafaela- Provincia de Santa Fe, para ello en su investigación empleo una clase de estudio interpretativo, llegando a la conclusión de que:

> [...] El principal tema dado, se entiende bajo dos conceptos: Que dichos instrumentos judiciales que tienen como finalidad un carácter probatorio, para indagar en el denominado "cyberdelito", es como tal la pericia especifica acerca de los medios probatorios del delito, además que en la ya mencionada jurisdicción legal y de manera concreta ubicado en este distrito judicial, se pueden hallar carencias e insuficiencias notables de lo que son los recursos humanos y técnicos para poder lograrlo (p.465)

Con respecto al presente antecedente realizado por Ceresole y Oyarzábal, en su trabajo de investigación *"Los delitos informáticos"* se debe hacer hincapié que con respecto al primer punto, los pilares fundamentales para la investigación del cyberdelito es la perecía específica, sobre los instrumentos del delito y como punto dos, la jurisdicción legal y de manera más concreta en este distrito judicial existen carencias e insuficiencias notables de recursos técnicos y humanos.

Es decir, de manera más centrada o abocada con el primer punto que como bien lo explica el autor es un factor principal para la investigación del delito que. es en este caso el cyberdelito es la pericia específica y esto se centra o bordea a lo que comúnmente se le conoce como "trabajo de campo" o "inteligencia" el cual es un instrumento muy útil y eficaz con lo que respecta a la lucha contra delitos en todas sus categorías, ahora bien con el segundo punto al cual hace alusión, debo hacer un especial hincapié, debido a que cuando no existe o se carece de recursos humanos y técnicos, todo lo demás se ve severamente interrumpido y obstaculizado, ubicándonos en un plano nacional, actualmente esto es una realidad evidente, comenzando que la DIVINDAT es el único ente encargado, que ve lo que son los delitos cibernéticos, además de ello que el Ministerio Público no tiene o posee una fiscalía especializada en estos temas, adicionalmente que en el Perú no cuenta con las herramientas técnicas para que las autoridades responsables puedan hacer frente a cualquier ataque cibernético en contra de la ciudadanía o de la normativa que en este caso es la leyN°30171, si sumamos todos estos factores ,que el mismo autor menciona a lo largo de esta explicación ,podemos denotar que se hallaría claramente un estado o país vulnerable a cualquier tipo de

ataques virtuales en cualquiera de sus modalidades o formas en que estos puedan presentarse.

Montaño (2008) de la Universidad Nacional Autónoma de México, realizo una tesis titulada "*La problemática jurídica en la regulación de los delitos informáticos*" teniendo como tipo de investigación descriptiva no experimental, tuvo como objetivo principal, estudiar los delitos informáticos analizados a través de un método histórico y documental de los antecedentes de la Informática, obteniendo como resultado que:

> [...] El legislador es un personaje que debe contar con toda la educación que le pueda aportar el Derecho Informático, y conjuntamente con esos conocimientos y la realidad social que pretende regular, debe formular una adecuada legislación entorno a su problemática ,dentro de todas las ramas de Derecho, la Policía Cibernética debe contar con elementos altamente capacitados bajo los principios de la Policía Científica, asistiéndose tanto del Derecho Informático como de las diversas Ciencias auxiliares, disciplinas y artes que le ayuden para la localización y detención del delincuente informático y por último es necesario que México pertenezca a organismos internacionales para llevar a cabo el combate de todo tipo de delincuencia que se da a nivel globalizado como la organizada, la financiera, el terrorismo, así como la informática.(P.154)

Rincon (2015) en su trabajo de investigación para su grado de doctorado denominada *"El delito en la cibersociedad y la justicia penal internacional"* dentro de esta mantuvo como objetivo principal que es propulsar un cimiento para la creación teórica desde la perspectiva dogmática penal internacional ,que conceda el hecho de debatir sobre la necesidad de incluir la investigación y juzgamiento de los ilícitos relacionados la informática o también denominados "delitos informáticos", de las telecomunicaciones y electrónicos dentro de la jurisdicción del estatuto de Roma , llegando a la conclusión en su estudio que :

> [...] El término "Globalización" como suceso o fenómeno ha producido dentro del globo una serie de avances de carácter significativo dentro del desarrollo , económico, político y social de los estados .La representación central material del mundo globalizado se ha producido por medio de los medios de comunicación, que a finales del siglo XX han sido revolucionados, gracias a nuevos instrumentos como tal es la denominada "INTERNET", en donde por medio de una red mundial o maestra ha sido una realidad compartir información y datos entre las personas, en cualquier sentido lugar, categoría,

una rapidez antes ni imaginable (p.147)

Por este mismo hecho se ha convertido en una acción de carácter imperativo que las naciones que se constituyan como miembros para la investigación, juzgamiento y castigo de los denominados "ciberdelitos", y como estrategia técnica internacional , acuerden la tipificación de los ilícitos como los ya mencionados delitos informáticos (ciberdelitos) , globales o universales revistiéndolos de las caracterizas técnicas que permitan su identificación , cuando su comisión ha surgido dentro del ciberespacio y de esta forma que no sobrepase las barreras del territorio.

Díaz (2014) en su investigación titulada *"Delitos Informáticos como combatirlos"*, tuvo como objetivo determinar cómo combatir los delitos informáticos, llego a la conclusión:

> Para poder combatir los delitos informáticos se debe: fortalecer la legislación nacional, establecer alianzas a nivel internacional, especializar a los cuerpos policiales y las autoridades judiciales sobre estos delitos, informar a los ciudadanos y recibir cooperación de los sectores privados y público (p.45)

1.1.2 Antecedentes Nacionales

Puelles (2014) en su trabajo de investigación titulada "*Luces y sombras en la lucha contra la delincuencia informática en el Perú*" esta mantuvo como objetivo central realizar un estudio y análisis de la respuesta que paulatinamente ha ido implementado el Legislador frente a los llamados "delitos informáticos" finalizando llego a la conclusión que:

> [..] Si bien es cierto nuestro Legislador se preocupó por penalizar este tipo de delitos o conductas ilícitas y algunas entidades como la Policía Nacional (PNP) realizaron intentos para poder luchar contra el cibercriminal por medio de la especialización de sus divisiones y efectivos, si se puede llegar a un concepto seria que muchas instituciones como el Ministerio Público y el Poder Judicial, han quedado rezagadas por lo que de igual forma deberían abrir las puertas a la modernización de sus equipos y especializar a sus operadores jurídicos pues las técnicas que se requieren para la investigación y persecución de esta actividad delictiva no es igual a la de los delitos que comúnmente se conocen. (p.157)

Ahora bien, con relación a lo que dijo el autor dentro de su trabajo titulado "*Luces y sombras en la lucha contra la delincuencia informática en el Perú",* es una cita obligatoria resaltar la total concordancia con lo expuesto por el autor esto debido o causado a los puntos que a continuación se pasara a exponer:

El autor dentro de su trabajo toca como primer punto de conclusión en mencionar que el legislador no tomó una preocupación mayor o una que lo amerite, al instante de penalizar como tal a los delitos o conductas ilícitas en temas relacionados a la ciberdelincuencia, que van en contra de los preceptos preestablecidos dentro de la sociedad y algunas instituciones como la Policía Nacional del Perú (PNP) realizan constantes intentos para luchar contra el ilícito llamado "cibercriminalidad",a través de la capacitación de varios cuerpos o efectivos. Ahora bien es imperativo centrarse en el segundo punto, que menciona el autor cuando dice "*el Ministerio Público y el Poder Judicial han quedado rezagadas, por lo que de igual forma deberían abrir las puertas a la modernización de sus equipos y especializar a sus operadores jurídicos",* aquí hay que hacer un énfasis, ya que centrándonos en la realidad que hoy en día, podemos ver la escases de los recursos técnicos y humanos para la lucha contra la delincuencia en todas sus modalidades y aún más contra una clase de ilícitos (delitos informáticos), que requieren de manera obligatoria un mayor hincapié en la modernización por parte de las instituciones que conforman el proceso administrador de justicia.

Por otro lado Fernández (2015) en su trabajo de investigación titulada "*Delitos Informáticos*", esta mantuvo como objetivo encontrar y definir en primer lugar las diferentes modalidades de cómo se presentas y se pueden encontrar en la realidad los ya mencionados Delitos informáticos viendo de la misma manera como es que la normativa actual actúa o regula estos casos, finalizando dicha investigación llegando a la conclusión que:

> [..] Las nuevas realidades que nos plantea la tecnología y la informática, se han ido desenvolviendo en estos tiempos modernos y fueron gracias al tan acelerado y veloz

> desarrollo, como de su incidencia directa en varios ámbitos dentro de nuestra sociedad; que han logrado alcanzar el estatus o denominación de "Bienes jurídicos" protegidos a su vez por el ordenamiento jurídico o las normas. Y esto al mismo tiempo nos hace pensar que estamos dentro de un procedimiento llamado "globalización", que se ha logrado conseguir esfuerzos para la creación e implantación de un sistema garantista, que cuente con la capacidad de poder asegurar y velar por los derechos de información y la tecnología, afirmar la promesa de la comunidad internacional con el fin de que regulen sus ordenamientos jurídicos para poder llegar a una uniformidad, siguiendo las pautas e indicaciones señaladas por las diferentes organizaciones mundiales y de esta manera los usuarios de la información y la tecnología sean protegidos de manera óptima dentro del mundo del ciberespacio (p.107)

Con relación a lo expuesto por Fernández, en su trabajo de investigación denominada *"Delitos Informáticos",* se debe mencionar que el autor en sus conclusiones es completamente atinado en cuanto a los puntos que se pasara a explicar*:*
El autor menciona como primer punto: que las nuevas tecnologías y la informática son un bien, debido a su acelerado desarrollo y su influencia directa en varios aspectos de nuestra vida.

Hoy en día se les ha otorgado el estatus de "bien jurídico protegido", por las normativas de la sociedad, ahora bien con lo que menciona el autor al momento de señalar, porque es protegido por parte de la normativa que casi en su totalidad es el derecho penal y esto es debido a la gran influencia que la tecnología e informática han tenido dentro de todas nuestras actividades cotidianas y esto más que una suposición, es un claro retrato de la realidad que hoy nos alberga a todos o al menos a la gran mayoría sin excepción.

Además nos habla, de que gracias a este avance tecnológico tenemos la "globalización", que ha sido un avance para logar la creación e implementación de un sistema garantista, donde la comunidad internacional tiene como objetivo asegurar y velar por los derechos de la información y la tecnología, a través de las diferentes organizaciones mundiales y sus diferentes normativas.

Así también Iglesias (2010) en su investigación titulada "*Análisis al convenio de Budapest*", tuvo como objetivo determinar si el convenio de Budapest era seguro o si causaba efectividad a los países firmantes, por tanto llegó a la conclusión que: "El convenio de Budapest obliga a recolectar y guardar información sobre comunicaciones, así como también a acceso a otros países firmantes que la soliciten". (p.32)

Para tratar de entender un poco más esto hay que remontarnos a lo que es un "bien jurídico protegido", como tal es un bien resguardado por las normas establecidas dentro de nuestro ordenamiento, sin embargo esta facultad no se le otorga a cualquier objeto (ejemplo, las piedras ,granos de arena, etc.) sino a las que cumplan una función de *Utilidad* para las actividades humanas, y volviéndonos a centrar en este caso, las tecnologías e informáticas , como tal se han vuelto en una parte esencial de la vida del ser humano, sea porque facilita mucho sus trabajos a desarrollar, o sea por el simple hecho que está dentro la naturaleza humana el progreso y la evolución.

Como segundo punto que el autor toca o menciona es cuando hace alusión a que hoy en día nos encontramos en un procedimiento de transnacionalización del derecho penal tal cual hoy en día se le conoce, además nos dice que para que este sistema protector de estos nuevos bienes jurídicos sea óptimo, se es completamente necesario que todas las naciones reafirmen su compromiso regulando sus ordenamientos jurídicos para llegar a una uniformidad entre todos los estados , pues bien , aquí es un punto obligatoriamente imperativo que menciona el autor menciona, como tal los ciberdelincuentes o los individuos quienes ejercen estos hechos delictivos cada día con el mismo avance de las nuevas tecnologías, van evolucionando para mejorar en el comisó de sus hechos ilícitos, y la única forma de poder enfrentar esta amenaza global ,es realizando un trabajo de cooperación y unificación internacional, ya que de otra manera todo estado a nivel mundial es totalmente vulnerable.

Voy a tomar como antecedente la norma o base legal Peruana con relación a los delitos informáticos, en un inicio se encontraba tipificado en el artículo 186 , inciso 3, del segundo párrafo dentro del Código Penal de 1991 , esta regulación no era propia de un ilícito o delito, sino en cambio lo tenían como una agravante del delito de hurto.

También es necesario mencionar que los delitos informáticos estaban previstos en el capítulo XII del Código Penal Peruano en los siguientes artículos:

- Artículo 207- A (Realizar interferencia , copia ilícita o acceso a una base de datos)
- Artículo 207- B (La alteración , destrucción o daño de una base de datos)
- Artículo 207- C (Las circunstancias agravantes ,cualificantes)
- Artículo 207- D(El tráfico ilegal de datos); también de las leyes penales

especializadas

De igual forma cabe mencionar que las leyes penales especiales, se encuentran en la Ley 30096 "*Ley de Delitos Informáticos",* esta ley estaba constituida por siete capítulos que se estructuraban de la siguiente manera:

- Capítulo 1; Objeto y finalidad de la ley
- Capítulo 2, Delitos contra sistemas y datos
- Capítulo 3 Delitos informáticos contra la libertad sexual y la indemnidad
- Capítulo 4, Delitos informáticos contra el secreto de las comunicaciones y la intimidad
- Capítulo 5, Delitos contra el patrimonio
- Capítulo 6, Delitos contra la fe pública
- Capítulo 7, Disposiciones comunes

Posteriormente se llegó a promulgar la Ley N° 30171 "Ley que modifica la Ley que modifica la Ley N° 30096 escuadrándolos a los parámetros legales del convenio de Budapest, al ingresar dentro de la redacción clásica de los artículos 2, 3, 4, 7, 8 y 10 de la mencionada ley.

Añadiendo dentro de la tipificación clásica de los artículos 2,3,4,7,8 y 10 , de la referida Ley la posibilidad de cometer el delito deliberada e ilegalmente.

Las correcciones o modificaciones dentro de la ya mencionada Ley N°30171, en relación a los delitos informáticos, se centra en lo siguiente:

- Artículo 1 con sus respectivas modificatorias, dos, tres, cuatro, cinco, siete, ocho y diez de la *Ley de delitos informáticos.*
- Artículo 2, con sus modificatorias de la 3ra , 4ta y 11va disposiciones complementarias finales de la Ley N° 30096
- Artículo 3, incorporación del articulo doce a la Ley N° 30096
- Artículo 4, modificaciones de los artículos 158,162 y 323 del Código Penal
- Artículo 5, Incorporación de los artículos 154-A y 183-B del Código Penal

1.2. MARCO TEÓRICO

En la presente investigación está dividida en aspectos según su nivel de relevancia para lograr sustentar y definir los conceptos fundamentales sobre el tema a investigar.

Zevallos (2011) se puede definir como marco teórico a una presentación de fundamentos que darán paso a la explicación especifica de temas y subtemas usados para el avance de la investigación (p.21)

1.2.1. Delito

Comúnmente se define al delito como la acción y omisión penada por ley, pero según el Código Penal lo define como: "Las acciones u omisiones dolosas o culposas penadas por Ley (*La acción activa o pasiva es la base de la conducta punible*)".

Gutiérrez (2010) menciona "Un delito es una conducta que, ya sea por propio carácter o por imprudencia, resulta contrario a lo establecido por la ley. El delito, implica una violación de las normas vigentes, lo que hace que merezca una sanción o pena". (p.12)

Esto nos quiere decir que el delito es un acto u omisión que reguladas en la Ley, son penadas por ser antijurídicas.

1.2.2. TICS (tecnologías de información y Comunicación)

Estas denominadas TICS vienen a ser el conjunto de tecnologías creadas para administrar información y enviarla de un lugar a otro. Contienen una gran cantidad de soluciones muy amplias y fáciles de acceder a todo tipo de información.

> En un ámbito más amplio podríamos inferir que las nuevas tecnologías de la información y la comunicación, son aquellas que orbitan alrededor de tres pilares básicos: La microelectrónica, la informática y las comunicaciones, sin embargo, no lo hacen de forma independiente, sino de forma más significante, interactiva e interrelacionadas, lo que provoca descubrir nuevas realidades comunicativas. (Cabrero, 1998, p.198)

Existe una diversidad de definiciones para las denominadas TICS a través de algunos benchmarching, las instituciones educativas y organizaciones internacionales las clasifican como una metodología de aprendizaje y/o un instrumento facilitador de las interrelaciones humanas. (Cobo, 2009, p.24)

1.2.3. Delitos informáticos

Mazuelos (2014) Los delitos informáticos son aquellos que se vinculan con la concepción de que la comisión del crimen se hacen a través del empleo de la computadora, internet, etc. (p.14)

Según el Convenio Internacional de Ciberdelincuencia llega a conceptualizar a los delitos informáticos como: "[...] Los actos señalados en contra de la confidencialidad, integridad y disposición de los sistemas informáticos, redes y datos de información, igualmente el abuso de esos sistemas".

Por otro lado la División de Investigación de Delitos de Alta Tecnología (DIVINDAT), señala a los Delitos Informáticos como: "Toda conducta, que atente los bienes jurídicos, para el cual se utilice medios informáticos en alguna de sus fases de ejecución, es decir es aquel delito que se realiza con la ayuda de la informática o de técnicas anexas y no necesariamente se trata de "Nuevos Delitos", sino de nuevas formas de ejecutar las figuras típicas tradicionales".

Por ello es que para este tipo de delitos el empleo de medios tecnológicos es la principal herramienta de la comisión del delito.

Cabe mencionar que en cuanto a la conducta sancionada:

Villavicencio (2015) "La criminalidad informática es aquel comportamiento basado en burlar los sistemas de seguridad de los dispositivos, por ejemplo invasiones a computadoras, correos o sistemas de datas; es decir conductas atípicas que pueden ser dadas a través de la tecnología". (p.16)

Callegari (2008) define a los delitos informáticos como "aquel delito que se realiza con la colaboración de la capacidad en informática o técnicas anexas" (p.65)

Rodríguez (1989) conceptualiza al delito informático como: "la ejecución de una acción que logra ser llevada a cabo utilizando un elemento informático o vulnerando los derechos del dueño de un instrumento informático, ya sea hardware o software" (p.23)

Define al delito informático como, "la realización de una acción que reuniendo que delimitan el concepto de delito, sea llevada a cabo utilizando un elemento informático y/o telemático, o vulnerando los derechos del titular de un instrumento informático, ya sea hardware o software" (p.23)

Además según Poinst (2003)

> Se pueden definir como delitos informáticos a aquellos comportamientos ilícitos efectuados por medio de procesos electrónicos, como tales delitos comunes que su ilicitud recaía en bienes que presentaban una configuración predeterminada en el desarrollo o también sobre nuevos objetos tales como software y hardware (P.165)

> Delitos informáticos, se usara el termino para hablar del comportamiento ilícito y criminal dentro de lo que abarca el ciberespacio, bien como una rama que abarca a todos (o a muchos de ellos), además de esto para estar frente la presencia de la cibercriminalidad no será basto que solo se encuentra en una de las TICS para ejecutar la acción delictiva, sino que será de obligatoria exigencia tal uso tenga que ver con algún elemento del delito (Felson, 2012, p.45)

Se usara el termino como tal delitos informáticos, para hacer alusión tanto ala as acciones ilícitas dentro del ciberespacio, y en muchos casos , para poder insertar el término de cibercrimen ,dentro de este fenómeno a un tipo de comportamiento en concreto (Miro, 2010, p.78)

Grrabosky (2010) Delitos informáticos hace referencia a todas las conductas que puedan reunir características de carácter tipológicas que forman parte del fenómeno. (p.15)

Callegari (2003), Delitos informáticos los podemos definir cómo las herramientas que da ayuda de la informática o de técnicas anexas , para lograr concretar una actividad ilícita se estaría cayendo dentro de lo que abarca la definición de este amplio termino. (p.56)

a) Tipos de Delitos Informáticos reconocidos por la Organización de las Naciones Unidas (ONU)

Los delitos informáticos reconocidos por la Organización de las Naciones Unidas en el XV congreso realizado, los clasificaron de la siguiente forma:

- **a)** Fraudes realizados por medio de manipulación de computadoras
- **b)** Falsificaciones informáticas

c) Modificaciones o daños de programas o datos computarizados

d) Otros ilícitos que podrían ser cometidos y que se hallen relacionados de manera directa con acciones efectuadas contra los propios sistemas

Adicionalmente estas ramificaciones tienen dentro delitos informáticos más específicos los cuales son detallados a continuación:

a.1) Fraudes realizados por medio de manipulación de computadoras

- Manipulación de datas de entrada:

Este tipo de engaño informático es famoso como sustracción de datos, la cual simboliza el delito informático más usual requerido ya que es sencillo de incurrir y a la vez muy difícil de ser descubierto. Este delito no necesita de conocimientos técnicos dentro de lo que es la informática, ya que se puede ejecutar por cualquier persona que tenga acceso a las datas o funciones normales de procesamiento informático o datos en la fase de adquisición (ONU, XV congreso, 2013, p.122)

- Manipulación de programas:

Es difícil de descubrir y generalmente pasa de manera inadvertida, razón por la cual el delincuente debe contar con conocimientos técnicos y definidos de informática. Este ilícito se centra en alterar programas o rutas. Una técnica más comúnmente empleada por personas que cuentan con conocimientos especializados en informática y programación, un ejemplo es conocido caballo de Troya, el cual se da mediante instrucciones computarizadas de forma camuflada en un programa informático para poder realizar una función no permitida en el mismo momento que se realiza su función normal. (ONU, XV congreso, 2013, p.122)

- Manipulación de datos de salida:

Se ejecuta colocando un objetivo dentro de la función del sistema informático. Tomando como ejemplo más frecuente el fraude realizado con el fin de atacar a los cajeros automáticos, mediante falsificación de instrucciones para el ordenador, en la fase de adquisición de data. De modo usual esos fraudes se entendían en base a tarjetas de crédito robadas, por ello en la actualidad se usan ampliamente programas y materiales especializados para decodificar indagación electrónica en las bandas magnéticas de las

tarjetas bancarias y tarjetas de crédito. (ONU, XV congreso, 2013, p.123)

- Fraude usado por manipulación informática:

Emplea las reproducciones de manera instantánea de las fases computacionales. Es un modo o habilidad en el uso de la palabra, especializada que se le designa "La técnica del Salchichón" en las que laminas muy finas, casi evidentes de intercambio financiero, se van restando de forma paulatina de una cuenta a otra (ONU, XV congreso, 2013, p.123)

a.2) Falsificaciones informáticas:

-Como objeto: Sucede en el momento que se modifica cifras, números, cantidad, referencia, de los documentos custodiados de forma computarizada.

-Como Instrumentos: Las computadoras mandan disponer de similar forma desarrollar adulteraciones de documentos de utilización mercantil. Cuando inicio a hallarse con fotocopiadoras computarizadas que contengan con colores a procedencia de rayos laser, se presentó una generación de adulteración o imitación fraudulentas. Es asi como estas fotocopiadoras pueden realizar duplicados de alta calidad, sin la necesidad de invocar al original, tanta es la similitud al original, que solo un entendido del tema podría diferenciarlos pero con complicaciones y dificultad con los originales (ONU XV, congreso, 2013, p.125)

a.3) Modificaciones o daños de programas o datos computarizados

Estas se consiguen lograr mediante:

-Sabotaje informático:

Es la acción que consiste en suprimir, borrar u modificar sin contar con un permiso, las actividades o datos de un ordenador con el deseo de estorbar u obstaculizar la actividad habitual del sistema. Los métodos que admiten perpetrar sabotajes informáticos son:

-Virus: Es una tipo de cifras programadas que sirven para unirse a los programas oficiales y transferirse a otros sistemas informáticos .Un virus logra perpetrar a un sistema a través de un canal de una sola parte oficial de soporte lógico que ha sido contagiado, así como también usando el modo del "Caballo de Troya"

-Gusanos: Se construye de modo similar a la creación de un "virus" , este cuenta con más intención de colarse en programas oficiales de proceso de tratamiento de datos o con el motivo de destruir o modificar la data, sin embargo en contra posición del virus , este no lograra renovarse .por ello podemos decir que el gusano es un cáncer benévolo

y el virus es un cáncer maligno .Si bien es verdad , el efecto del daño de un gusano podrían ser tan peligroso al igual que las de un virus .Como modelo podemos manifestar que un programa gusano que provisionalmente se demolerá podría dar órdenes a un sistema informático de una financiera para que traslade incesantemente riqueza a una cuenta ilegal.

-Bomba cronológica o lógica: Esta solicita de modo forzoso entendimiento especializados, ya que requiere de una programación especial, para la aniquilación o transformación de datos en un instante dado a posterior .Pues bien al opuesto del virus o gusanos como tal , las llamadas "Bombas lógicas" son muy complejas de descubrir antes de que estallen ; por ello del conjunto de aparatos informáticos delincuenciales, las bombas lógicas son las que adquieren la mayor potencia de daño .Su estallido puede planificarse para que cause un daño muy alto y para que goce de una zona su estallido un periodo de tiempo después de que se vaya el delincuente .La bomba lógica puede emplearse asimismo como un arma para la extorsión o amenaza y se puede requerir un pago de liberación a cambio de enterarse donde se localiza la bomba (ONU XV, congreso, 2013, p.126)

-Entrada no permitida a servicios y sistemas informáticos:

Suceden por muchas justificaciones y argumentos, desde sencilla fisgonearía, tal como el tema de los piratas informáticos "hackers" inclusive al sabotaje o espionaje informático (ONU, X V congreso, 2013.p.190)

-Hackers o Piratas informáticos:

Este tipo de entrada se efectúa de forma usual desde un sitio apartado, instalado en la red de transmisión, invocando a varios medios de entrada .El delincuente puede emplear la carencia de inflexibilidad de los sistemas de seguridad para poder tener dominio de entrada o descubrir debilidades en las medidas de seguridad o en procedimientos del sistema. Usualmente los piratas informáticos simulan ser usuarios verdaderos o auténticos del sistema, esto suele pasar con excesiva continuidad en los sistemas en los que los usuarios pueden emplear contraseñas sencillas o passwords de mantenimiento que están en el propio sistema (ONU, X V congreso, 2013.p.190)

-Copias no autorizada de programas informáticos de seguridad legal:

> Puede encontrarse una gran pérdida monetaria para los verdaderos titulares del programa. Dentro de muchas competencias han estandarizado como delito este tipo de actividades y las han sancionado con penas de carácter penales. El punto de la cuestión ha logrado magnitudes de naturaleza transnacional, con la piratería de esas copias no autorizadas a través de las redes de comunicación del hoy en día. Con respecto, a la reproducción no autorizadas de sistemas informáticos no es un delito ya que el bien jurídico protegido a tutelar es la propiedad intelectual (ONU, X V congreso, 2013.p.190)

a.4) Otros delitos que lograrían ser perpetradas y que se encuentran atados directamente a actividades realizadas contra los mismos sistemas:

- Acceso no autorizado: se da con la utilización adulterada de contraseñas y entrada de un sistema informático sin el permiso del dueño.
- Destrucción de datos: este delito provoca daños en la red debido a la inserción de virus, bombas lógicas, etcétera.
- Transgresión al Copyright de base de datos: este delito empieza con el empleo no legal de datos guardados en una base de información.
- Interceptación de mensajes electrónicos: se da por la sencilla leída de un mensaje electrónico que no es nuestro.
- Fraudes electrónicos: este tipo de delito se da atreves de ejecutar compras por internet.
- Traspaso de dinero: este delito funciona mediante mentiras en la ejecución de operaciones financieras vía electrónicas (ONU, XV, congreso, 2013, p.210)

b) Clases de Delitos Informáticos

Según la DIVINDAT (2012) Se clasifican en:

b.1) Método: Se da en conductas criminológicas donde los sujetos usan formas electrónicas para conseguir un resultado ilegal.

b.2) Medio: Se les denomina a los comportamientos ilícitos que se realizan por medio del empleo de artefactos como computadoras como instrumento.

b.3) Fin: Acciones de índole criminal que son destinadas en contra de las computadoras,

programas o accesorios como entidad física (p.45)

c) Los delitos informáticos con mayor incidencia en Perú

Por otro lado, tal como explica el Mayor PNP Juan Manuel Moretti, de la DIVINDAT. Menciona que los siguientes delitos informáticos son los más frecuentes:

c.1) Clonación de tarjetas o skimming

> Esta modalidad consiste en copiar la banda magnética de la tarjeta para luego transferir la información confidencial (número y clave) a otra tarjeta en blanco. Y una vez realizado este proceso, los delincuentes realizan retiros a través de cajeros automáticos o efectúan pagos en dispositivos POS con tarjeta clonada como si fueran el titular (DIVINDAT, 2015, p.5)

c.2) Pharming

> Es otro de los mecanismos más usados por los delincuentes para llegar hasta las cuentas bancarias de sus potenciales víctimas. Para esto se hace uso de páginas web falsas que suplantan a las originales. Con el Pharming, el hampa busca atraer a sus víctimas hasta estos websites para apoderarse de información confidencial que luego usaran en su perjuicio. (DIVINDAT, 2015, p.5)

c.3) Phishing

> A través de esta modalidad de fraude los delincuentes buscan acceder a esta información personal mediante el envío de correos falsos que solicitan actualización de información personal. Así como buscar conocer números de las cuentas bancarias y claves de seguridad. (DIVINDAT, 2015, p.5)

1.2.4. Perfil del Ciberdelincuente

Robles (2010) menciona que: “El perfil del ciberdelincuente (sujeto activo) en esta modalidad delictual requiere que este posea ciertas habilidades y conocimientos detallados en el manejo del sistema informático”. (p.88)

Es en razón a esas cualidades que se les ha calificado a los sujetos activos como a los denominados delincuentes de "cuello blanco" que tienen como características:

> **a)** Poseer importantes conocimientos informáticos, b) Ocupar lugares estratégicos en su centro laboral, en los que se maneje información de carácter sensible, se denominan delitos ocupacionales, debido a que se cometen por la ocupación que se tiene y el acceso al sistema". (Robles, 2010, p.89).

Para Manson (2010) afirma que:

> "[…] Los infractores de la ley penal en el caso de delitos informáticos, no son delincuentes comunes y corrientes, sino que por el contrario, son personas especializadas en la materia informática, además que "los sujetos que incurren en estas infracciones, son las que poseen ciertas particularidades, que no presentan el perfil usual esto es, competencias para el empleo de los sistemas informáticos y que por su localización trabajan en lugares importantes, donde se maneja información personal" (p.89)

Camacho (2014) considera que: "[…] el perfil de los delincuentes informáticos, no coincide con el delincuente marginal y se caracteriza a los autores de estos delitos como empleados de confianza en las empresas que se ven afectadas por esta modalidad delictual" (p.36)

Vives, Antón y Gonzales afirman que: "[…] el sujeto activo puede ser tanto las personas que legítimamente autorizadas puedan acceder y operar el sistema tales como los operadores u programadores. Como terceros no autorizados que acceden a las terminales públicas o privadas (p.54)

Asimismo Gutiérrez y Ruiz (2012) definen desde sus puntos de vista y sostienen que: "[…] el autor del delito informático puede serlo cualquiera, no precisando el mismo de determinados requisitos personales o conocimientos técnicos cualificados" (p.78)

Por mi parte, considero que el sujeto activo puede ser cualquier persona que con conocimientos y habilidades en informática, si bien comparto en parte la postura de que el sujeto activo debe ocupar un puesto laboral que le permita acceder a información sensible,

no por ello estarán excluidos los sujetos que sin ocupar algún cargo estratégico pueden ser sujeto activo, por sus habilidades y conocimientos sobre la informática. Por ende, a estos sujetos se les denomina de diferentes maneras dependiendo en el modo de cómo actúan y que conductas son las que realizan

a) Tipos de Delincuentes Informáticos

Los delincuentes informáticos se dividen en:

- **Hackers**:

Saín (2010) menciona que:

> […]La palabra "hacker" aparece en la década del 60 en Estados Unidos, así se autodenominaban los miembros del Instituto de Tecnología de Massachusetts (MIT), aquellos programadores que trabajan en el campo de la informática interactiva para que las computadoras pueden comunicarse entre sí a través de la innovación tecnológica. (p.32)

Son aquellos que dolosamente interceptan un medio de índole informática, con la finalidad de afectar, obstaculizar, viciar, divulgar, eliminar información de carácter público o particular halladas en ordenadores (Mamani, 2017, p.34)

Para Sain (2010)

> […] En la actualidad existe una clasificación, que los divide en hackers de sombrero blanco y hackers de sobrero negro. Los hackers de sombrero blanco o hackers éticos que actúan para proteger los sistemas buscando vulnerabilidades para solucionarlas, el conocimiento, el descubrimiento y cómo funcionan las cosas. Los hackers de sombrero negro tienen fines ilícitos y buscan dañar o beneficiarse económicamente en base a terceros e intentan penetrar en las redes para extraer información, virus plantares, correos de hackear, etc. (p.23)

- **Crackers**:

Meléndez (2009) “el cracker es también un apasionado del mundo informático. La principal diferencia consiste en que la finalidad del cracker es dañar sistemas y ordenadores. Tal como su propio nombre indica "rompedor", su objetivo es el romper y producir el mayor daño

posible". (p.43)

Se le denomina ad esta forma a aquel delincuente más dañino que el denominado "hacker", ya que se subdivide en dos clases: A) Aquel que se inmiscuye o adentra en un sistema informático para hurtar información y destrozarla. B) El que suprime las seguridades de páginas webs, programas y destruye anti copias (Mamani, 2017, p.35)

- **Phreaker:**

Son delincuentes que entran a un medio de telefonía con o sin ordenadores con la finalidad de adueñarse, obstaculizar, lacerar, eliminar, revisar, distribuir, acabar. Además es también para dañar los medios de control, pago y facturación (el más conocido es para clonación tarjetas) (Mamani, 2017, p.35).

- **Virucker:**

Son los que crean virus que afectan los dispositivos móviles o computadoras (Mamani, 2017, p.35)

- **Pirata Informático:**

Quien copia, reproduce, vende, dona programas de software que no le pertenece o que no tiene licencia para ello. Se puede decir que es quien adultera el programa informático, su instalación o su documentación (Mamani, 2017, p.35).

Además es importante señalar que la entidad encargada de perseguir a estos delincuentes informáticos es la DINVINDAT.

1.2.5. Capacitaciones sobre Delitos Informáticos

Para empezar con el tema de las capacitaciones acerca de los delitos informáticos primeramente debemos definir qué es capacitación, es por ello que para Mene (2002) "Capacitación es el proceso de desarrollo que sigue el sujeto humano hasta alcanzar un estado de plenitud personal, las maneras en que se puede ayudar en el empeño mediante un influjo metódico con arreglo a un plan". (p.34)

También es importante lo que dice el país de Colombia, respecto a las capacitaciones en estos temas.

> […] La capacitación de los comisarios en Colombia ha servido para brindar los instrumentos con estándares internacionales en la atención y prevención, para el caso de delitos informáticos; así como entrenamiento en la valoración de riesgo, proceso de atención y seguimiento sobre las medidas de protección recibidas. Los comisarios y los usuarios pueden acceder al proceso, en las comunidades sin acceso a la justicia. (Consejo de la Judicatura, 2013, p.3).

En el caso peruano para la capacitación de delitos informáticos la Ley Nº 30096 en su quinta disposición complementaria no derogada señala que:

> *"Las instituciones públicas involucradas en la prevención y represión de los delitos informáticos deben impartir cursos de capacitación para mejorar la formación profesional de su personal, especialmente de la Policía Nacional del Perú, el Ministerio Público y el Poder Judicial en el manejo de los delitos previstos en la presente Ley".*

1.2.6. División de investigación de delitos de alta tecnología (DIVINDAT)

> [...] Es el organismo encargado de la "dirección de investigación criminal de la Policía Nacional del Perú (PNP) , que tiene como objetivo principal, investigar denunciar y combatir el criminen organizado transnacional, así como también otros delitos transcendentes a nivel nacional en el campo de los "delitos contra la libertad, el patrimonio, la seguridad pública, tranquilidad ciudadana, la defensa y seguridad nacional, la propiedad industrial y otros, que se cometan mediante el uso de la tecnología y redes de comunicación, capturados los indicios, pruebas y evidencias, para identificar, ubicar y detener a los autores del delito, a fin de colocarlos a la disposición de las autoridades pertinentes (MININTER, 2006, p.2).

> […] La División de investigaciones de delitos de alta tecnología (D.I.V.I.N.D.A.T) que pertenece al organismo de la DIRINCRI – PNP, tiene como responsabilidad patrullar lo que es todo el ciberespacio de los ciudadanos peruanos. La DIVINDAT nació en agosto del año 2005 (antes de la aparición de esta entidad los delitos mencionados eran tratados por la División de Estafas de la DIRINCRI). Durante ese año se registraron 456 denuncias, de ellas 243 casos se resolvieron quedando pendientes 213 casos (DIVINDAT, 2006, p.3).

1.2.7. Ordenamiento Nacional

Cabe mencionar que en el ordenamiento nacional los delitos informáticos estuvieron regulados de manera general en el Código Penal hasta el año 2000 en el cual se aprobó la Ley N° 27309, Ley que incorpora los delitos informáticos al Código Penal. De ahí en el año 2014 se aprobó la Ley Nº 30096, Ley de Delitos Informáticos, que debido a problemas de redacción típica fue modificada por la actual Ley Nº 30171, modificando los artículos 2,3,4,5,7,8 y 10.

Adicionalmente cabe señalar las normas complementarias

- Decreto Legislativo Nº 1182 (Decreto Legislativo que regula el uso de los datos derivados de las telecomunicaciones para la identificación, localización y geolocalización de equipos de comunicación, en la lucha contra la delincuencia y el crimen organizado).
- Ley Nº 28493, Ley que regula el uso del correo electrónico comercial no solicitado (SPAM) y su reglamento D.S. Nº 031-2005-MTC.

1.2.8. Finalidad y objeto de la Ley

Dentro del artículo 1 de la *Ley de Delitos informáticos* señala:

> *"La ley tiene como objetivo principal o finalidad prevenir y sancionar las conductas ilegales que afectan los sistemas, las datas informáticas, el secreto de las comunicaciones y otros bienes jurídicos de relevancia penal (tales como la fe pública, el patrimonio, la libertad sexual, etc.) Que pudieran verse afectados, por medio del empleo de las TICS (Tecnologías de la información y comunicación) teniendo como finalidad la de asegurar las condiciones mínimas para que las personas gocen del derecho a la libertad y el desarrollo"*

De la misma forma que se ha visto anteriormente dentro del artículo 1 de la Ley de delitos informáticos establece que el fin perseguido por dicha normativa es de prevenir y sancionar las conductas ilícitas que afectan los sistemas, las datas informáticas, el secreto de las comunicaciones; y otros bienes jurídicos de relevancia penal (como lo es la fe pública, la libertad sexual, etc.) y que estas pueden ser afectados mediante la ubicación de las TICS,

con la finalidad de garantizar las condiciones mínimas para que las personas gocen del derecho a la libertad y al desarrollo. Gracias a esta ley se puede tratar de garantizar la lucha óptima contra la ciberdelincuencia.

Esta ley no responde solo a la necesidad de ejercer acción punitiva del estado enfocado en la protección de la información; sino que tiene como principal objetivo la estandarización de la ley penal peruana con el ordenamiento penal internacional de manera principal por el convenio contra la cibercriminalidad del consejo europeo denominado "convenio de Budapest".

Además es relevante hacer mención cual es el Bien Jurídico Tutelado de este delito , según la Ley antes mencionada , dicta que: "*El bien jurídico protegido en los delitos informáticos se crea de manera unísona y enlazada, siendo que el primero se haya la información de manera general(información almacenada, tratada y trasmitida mediante los sistemas de tratamiento automatizado de datos) y en el segundo plano , los otros bienes que son afectados por medio de estos tipos de ilícitos, tales como la identidad sexual , intimidad , etc.".*

Respecto de la información deber ser entendido como el contenido de las datas y las bases de estas mismas y/o banco de información o el producto de los procesos informáticos automatizados; Por lo tanto se constituyen un bien autónomo de valor económico y es la importancia de la información lo que ha hecho que se inserte como bien jurídico tutelado.

No obstante, es necesario señalar también cuales son los sujetos en el tipo penal de delitos informáticos.

1.2.9. Sujeto Activo

Según Garrido (1993) menciona

> "Las personas que realizan o cometen los delitos informáticos, son quienes tienen algunas características que no poseen el común de las personas quienes delinquen, como, estas personas activas poseen cualidades para el empleo de sistemas informáticos y usualmente por su situación de trabajo donde puedan encontrarse en sitios valiosos donde se hace uso de datas de carácter sensible o bien poseen habilidades que se desarrollan en el empleo de sistemas computarizados, aun cuando en muchos de los sucesos, no se desenvuelvan tareas laborales que faciliten la ejecución de este modo delictivo" (p.54).

En lo remarcado con anterioridad por Garrido se puede decir que el sujeto activo debe ser quien tenga conocimientos bastos y técnicos de la rama de la informática, esto quiere decir, una persona con un alto grado de instrucción en cómputo para conseguir manipular la información contenida en los sistemas, que como menciona el autor bien podría ser su centro de trabajo en caso se maneje información.

1.2.10. Sujeto pasivo

Según Rivero (2008) menciona que:

> El sujeto pasivo es aquella sujeto quien es dueño del bien jurídico, que el juez protege y sobre la cual recaer la actividad típica del sujeto activo, adicionalmente que el sujeto pasivo o también conocido como el perjudicado del delito es la persona que recibe la conducta de acto u omisión que ejerce el sujeto llamado activo y en el temas de los delitos informáticos, los perjudicados suelen ser personas, gobiernos, inclusive financieras, etc., todo aquel que utilice sistemas que se hallan automatizados en el manejo de datos informáticos usualmente estarán unidos a otros (p.23).

Por consiguiente, el sujeto pasivo pueden ser aquellas personas, instituciones de crédito, esto quiere decir entidades que usan sistemas automatizados de información así como también cualquier persona natural que haya visto vulnerada por el actuar ilícito del sujeto activo.

1.2.11. Bien jurídico protegido

Ahora, el bien jurídico protegido en general es la información, pero está considerada en diferentes formas, puede que sea como un valor económico, o también puede considerarse como un valor intrínseco de la persona, por su fluidez y trafico jurídico y finalmente por los sistemas que la procesan o automatizan los mismo que se equiparan a los bienes jurídicos protegidos conocidos como tales:

a) El patrimonio

"Dentro de la amplia gama de fraudes informáticos y manipulaciones de datos podemos observarlas" (Acurio, 2006, p.34).

b) La reserva, la intimidad y confidencialidad de los datos:

Acurio (2006) “En escenario donde se nos plantea las agresiones informáticas a la esfera de la intimidad en forma general, especialmente en el caso de los bancos de datos” (p.34)

c) La fiabilidad, seguridad del tráfico jurídico probatorio:

Es cuando hay una existencia de falsificación de datos o documentos probatorios vía medios informáticos” (Acurio, 2006, p.34)

d) El derecho de propiedad

Acurio (2006) “Este escenario que nos habla sobre la información o sobre los elementos físicos, materiales dentro de un sistema informático, que es vulnerado por los daños y el llamado terrorismo informático” (p.32)

Por otro aspecto Villavicencio (2015) menciona:

> Es imperativo hacer mención que el bien jurídico tutelado en los delitos informáticos se concibe en los plenos de forma agrupada y conjunta; en el primero se encuentra la información de manera general (información almacenada, tratada y transmitida mediante los sistemas de tratamiento automatizado de datos) y en el segundo plano, los demás bienes afectados por medio de esta clase de ilícitos como son la indemnidad sexual, intimidad etc. (p.45)

Con relación a la información debe ser entendido como el contenido de las bases y/o banco de datos o el producto de los procesos informáticos autorizados; por lo tanto se conforma como un bien de autónomo de valor económico

Además es la relevancia del valor económico de la información lo que ha hecho que se instale como bien jurídico protegido

Asimismo Villavicencio (2015)

> […] la información se debe considerar de diferentes maneras , y no solo como un valor económico , sino como un valor intrínseco de la persona por la fluidez y el tráfico jurídico, y por los sistemas que lo procesan o automatizan, los mismos que se equiparan a los bienes protegidos comúnmente, tales como: el patrimonio (fraude Informático), la reserva a la intimidad y confidencialidad de los datos (agresiones informáticas a la esfera de la intimidad), la seguridad o fiabilidad del tráfico jurídico probatorio (falsificación de datos o documentos probatorios), etc. (p.25)

Por consiguiente, en esta clase de delitos no se puede plantear a la información como el único bien jurídico afectado, por ser el principal y el más importante, sino a un grupo de bienes

que son vulnerados, debido a la característica de la conducta típica en esta modalidad delictiva que colisiona con diversos intereses colectivos. En ese sentido que coincidimos.

1.2.12. Convenio Internacional sobre Cibercriminalidad

Según Prado (2008) menciona que: "Debido al incremento de los delitos digitales, el consejo europeo, en el 2001 público un proyecto que buscaba homogenizar las legislaciones de sus 48 miembros y de los países observadores para apoyar la lucha contra los crímenes en el sistema digital. Así, The Convention on Cybercrime (ETS), entro en vigencia tres años después y en la actualidad cuenta con 45 miembros adicionales a los europeos. Entre los delitos que se buscan perseguir destacan la pornografía infantil y el fraude informático" (p.24)

Además Díaz (2010) nos menciona que el convenio de Budapest está dividido de la siguiente manera:

> "{...] En cuanto a la estructura del Convenio sobre la Cibercriminalidad, éste consta de 48 artículos y un preámbulo inicial. En concreto encontramos hasta cuatro capítulos, divididos en secciones y títulos. El primer capítulo tan sólo comprende un precepto, referido a la terminología usada en el texto. El capítulo segundo «Medidas que deberán adoptarse a nivel nacional», incluye elementos tanto de Derecho material (responsabilidad penal, tentativa, complicidad) como procesal (procedimiento, salvaguardas, datos, registros, jurisdicción). (p.195)

En cuanto al tercero, se perpetra abiertamente en la ayuda internacional. Abarcando debates tales como: la extradición, la asistencia entre países, la información, el traspaso de información y la instauración de una red 24/7. El último título comprende las disposiciones finales inherentes a un Tratado internacional: adhesión, entrada en vigor, aplicación territorial, efectos, régimen de reservas, denuncias, notificaciones, etc." (Díaz, 2010, p.196)

> […] Es también conocido como el convenio de Budapest dado en el año 2004 es el primer Tratado Internacional que explora e investiga para enfrentarse a las infracciones informáticos incurridos a través de métodos de tecnología yla red, a través de legislación nacional, el mejoramiento de los métodos de exploración y colaboración entre países, Asimismo se exige a cada estado participante a prestar colaboración entre países en lo más, que sea posible para la ejecución de indagaciones y métodos concernientes a delitos

> penales asociados al sistemas o para bases de datos para la recogida de pruebas electrónicas respecto a una infracción penal". (Cabrera, 2014, Pag.40)

Por otro lado, Alejos (2016) menciona que:

> "Este convenio es necesario para prevenir los actos que atenten a la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos de las redes y de los datos, así como el uso fraudulento de esos sistemas, asegurando la incriminación de dichos comportamientos, como los descritos y atribución de poderes suficientes para permitir una lucha eficaz contra estas estas infracciones penales, facilitando la detección, la investigación y la persecución, tanto a nivel nacional como internacional y previniendo algunas disposiciones materiales a la cooperación internacional rápida y fiable, al ser uno de los primeros convenios que marca la pauta donde comienza el derecho en la era digital" (p.17)

Finalmente, Lerna (2014) menciona que: "El convenio de Cibercriminalidad persigue básicamente tres objetivos en torno a los cuales se estructura, a saber: armonizar el Derecho Penal material, establecer medidas procesales o cautelares adaptadas al medio, digital y poner en funcionamiento un régimen rápido y eficaz de cooperación internacional" (P.89)

1.2.13. Modelos de tratamiento de los delitos informáticos en el derecho comparado

a) Modelo de Alemania

En Alemania, para hacer frente a la delincuencia relacionada con la informática, el 15 de mayo de 1986 se adoptó la Segunda Ley contra la Criminalidad Económica. Esta ley reforma el Código Penal (artículo 148 del 22 de diciembre de 1987) para contemplar los siguientes delitos:

- Espionaje de datos (202a).
- Estafa informática (263a).
- Falsificación de datos probatorios (269) junto a modificaciones complementarias del resto de falsificaciones documentales como el engaño en el tráfico jurídico mediante la elaboración de datos, la falsificación ideológica, el uso de documentos falsos (270, 271, 273).

- Alteración de datos (303a) es ilícito cancelar, inutilizar o alterar datos e inclusive la tentativa es punible.
- Sabotaje informático (303b).
- Destrucción de datos de especial significado para medio de deterioro, inutilización, eliminación o alteración de un sistema de datos. También es punible la tentativa.
- Utilización abusiva de cheques o tarjetas de crédito (266b).
- Por lo que se refiere a la informática, el perjuicio patrimonial que se comete consiste en influir en el resultado de una elaboración de datos por medio de una realización incorrecta del programa, a través de la utilización de datos incorrectos o incompletos, a través de la utilización no autorizada de datos a través de una intervención ilícita. Esta solución también se adoptó en los Países Escandinavos y en Austria**.**

b) Modelo de Estados Unidos

Considerado importante mencionar la adopción de los Estados Unidos en 1994 del Acta Federal de Abuso Computacional (18 USC Sec.1030) que modificó el Acta de Fraude y Abuso Computacional de 1986. Con la finalidad de eliminar los argumentos hiperténicos acerca de qué es y que no es un virus, un gusano, un caballo de Troya, etc. y en que difieren de los virus, la nueva acta prohíbe la transmisión de un programa, información, códigos o comandos que causan daños a la computadora, al sistema informático, a las redes, información, datos o programas (18 USC: Sec. 1030 (a) (5) (A). La nueva ley es un adelanto porque está directamente en contra de los actos de transmisión del virus El Acta de 1994 diferencia el tratamiento

Un daño por la transmisión de un virus, el castigo de hasta 10 años en prisión federal más una vez y para aquellos que lo transmiten de manera imprudente la sanción fluctúa entre una mañana y un año en prisión.

Nos llamó la atención que el Acta de 1994 nos dijo que el creador de un virus no pudo escudarse en el hecho de que no conocía que con su actuación iba a causar daño a alguien o que solo quería enviar un mensaje. En la opinión de los legisladores estadounidenses, la nueva ley no está relacionada con el problema de los virus informáticos, específicamente no hay virus que describan el acto para dar cabida en un futuro a la nueva era de ataques tecnológicos a los sistemas informáticos, en cualquier forma en que se realicen.

Diferenciando los niveles de delitos, la nueva ley del lugar que se contemple, que se debe entender como acto delictivo.

En el Estado de California, en 1992 se adoptó la Ley de Privacidad en la que se contemplaba el delito informático pero en menor grado que los delitos relacionados con la intimidad que constituyen el objetivo principal de esta Ley. Se considera importante destacar las enmiendas realizadas a la Sección 502 del Código Penal a los delitos informáticos en la que, entre otros, se amplían los sujetos susceptibles de ser afectados por estos delitos, la creación de sanciones pecuniarias de $ 10, 000 por cada persona afectado y hasta $ 50,000 el acceso imprudente a una base de datos, etcétera.

El objetivo de los legisladores al realizar estas enmiendas, según se infiere, era la posibilidad de aumentar la protección a los individuos, negocios y agencias gubernamentales de la interferencia, daño y acceso no autorizado a las bases de datos y sistemas computarizados creados legalmente. Asimismo, los legisladores consideran que la proliferación de la tecnología de las computadoras ha traído consigo la expansión de delitos informáticos y otras formas no autorizadas de acceso a los ordenadores, sistemas y las bases de datos y que la protección jurídica de todos sus tipos y formas es vital para la seguridad de la intimidad de los individuos así como para el bienestar de las instituciones financieras, de negocios, agencias gubernamentales y otras relacionadas con el estado de California que legalmente usa esas computadoras, sistemas y bases de datos.

Es importante mencionar que en uno de los departamentos de esta ley, se contempla la regulación de los virus (computadora contaminante) conceptualizándolos aunque no los límites a un grupo de instrucciones informáticas populares llamados “virus o gusanos” sino que se contempla a otras las instrucciones designadas a contaminar a otros grupos de programas o bases de datos, modificar, destruir, copiar o transmitir datos o alterar la operación normal de las computadoras, los sistemas o las redes informáticas.

c) Modelo de Francia

Ley número 88-19 de 5 de enero de 1988 sobre el fraude informático. O Acceso fraudulento a un sistema de elaboración de datos (462-2).

En este artículo se incluye tanto el acceso al sistema como el que permite mantener y aumentar la sanción correspondiente de ese acceso, la supresión o modificación de los datos contenidos en el sistema o resultante de la alteración del funcionamiento del sistema.

- Sabotaje informático (462-3).- En este artículo se sanciona a quien impida o falsee el funcionamiento de un sistema de tratamiento automático de datos.

- Destrucción de datos (462-4).- En este artículo se sanciona a quien intencionadamente y con menosprecio de los derechos de los datos ingrese en un sistema de tratamiento automático de datos o suprima o modifique los datos que este contiene o los modos de tratamiento o de transmisión.

- Falsificación de documentos informatizados (462-5).- En este artículo se sanciona a alguien por cualquier modo falsificado documentos informatizados con intención de causar un perjuicio a otro.

- Uso de documentos informatizados falsos (462 - 6). En este artículo se sanciona a quien conscientemente haga uso de documentos falsos tomando como referencia al artículo 462-5.

d) Modelo de Austria

Ley sobre la reforma del Código Penal de 22 de diciembre de 1987

Esta ley establece los siguientes crímenes:

- Destrucción de datos (126). Este artículo no sólo regula los datos programas personales, pero también no personales y Estafa informática (148).

Este artículo castiga a los que pretenden causar una pérdida financiera a un tercero en influir en el resultado de un procesamiento de datos automático gracias a la preparación del programa, la introducción, cancelación o modificación de datos o actuar en el curso procesamiento de datos. También incluye sanciones para aquellos que ellos cometen este hecho con su profesión.

e) Modelo de Chile

En junio de 1993, la Ley del Cibercrimen

Ley No. 19223 Su propósito es proteger una nueva propiedad tal como es: "la calidad, pureza e idoneidad de la información con respecto a tal, contenido en un sistema de procesamiento automatizado del mismo y el producto obtenido de una operación que se tenga".

La Ley No. 19223, es una ley especial, código adicional y consta de 4 artículos:

> *Artículo 1. "Que maliciosamente destruye o deshabilita un sistema de Procesamiento de información o partes o componentes, impida, u obstaculice o modifique su funcionamiento, sufrirá la pena de Presidio menor en grado medio máximo. Si como resultado de estos comportamientos, los datos se vieron afectados Contenido en el sistema, se aplicará la penalización indicada en la subsección anterior, en su grado máximo".*
>
> *Artículo 2. "Con la intención de apoderarse, usar o conocer indebidamente la información contenida en un sistema de tratamiento de la misma, lo intercepte, interfiera o acceda a él, será punible con una pena mínima de prisión de mínimo a mediano".*
>
> *Artículo 3. "El que con malicia altere, dañe o destruya los datos contenidos en un sistema de procesamiento de información será castigado con una pena de prisión menor en un grado medio"*
>
> *Artículo 4. "El que maliciosamente revela o disemina los datos contenidos en un sistema de información será sentenciado a prisión menor en su grado promedio si el que se involucra en estos comportamientos es el responsable del sistema de información, la pena se incrementará una grado. "*

La Ley 19223 prevé delitos informáticos de sabotaje y espionaje informático, pero no de manera clara. Entonces, en el Artículo 1, el primer párrafo se refiere al daño que puede ser hardware, ya sea destruyéndolas o inutilizando, por lo que no sería crimen informático, sino más bien un delito convencional. Está en el artículo 3 es donde encontraríamos la figura del

sabotaje informático en castigar cualquier persona que manipuló, dañó o destruyó los datos contenidos en un sistema.

En conclusión, podemos decir que las deficiencias la ley chilena sobre la regulación de delitos informáticos, no cabe señalar que la Ley N ° 19223 es la pionera de la región abordar expresamente el tema de los delitos informáticos.

f) Modelo de España:

En España, el tratamiento otorgado a este tema se aborda en el nuevo Código penal de 1995 aprobado por la Ley Orgánica 10/1995 de 23 de noviembre y publicado en BOE No 281 de 24 de noviembre de 1995.

El Código Penal actual incorpora delitos comunes la realidad en una forma global (informática), no se limita a la regulación de crímenes sólo informáticos con más conocimiento de la doctrina y otra legislación.

Pero a pesar de las críticas que se pueden hacer de este cuerpo normativo, es sin duda su intento de conseguir la armonía jurídica entre las figuras clásicas sanciones y el fenómeno de la computadora, que requiere un gran esfuerzo, Entonces la solución adoptada por otros sistemas legales, que se limitaron a lidiar con el problema a través de leyes especiales, que considerar el fenómeno de la computadora aislada del resto de la legislación, de una buena técnica jurídica, como en el caso de Chile.

g) Modelo de Holanda

El 1 de marzo de 1993, entró en vigencia la Ley de Delitos Informáticos, que penaliza el hacking y preancking (uso de servicios de telecomunicaciones que evitan el pago total o parcial de dicho servicio), ingeniería social (el arte de convencer a las personas para que proporcionen información que, en circunstancias normales, no cumpliría), y la distribución de virus.

h) En el caso de Reino Unido, Gran Bretaña e Irlanda del norte

En 1991, la Ley de Computer Misuse act, Ley de Abuso informático, comenzó a prevalecer.

Gracias a esta ley, el intento de alterar o no los datos de la computadora se castigan con cinco años de prisión o multas. También penaliza la modificación de datos sin permiso cuando se incluyen virus (Rodríguez, 2009, p.45).

i) Organización de Estados Americanos.

Internet, las redes y tecnologías relacionadas se han convertido en herramientas esenciales para los Estados Miembros de la OEA. Internet ha impulsado el crecimiento de la economía mundial y ha aumentado eficiencia, productividad y creatividad en todo el hemisferio.

Los individuos, las empresas y los gobiernos utilizan cada vez más las redes de información integral de Internet para hacer negocios; organizar y planificar actividades personales, comercio y gobierno; transmitir comunicaciones; y realizar investigaciones y también en la Tercera Cumbre de las Américas, Quebec, Canadá, en 2001, nuestros líderes se comprometieron a Mayor conectividad en las Américas.

La estrategia general de seguridad informática interamericana se basa en los esfuerzos y la experiencia de la Comisión Interamericana contra el terrorismo (CICTE), la Comisión Interamericana de Telecomunicaciones (Citel) y la reunión de ministros de justicia o ministros o Procuradores Generales de las Américas (REMJA). La estrategia reconoce el necesidad de todos los participantes en redes y sistemas de información estar al tanto de sus roles y responsabilidades con respecto a seguridad para crear una cultura de seguridad informática.

La estrategia también reconoce que un marco de protección eficaz de redes y sistemas de información que componen Internet y responden Los accidentes y su recuperación dependerá en la misma medida que:

La información se proporciona a los usuarios y operadores ayudarlos a proteger sus computadoras y redes de las amenazas y vulnerabilidad, y para responder a accidentes y recuperarse de ellos.

Se alienta a las asociaciones públicas y privadas a aumentar la educación, la conciencia y trabajar en conjunto, ya que se posera y operara más infraestructuras de información donde las naciones puedan identificar y evaluar estándares técnicos ,mejores prácticas ,para

garantizar la seguridad de la información transmitida por internet y otras redes de comunicación ,para promover la adopción de ellos

Promover la adopción de políticas y leyes sobre delincuencia cibernética que protege a los usuarios, evita, desalienta el mal uso y el uso ilícito de computadoras y redes

1.2.14. Convención de las Naciones Unidas contra Delincuencia organizada transnacional

El crimen organizado se refiere principalmente a la búsqueda de ganancias y puede entenderse en términos de Clausewitzian (2014) "[...] como una continuación de negocio criminal (p.32).

Phil (2013) Profesor Estudios internacionales de seguridad, Universidad de Pittsburgh. ¿Por qué? por lo tanto, al igual que las empresas de ladrillo y mortero se mueven empresas para la World Wide Web que buscan nuevas oportunidades para obtener ganancias, las sociedades criminales hacen lo mismo." (p. 54)

Organizaciones criminales no son los únicos participantes en los mercados ilícitos, pero a menudo, sobre todo, no solo por la "competitividad" adicional que la amenaza de la violencia organizada. Además, las organizaciones criminales tienden a ser excepcionalmente capaces de identificar y explotar oportunidades para nuevos negocios y actividades ilegales. En este contexto, Internet y el crecimiento continuo del comercio electrónico ofrece nuevas y enormes oportunidades (Convenio ONU, delincuencia Organizada, 2015, p.41).

Del mismo modo, debe tenerse en cuenta que el Convenio posibilidad de obtener formación y asistencia de los Estados miembros signatarios sobre la prevención e investigación de tales crímenes, es preciso tener entrenamiento y programas con este fin, para personas responsables del cumplimiento de la ley como jueces, fiscales y policías. También insiste en el uso de técnicas especiales de investigación como monitoreo electrónico. (Convenio ONU, delincuencia Organizada, 2015, p.42).

1.2.15. **Seguridad informática y normativa**

Para prevenir los ataques de cibercrimen ya sean nacionales o transnacionales, deben tener variables importantes estos son:

a) **Seguridad física:** Es aquello que está relacionado con el la protección de la computadora en sí misma, asegura que las personas que lo manejan, tienen permiso, lo da todo indicaciones técnicas para evitar cualquier daño equipo físico en una computadora. (Guzmán, 2010, p.45)

b) **Seguridad de datos:** Este es el que indica los procedimientos necesarios para evitar el acceso no autorizado, permite el control el acceso remoto a la información, en resumen, protege la integridad de los sistemas de datos. (Guzmán, 2010, p.45)

c) **Datos de apoyo y recuperación**: Proporciona ajustes básicos para usar los sistemas de recuperación de datos y soporte de sistemas informáticos. Permite recuperar la información necesaria en el caso sufrir daño o pérdida. (Guzmán, 2010, p.45)

d) **Disponibilidad de recursos:** Este cuarto componente prueba los recursos y datos almacenados en el sistema que deben ser rápidamente accesible por las personas que lo requieren, para permitirles evaluar constantemente los puntos críticos del sistema para que puedan ser corregidos de inmediato. (Guzmán, 2010, p.45)

e) **Política de seguridad:** Conjunto de estándares, criterios y principios básicos que determinan que está relacionado con el uso de los recursos de cualquier organización. (Guzmán, 2010, p.45)

f) **Análisis médico y legal:** El análisis forense aparece como consecuencia de la necesidad de investigar incidentes de seguridad de la información que ocurren en las entidades. Siga la identificación del autor y la razón del ataque. Además, trate de encontrar una forma de evitar ataques similares en el futuro y obtener pruebas especializadas, (Guzmán, 2010, p.45)

g) **Seguridad normativa:** Principios de legalidad y seguridad jurídica, hace referencia a las normas jurídicas necesarias para prevención y supresión de posibles comportamientos que pueden ir en contra integridad y seguridad de los sistemas de información. (Guzmán, 2010, p.45)

1.2.16. Marco conceptual

> Se entiende por marco conceptual al dominio que tiene una persona sobre conceptos con el tema que está investigando, al compilado de expresiones con carácter de exactitud y concisión, de modo que el conjunto de estos nos manifieste un significado que apoye a la comprensión del tema planteado. (Carrasco, 2007, p.151)

a) Sistema informático:

Todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, cuya función o la de alguno de sus elementos, sea el tratamiento automatizado de datos en ejecución de un programa (El Peruano, 2013.p.3)

b) Datos informáticos:

Toda representación de hechos, información o conceptos expresados de cualquier forma que se preste a tratamiento informático, incluidos los programas diseñados para que un sistema informático ejecute una función. (El Peruano, 2013.p.3)

c) Convenio o tratado internacional:

Acuerdo entre Estados u organizaciones internacionales, regido por el derecho internacional, con la finalidad de establecer normas de relación o de resolver problemas concretos. (RAE, 2018, p.1)

d) Funcionario público:

Persona que desempeña profesionalmente un empleo público /empleado jerárquico, particularmente estatal. (RAE, 2018, p.1)

e) Ciberdelincuencia:

Es toda acción antijurídica, típica y culpable que se realiza con el objetivo de destruir y dañar computadoras y redes por vías informáticas. (Journal, 2015, p.6)

f) Delitos informáticos:

Actos dirigidos contra la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, así como el abuso de dichos sistemas, redes y datos.

1.3. FORMULACIÓN DEL PROBLEMA

El enfoque cualitativo utiliza la recolección de datos sin necesidad de requerir una medición numérica para realizar preguntas de investigación en el proceso de interpretación. (Sampieri, 2014, P.14)

1.3.1. Problema General

¿Cuáles son los factores principales que impiden la aplicación de la Ley N° 30171 en el sector Lima Norte en el año 2016?

1.3.2. Problema Especifico 1

¿Porque la falta de capacitación de los magistrados, fiscales y PNP, es un factor principal que impide la aplicación de la ley N° 30171 en el sector Lima Norte en el año 2016?

1.3.3. Problema Específico 2

¿Porque la falta de adhesión al convenio de Budapest es un factor principal que impide la aplicación de la ley N° 30171 en el sector Lima Norte en el año 2016?

1.4. JUSTIFICACIÓN DEL ESTUDIO

Sampieri (2003) menciona que:

> Las investigaciones se efectúan con un propósito definido y no se hacen simplemente por el capricho de una persona y ese propósito debe ser lo suficientemente fuerte para que se justifique su realización. Es por ello que la justificación de una investigación debe explicar porque es conveniente realizarlo y que beneficios derivaran de ella (p.45)

1.4.1. Justificación Teórica

El presente trabajo de investigación tendrá como base teórica, el ordenamiento nacional respecto a los delitos informáticos, el contexto del Convenio Internacional de Ciberdelincuencia, también llamado convenio de Budapest y demás normas complementarias, así como por la doctrina y jurisprudencia respecto al tema de investigación

1.4.2. Justificación Metodológica

La investigación será en una metodología cualitativa ya que se basara en las vivencias del día a día desde la perspectiva de los especialistas en el tema, se aplicará con un alcance descriptivo-explicativo utilizando el diseño no experimental.

1.4.3. Justificación Práctica

Para Moreno (2013) menciona que:

> "La justificación práctica indica la aplicabilidad de la investigación, su proyección de la sociedad, quienes serán beneficiados de esta investigación, ya sea un grupo social o una organización. Otros autores además sostienen que la investigación practica ayuda a resolver un problema o poner estrategias que contribuirían a resolverlo, es decir porque es conveniente llevar a cabo la investigación y que beneficios traería" (p.28)

El presente trabajo de investigación tiene relevancia social ya que el problema materia de estudio respecto a los delitos informáticos es existente en nuestra sociedad, entendida como una cuestión presente y latente en nuestro entorno ya que según la DIVINDAT al año ya ha existido más de 2,500 casos reportados sobre estos delitos y que sobre todo la mayor incidencia se ha dado a empresarios y pequeños empresarios, con esta investigación se busca lograr determinar qué es lo que está impidiendo que muchas veces este delito quede impune y que los autores sigan cometiendo este ilícito sin ninguna restricción.

1.5. SUPUESTOS Y OBJETIVOS

1.5.1. Objetivos

Para Behar (2008) "El objetivo de la investigación es aspirar al propósito del cual se desarrolla la investigación. A partir del problema de investigación el investigador planteara el resultado que se espera lograr como consecuencia de un mejor conocimiento" (p.34)

a) Objetivo General

Analizar cuáles son los factores principales que impiden la aplicación de la Ley N° 30171 en el sector Lima Norte en el año 2016.

b) Objetivo Especifico 1

Determinar si la falta de capacitación de los magistrados, fiscales y PNP, es un factor principal que impide la aplicación de la ley N° 30171 en el sector Lima Norte en el año 2016.

c) Objetivo Especifico 2

Determinar si la falta de adhesión al convenio de Budapest es un factor principal que impide la aplicación de la ley N° 30171 en el sector Lima Norte en el año 2016.

1.5.2. Supuestos Jurídicos

a) Supuesto Jurídico General

Los factores principales que impidieron la correcta aplicación de la Ley N° 30171 en el sector Lima Norte, fueron: La falta de capacitación a los magistrados, fiscales y PNP, respecto a los delitos informáticos y la falta de adhesión al convenio de Budapest en el sector Lima Norte en el año 2016.

b) Supuesto Jurídico Especifico 1

La falta de capacitación de los magistrados, fiscales Y PNP respecto a los delitos informáticos, es un factor principal que impidió la correcta aplicación de la ley N°30171 en el sector Lima Norte en el año 2016

c) Supuesto Jurídico Especifico 2

La falta de adhesión al convenio de Budapest es un factor principal que impidió la correcta aplicación de la ley N° 30171 en el sector Lima Norte en el año 2016

1.5.3. Relevancia

La presente investigación tendrá relevancia social en que el tema de estudio con relación a los delitos informáticos contemplados en la Ley N°30171, modificatoria de la Ley 30096, es

un tema de interés actual y de gran relevancia dentro de la sociedad donde vivimos ,debido a que la tecnología como tal es parte de la vida cotidiana de todo ciudadano y los problemas que estos que pueden llegar causar deben ser tratados con carácter de urgencia como los son: Robo de data, Pornografía infantil, clonación de tarjetas entre otros

1.5.4. Contribución

Esta investigación contribuye analizar si los delitos informáticos tienen una gran repercusión dentro de la ciudadanía como tal y si las leyes que existen son suficientes para poder regularlas y sancionar a los actores de dichos delitos.

.

II. MÉTODO

2.1. DISEÑO DE INVESTIGACIÓN

El presente trabajo de investigación utiliza como tipo de estudio la comprensión de la realidad problemática, es por ello que será cualitativo, ya que se observara y explicara la problemática de este trabajo entorno a los factores que impidieron la aplicación de la Ley Nº 30171.

2.1.1. Cualitativa:

El investigador cualitativo empieza con la idea de que el mundo social es "relativo" y por ello solo puede verse desde la vista de los actores estudiados. Mejor entendido como el mundo lo construye el investigador. (Sampieri, 2015, p.7)

2.1.2. Descriptivo:

Consiste en la investigación de hechos, caos y fenómenos. Que se sitúa en el presente, pero no únicamente se limita a la simple recopilación y la tabulación de datos, sino que hace la deducción y la observación ecuánime de los mismos. (Lara, 2014, p. 129)

De la misma manera como indican Hernández, Fernández y Baptista (2007): "Los estudios descriptivos buscan especificar las propiedades, las características y los perfiles importantes de personas, grupos, comunidades o cualquier otro fenómeno que se someta a un análisis". (p. 60)

Teniendo en cuenta estas dos definiciones, podemos señalar que es la capacidad por la cual se va determinar las características del objeto de estudio y realizar una descripción de las partes del objeto de estudio.

Respecto al tema para Hernández (1999) "El diseño metodológico señala al investigador lo que debe hacer para alcanzar sus objetivos de estudio, contestar las interrogantes que se han planteado y analizar el supuesto formulado en un contexto en particular" (p.24)

Esto quiere decir que van a utilizar las habilidades correctas para dar una respuesta certera al planteamiento del problema verificando y estableciendo los supuestos que se han realizado.

Orbegoso (2008) Indica que la denominada investigación básica carece de propósitos aplicativos, raudoz o dinámicos sino que a diferencia de otras investigaciones busca profundizar los conocimientos científicos en la realidad (p.54)

Conforme al nivel de competencia científica esta investigación es básica porque está orientada para producir nuevos conocimientos y reflexionar la información en la sociedad, pues lo que se persigue en ese estudio es socavar conocimientos y exponer cuales son los factores principales que impiden la correcta aplicación de la Ley N°30171.

Este trabajo de investigación utilizara la teoría fundamentada debido a que con esta se describe, interpreta y se puede realizar entrevistas, logrando explicar con amplitud el fenómeno del estudio.

Figueroa (2006) la teoría fundamentada se remonta en la argumentación conduce una forma sistemática, y cualitativa para producir una teoría, que con ella compruebe un nivel conceptual de hecho, una interacción o un campo particular (p.42).

2.1.3. Caracterización de sujetos

Benites (2005) Es el momento de la investigación radica en la esencia de la explicación que se le efectúa a los implicados en la averiguación de información (p.45).

Está representada por las personas que ayudarán con la búsqueda de la información relacionada a la investigación los mismos que serán parte de las entrevistas, como parte fundamental del desarrollo de esta investigación, la opinión de los sujetos que intervendrán serán necesariamente colegiados especialistas en lo penal cuyo amplio conocimiento se ve incuestionable por ser de práctica diaria, los que observan el problema.

Tabla 01. Caracterización de Sujetos

N°	Apellidos y Nombres	Profesión	Experiencia	Cargo
1.	Acosta Ruiz, Ana Isabel	Abogada	Abogada del ministerio del interior, abogada del ministerio público	Abogada coordinadora de la procuraduría publica especializada en delitos de terrorismo

			procuradora anti terrorismo	del Ministerio del Interior
2.	Escobar Pérez Cesar	Abogado	Docente en la universidad mayor de san marcos , abogado asesor en el estudio Nagasaki,	Docente de la Universidad Cesar Vallejo
3.	Francia Aburto, Jacinto	Abogado	Asesor legal de empresas de softwares y antivirus, jefe del área legal y sistemas de Aillus	Jefe del área legal de la empresa NUMAY.SAC
4.	Minaya Gamarra, Martin	Asesor en Sistemas	Ingeniero en sistemas en consultorías de desarrollo de software, asesor en sistemas en el Estudio Lescano	Asesor en sistemas en el Estudio Lescano
5.	Sulca Pizarro, Alberto Fidel	Abogado	Abogada de D&f abogados	Abogada de D&f abogados
6.	Robles Sotelo, Marcos	Abogado	Asesor penal y consultor de empresas	Abogado independiente

7.	Román de la Puente, Oscar	PNP, de la Drincri. DIVINDAT	Efectivo encargado de la recepción de denuncias del ámbito informático	Efectivo en servicio de la DIVINDAT
8.	Salazar Leyton, Elmer	Abogado	Asistente legal en la procuraría del Ministerio Publico, Licenciado de la Universidad Inca Garcilaso de la Vega	Abogado en estudio Jurídico
9.	Sánchez Guerrero, Hernán	Técnico en la Fuerzas Armadas, PNP, de la Dirincri. DIVINDAT	Efectivo	Efectivo en servicio de la DIVINDAT
10.	Urbina Zambrano Oscar	Abogado	Abogado del Estudio D&f abogados	Abogado de D&f abogados

Fuente: Propia

2.2. METODOS DE MUESTREO

2.2.1. Población y Muestra

a) Población:

Según Tamayo (2011) señala que "La población es la totalidad de un fenómeno de estudio que incluye las unidades de análisis que se integran a dicho fenómeno y que deben cuantificarse para un determinado estudio en donde participan con una determinada

característica, se podría decir que la población es aquella que constituye la totalidad del fenómeno" (p.46)

Por lo anterior mencionado la población de la presente investigación será el sector de Lima Norte.

a) Muestra:

Para Sampieri (2015) "En el proceso cualitativo la muestra es un grupo de personas, eventos, sucesos comunidades, etc. Sobre los cuales se recolectaran datos, sin que sea necesario representativo la población que se estudia" (p.35).

Es por ello que en esta investigación tomare como muestra a los Conocedores y/o especialista sobre los Delitos Informáticos, tales como colegiados especialistas y agentes de la DIVINDAT

2.3. RIGOR CIENTIFICO

El rigor científico en esta oportunidad se dará definiendo los instrumentos que se utilizaron en la investigación.

2.3.1. Entrevista:

Para Peláez (2008) "es un procedimiento de intercomunicación que se efectúa de manera normal entre dos personas, en este procedimiento, el entrevistador adquiere información del entrevistado de manera directa" (p.76).

Según López (2004) menciona:

> La entrevista es una forma específica de interacción social que tiene por objeto recolectar datos para una indagación. El investigador formula preguntas a las personas capaces de apórtale datos de interés, estableciendo un dialogo, donde una de las partes busca recoger informaciones y la otra es la fuente de esa información (p.32).

Además como menciona Ramos (2004)

> "La entrevista se hace a una persona pero se habla de un tema en específico, se elige a esta persona ya sea por ser profesional en el tema o por ser parte de la investigación, o por tener un fin marcado sobre la misma, lo que se busca es la

verdad sobre un hecho, situación o persona, es por ello que usualmente el tipo de pregunta en una entrevista es abierta" (p.54).

a) Guía de Entrevista

Según Silva (2015) "es una ayuda de memoria para el entrevistador, tanto en un sentido temático (ayuda a recordar los temas de la entrevista) como conceptual (presenta los tópicos de la entrevista en un lenguaje cotidiano, propio de las personas entrevistadas)" (p.45)

Dentro de la Técnica de entrevista se utilizara como instrumento a la Guía de entrevista anteriormente mencionada.

2.3.2. Análisis documental.

Según Gutiérrez (2006) "El análisis documental representa la información de un documento en un registro estructurado, reduce todos los datos descriptivos físicos y de contenido en un esquema inequívoco" (p.87).

a) Guía de Análisis Normativo

Melendez (2010) "Es una descripción de la norma acompañada de una interpretación por parte del investigador, sustentada en conocimientos jurídicos para su comprensión" (p.54).

En el presente trabajo de investigación esta guía de análisis normativo será utilizada como instrumento de la técnica del Análisis Documental.

2.3.3. Validez de los instrumentos de recolección de datos

La validez de la presente investigación está basada en las técnicas e instrumentos utilizados, como las entrevistas a los especialistas y la recolección de la información a través de los análisis de los documentos, donde se logrará fundamentar las soluciones propuestas en la aproximación problemática.

Tabla. 02. Validación

Nº	**Nombres y Apellidos del Validador**	**Especialidad**	**Cargo**	**Instrumento**

1	Esaú Vargas Huamán	Temático	Docente de la UCV- Lima Norte	Guía de Instrumento Nº 01
2	Luca Aceto	Temático	Docente de la UCV- Lima Norte	Guía de Instrumento Nº 01
3	Fabricio Marvilla Fraga de Mezquita	Temático	Docente de la UCV- Lima Norte	Guía de Instrumento Nº 01

Fuente: propia

Confiabilidad

Es la capacidad del mismo instrumento para producir resultados congruentes cuando se aplica por segunda vez en condiciones tan parecida como sea posible.

2.3.4. Análisis cualitativo de los datos

Para llevar a cabo la determinación de los datos a lo largo del proceso de investigación es necesario utilizar los instrumentos seleccionados, preparar el análisis de datos, verificar los documentos y grabaciones utilizados. En consecuencia, se podrá determinar la unidad de análisis adecuada para la investigación.

a) Tratamiento de unidades temáticas de categorización

En una investigación cualitativa se encuentran las denominadas "unidades de análisis'' para categorizar y codificar, por lo que consisten en identificar los contenidos o fragmentos dentro de las entrevistas.

Tabla 03. Unidad de Análisis

Categorías	Definición	Sub categorías
Aplicación de la Ley Nº30171	Álvarez (2003) se determina el derecho aplicable a una determinada vida no por su nacionalidad, sino por las	Capacitación a la PNP, jueces y fiscales. Adhesión al Convenio de Budapest.

	leyes que rigen del estado en que se encuentra. (p.45)	
Ley Nº30171	Es la ley que Modifica los artículos 2, 3,4, 5, 7, 8 y 10 de la Legislación 30096, Ley de Delitos Informáticos,	Delitos Informáticos Elementos del delito La ley Nº30096

Fuente: Propia

2.4.ASPECTOS ETICOS

La presente investigación se realiza respetando el método científico siendo de enfoque cualitativo, respetando las normas establecidas por la Universidad y siguiendo las indicaciones del asesor metodológico.

De igual manera la presente investigación se realizara respetando los derechos de autor en concordancia con lo previsto por la Ley sobre el derecho de autor Decreto Legislativo N° 822, citando en las referencias bibliográficas el estilo APA (AMERICAN PSYCOLOGICAL ASSOCIATION).

III. DESCRIPCION DE RESULTADOS

En este capítulo de esta investigación se expondrá todos los datos recolectados mediante los instrumentos utilizados, tales son la entrevista y el análisis documental.

Para Asenjo (2006) define a la descripción de resultados como la narración de la información relevante recogida a través de los instrumentos (p.34).

Descripción de los resultados de las entrevistas

Entrevista Nº 01

En la presente prueba después de haber realizado las entrevistas a diez abogados y profesionales de la DIVINDAT especializados en el tema de investigación, se logró obtener los siguientes resultados para alcanzar el objetivo general:

Objetivo General: Analizar cuáles son los factores principales que impiden la aplicación de la Ley N° 30171 en el sector Lima Norte en el año 2016

Pregunta 1: De acuerdo a su experiencia ¿Considera Usted que existan factores que impidan la aplicación de la Ley N°30171, "Ley de delitos informáticos" en el sector Lima Norte? De existir esos factores ¿Cuáles considera Usted que serían?

Francia (2018) manifestó lo siguiente:

La Ley es muy amplia y genérica, tiene que capacitarse a los jueces, fiscales, abogados y a todos los que intervengan en estos casos recuerdo que la misma policía no está capacitada para detectar a los que roban mediante tarjetas de consumo.

Acosta (2018) respondió lo siguiente:

> En mi opinión si considero que existen factores que no permiten la aplicación de dicha Ley, uno de ellos podemos pensar que es el atraso tecnológico que existe en nuestro país.

Robles (2018) señala que:

> Bajo mi perspectiva yo considero que existen una variedad de factores, como puede ser el mismo pensamiento nacional influenciado por las costumbres, entre otros

Minaya (2018) manifestó lo siguiente:

> Como factor principal requeriría el registro inequívoco del delito (que se pueda probar) y de otra parte que pueda imputarse el autor o autores del mismo, toda vez que se trata de información virtual y que desde el punto de vista informático puede ser fácilmente manipulada.

Escobar (2018) menciona que:

> No, considero que existan factores que impidan la aplicación de la Ley 30171, debido a que toda Ley es de carácter imperativa.

Salazar (2018) menciona que:

> Si, considero que existen factores que impiden la aplicación de la Ley N° 30171, considero que entre los más resaltantes factores es, la falta de capacitación o información a las autoridades encargadas de estos temas.

Urbina (2018) menciona que:

> En efecto siempre es deber del Estado velar por el correcto cumplimiento y evitar factore que obstaculicen su aplicación como la carencia de conocimientos de los funcionarios encargados o de indumentaria necesaria.

Sulca (2018) menciona que:

> Sin duda alguna, si se puede ver diversos factores que dificulten la aplicación de dicha Ley, que pueden ser la falta de conocimiento en todos sus ámbitos (técnico, informático o jurídico) de jueces y fiscales y todos los encargados, asi como también la falta de cooperación internacional.

Sánchez (2018) menciona que:

> Nosotros como ente encargado de perseguir y desarticular crímenes informáticos, podemos mencionar que desde nuestra perspectiva uno de esos

factores viene desde las políticas estatales cursando hasta la poca atención en este ámbito.

Román (2018) menciona que:

> De existir algún factor resaltante es la poca ayuda se brinda a este sector del Ministerio del Interior ya sea en apoyo técnico o de conocimiento procedimental, como legal.

Pregunta 2. ¿Dentro de su consideración, cree usted que es asunto del Estado velar porque se cumpla la aplicación de la Ley N°30171, a pesar de ser una Ley especial? ¿Por qué?

Francia (2018) manifestó lo siguiente:

> Toda Ley es obligación de su aplicación no solo del Estado, es obligación de todos especialmente de los operadores directos.

Acosta (2018) respondió lo siguiente:

> Siempre se va ser una obligación de toda nación o gobierno velar por el cumplimiento de las leyes sea cual sea su naturaleza.

Robles (2018) señala que:

> Es asunto de todo gobierno velar por el cumplimiento de toda Ley o norma sea del tipo que sea, porque como bien sabemos es asunto del Estado todo lo concerniente a protección de derechos y si se ha creado una ley para protegernos ante los delitos informáticos, pues es también deber del Estado velar porque esta se cumpla.

Minaya (2018) manifestó lo siguiente:

> Es asunto del Estado definitivamente, como parte de la protección a los derechos fundamentales de toda persona.

Escobar (2018) menciona que:

> Sí, es asunto del Estado velar porque se cumpla la aplicación de la Ley 30171, ya que el Estado debe hacer respetar y aplicar adecuadamente la Ley para beneficio de la ciudadanía

Salazar (2018) menciona que:

> El tema que abarca en su totalidad al Estado es la de hacer que todas sus legislaciones sean complementarias o no.

Urbina (2018) menciona que:

> El Estado es quien emite las normas por las cuales se rige la sociedad en que vivimos y por lo cual es un escenario absurdo que no asegure el cumplimiento de algo que el mismo ente emite.

Sulca (2018) menciona que:

> Más que asegurar su cumplimiento, es de contar con una buena organización para que de esta forma con la que se realización de cada una de sus funciones, se logre llegar al cumplimiento de la norma.

Sánchez (2018) menciona que:

> Parte de las funciones del Estado aparte de legislar y emitir normas es aseverar el cumplimiento de estas, así como designando entidades que apoyen en dicha misión.

Román (2018) menciona que:

> Como DIVINDAT somos el ente encargado de regular lo concerniente a los delitos informáticos en afán de apoyar en el cumplimiento de la Ley N° 30171 (modificatoria) en favor del Estado y del ciudadano.

Objetivo Especifico 1: Determinar si la falta de capacitación de los magistrados, fiscales y PNP, es un factor principal que impide la aplicación de la ley N° 30171 en el sector Lima Norte en el año 2016.

Pregunta 3. ¿Cree Ud. que el estado debería brindar más alcances e información (charlas, capacitaciones, talleres, etc.) a los magistrados, fiscales y PNP sobre la Ley N° 30171 y la finalidad de esta? ¿Por qué?

Francia (2018) manifestó lo siguiente:

> Si, efectivamente, tiene que haber una capacitación totalmente integral, pero además es necesario un equipo experto en informática, porque los abogados solo estamos preparados en leyes y nada más, el resto de cosas solo podremos conocerlas a grandes rasgos pero en sí, se requiere la ayuda de un experto en informática para la realización de las capacitaciones.

Acosta (2018) respondió lo siguiente:

> Considero que el Estado tiene la obligación de dar todos los alcances necesarios para el cumplimiento de las funciones de las entidades estatales.

Robles (2018) señala que:

> Porque es obligación del Estado ayudar y promover instrumentos que faciliten la impartición de justicia en especial sobre una ley que especifica un tema tan latente, como lo es los delitos informáticos.

Minaya (2018) manifestó lo siguiente:

> Sería deseable en todo caso, aunque desde el punto de vista profesional se entiende que deben de existir o crearse instituciones o departamentos ad. Hoc con agentes especializados.

Escobar (2018) menciona que:

Sí, es necesario la capacitación a los magistrados, fiscales para su conocimiento e instrucción a su personal, para poder manejar de manera eficiente los casos por delitos informáticos.

Salazar (2018) menciona que:

> Siempre es algo positivo reforzar los alacnaces que puedan tener nuestros funcionarios públicos y con mayor razón a quienes manejan temas tan delicados como la lucha contra la ciberdelincuencia.

Urbina (2018) menciona que:

> Es parte de las funciones del Estado renovar y proveer de nuevo y mejores recursos tanto intelectuales en el caso de boletines informáticos, talleres y capacitaciones como en recursos técnicos como los son los materiales de trabajo para darle el tratamiento adecuado para esta modalidad.

Sulca (2018) menciona que:

> El Estado en su afán de querer mejorar la inseguridad que muchas normas provocan debería brindar a los funcionarios encargados mayores alcances para que desempeñen sus funciones de manera más óptima.

Sánchez (2018) menciona que:

> Es bien recibido siempre por parte del Ministerio del Interior todo apoyo sea en forma de capacitación a los efectivos como otras formas de capacitación.

Román (2018) menciona que:

> Consideramos que más que una acción particular vendría a convertirse más, en una actividad habitual del Estado para poder desempeñarnos con mayor efectividad.

Pregunta 4. De lo mencionado anteriormente ¿Considera usted que la falta de información a los magistrados, fiscales y PNP, que debe brindar el estado es un factor determinante que impide la correcta aplicación de la ley N° 30171?

Francia (2018) manifestó lo siguiente:

> Sí, pero también es la inoperancia de no seguir preparándose individualmente.

Acosta (2018) respondió lo siguiente:

> Es imperativo que se le otorgue toda clase de información a los funcionarios públicos que tienen como misión la aplicación de la justicia.

Robles (2018) señala que:

> A criterio personal, la falta de información a las autoridades que se encargan del seguimiento y de la administración del justicia, es un factor determinante, ya que los magistrados son los encargados de hacer cumplir lo que dicta la norma, y el desconocimiento en este asunto impediría la función de igual forma, y de la misma manera sucedería con los demás servidores públicos.

Minaya (2018) manifestó lo siguiente:

> No, la falta de información que el Estado no brinda no determina, toda vez que magistrados, fiscales y la PNP pueden obtener asesoría especializada que garantice la correcta implementación y aplicación de la ley.

Escobar (2018) menciona que:

> Sí, porque no estar informado y/o capacitado puede generar problemas en la aplicación de la Ley, porque se entiende que para poder aplicar algo primero se debe saber de qué trata.

Salazar (2018) menciona que:

> Por este punto, hay que decir, diciendo que para la inaplicación de una norma como ya se ha dicho que hay muchos factores, y en concreto cuando se puede aprender de forma casi imposible, aplicar la ley en su plenitud.

Urbina (2018) menciona que:

> Si bien es correcto, que la ausencia de información de una norma ocasiona que no pueda ser aplicada correctamente, existen otros muchos factores que pueden influenciar en este caso, pero considero que la ausencia de información es el más relevante.

Sulca (2018) menciona que:

> Si, considero que la falta de información a los funcionarios encargados es un factor fundamental para una correcta aplicación de la norma.

Sánchez (2018) menciona que:

> El cuerpo de efectivos de la DIVINDAT, rama de la PNP, se encuentra capacitado y adicionalmente posee y se rige por el código de procedimientos.

Román (2018) menciona que:

> No se discute que con algo más de preparación se puede realizar un mejor rendimiento por parte, no solo de nosotros como DIVINDAT, sino también al Poder Judicial y el Ministerio Público, siendo la falta de esta un factor perjudicial.

Objetivo Especifico 2: Determinar si la falta de adhesión al convenio de Budapest es un factor principal que impide la aplicación de la ley N° 30171 en el sector Lima Norte en el año 2016

Pregunta 5. Dentro de su consideración ¿Cree Ud. que es la falta de adhesión al convenio de Budapest el factor fundamental que impide la aplicación de la ley N° 30171?

Francia (2018) manifestó lo siguiente:

> La ley se puede aplicar con sus defectos, naturalmente en este tipo de casos adecuarse al convenio, debido a que hasta la fecha el Perú, aún no ha ingresado al tan conocido Convenio Internacional de Budapest.

Acosta (2018) respondió lo siguiente:

> Considero que el Estado tiene la obligación de dar todos los alcances necesarios para el cumplimiento de las funciones de las entidades estatales

Robles (2018) señala que:

> De existir ya una tratativa de carácter internacional es de suma importancia nuestra adhesión, debido a que entre nuestras fuentes del derecho se encuentras los tratados internacionales como fuente para regular criterios que se acepten a nuestra realidad.

Minaya (2018) manifestó lo siguiente:

> Ser parte o no de un convenio, no impide la aplicación de la Ley 30171. Sería deseable sí, porque se facilitaría la cooperación internacional e implementación de mecanismos de control y seguimiento a nivel global del delincuente cibernético.

Escobar (2018) menciona que:

> Si, estar adscritos al convenio de Budapest, considero que es un factor que impide la aplicación de la Ley de delitos informáticos, por ello considero que es un factor que impide la aplicación debido a que atrasa la captura al delincuente cibernético, y además es un claro reflejo de que nuestra legislación aun no cumple con los estándares internacionales, para encontrarse dentro de dicho convenio.

Salazar (2018) menciona que:

> Creo que la adhesión al convenio de Budapest lo cambia todo, ya que acarrearía muchas cosas positivas para nuestro sistema y el hecho de que aún no estemos dentro del convenio si es un factor de que algo no anda bien en nuestra legislación.

Urbina (2018) menciona que:

> Tomando en cuenta que un convenio internacional se crea para resolver un problema que afecta a todos, y por ello significa que ese problema lo tienen otros países, y que por sí solos no puede hacer frente, por diferentes motivos, en el cambio si se agrupan para optar medidas que ayuden a dar solución al problema, eso sí podría funcionar, y si el Perú todavía está incluido, es Ahí donde encontramos la falla de una mala ejecución de nuestras normas y sistema siendo este un factor detonante.

Sulca (2018) menciona que:

> Se cuenta actualmente con una normativa que regula la clase de delitos, sin embargo, no está respaldada por un tratado o convenio y al no respaldado por otra forma, se dificulta la aplicación de la ley actual.

Sánchez (2018) menciona que:

> Si, consideramos que la ausencia de la adhesión al convenio de Budapest, es un factor clave en la problemática, es por ello conocemos que hace algún tiempo el Perú, ha estado interesado en la adhesión a este convenio ya que países como argentina, México, Panamá, Costa Rica y Colombia ya se encuentran dentro de dicho convenio.

Román (2018) menciona que:

> En parte podría decirse que es cierto pero más afirmamos que un factor importante es el constante aumento de los crímenes de este tipo.

Pregunta 6. ¿De qué manera influiría a nuestro sistema legal actual la incorporación al convenio de Budapest?

Francia (2018) manifestó lo siguiente:

> Permitiría, ser un bloque homogéneo contra la CIBERDELINCUENCIA, habría una capacitación mayor y muy seria.

Acosta (2018) respondió lo siguiente:

De manera positiva, tanto con la cooperación internacional para la captura del delincuente cibernético como para la seguridad de la información como bien jurídico protegido de los delitos informáticos.

Robles (2018) señala que:

> Influiría de manera positiva en muchos ámbitos tanto en la cooperación internacional como en la capacitación al personal encargado.

Minaya (2018) manifestó lo siguiente:

> La incorporación al convenio debería aportar, pero en realidad no afecta el sistema legal propiamente dicho, toda vez que, ni el estado muestra interés, ni el legislativo está en capacidad, a pesar de haber habido intentos en la incorporación al referido convenio no se ha llegado a concretar nada aun.

Escobar (2018) menciona que:

> No, considero que su incorporación afectaría nuestro sistema legal, sino que se ampliaría.

Salazar (2018) menciona que:

> Si, mejoraría nuestro sistema legal, la manera más evidente de ayuda internacional, entre otras posibilidades.

Urbina (2018) menciona que:

> Influenciar de manera positiva, ya que la razón de la creación de los convenios es para resolver los problemas que los países solos no pueden.

Sulca (2018) menciona que:

> La infracción que es notable y que el crecimiento delincuencial, va en aumento.

Sánchez (2018) menciona que:

> Dentro del ámbito de la DIVINDACIÓN puede obtenerse un conjunto de medidas para evitar el incumplimiento de las normas y otras negativas como la falta de auxilio de otras naciones para el Perú.

Román (2018) menciona que:

> Nunca se ha llegado al Perú a adherirse en ese sentido, los delitos informáticos son temas que para su sustentación de la investigación son informes de carácter técnico puro, por lo que se requiere de especialistas en este ámbito y estar capacitando para que interpreten bien el informe técnico.

Pregunta 7. Finalmente, ¿Considera Ud. que el convenio de Budapest ayudaría cumplir la finalidad por la que se creó en primer momento la ley N° 30171? ¿Porque?

Francia (2018) manifestó lo siguiente:

> Si ayudaría, porque se conduciría a buscar como siempre el equilibrio en las acciones penales y los derechos humanos que nos asisten.

Acosta (2018) respondió lo siguiente:

> Considero que si ayudaría a cumplir, ya que es una norma de carácter internacional especializada en dicho tema.

Robles (2018) señala que:

> Definitivamente si, ayudaría debido a que es una suma de todos los esfuerzos de la comunidad internacional.

Minaya (2018) manifestó lo siguiente:

> Claro que sí, porque se implementaría la Ley de modo correcto con acceso a informática forense (lo que en nuestro país dudo mucho que exista).

Escobar (2018) menciona que:

> No, considero que el convenio de Budapest se creó para países en los que la legislación respecto a este tema ha sido trata a lo largo de varios años y que ha existido un alto índice de este tipo de delitos, pero en el Perú, el tema de delitos informáticos es muy nuevo.

Salazar (2018) menciona que:

> Si, ayudaría porque al tener de nuestro lado a países especializados en este tema, tendríamos una mayor posibilidad de poder capturar a los ciberdelincuentes y que el número de delitos cometidos en este tema sea menor.

Urbina (2018) menciona que:

> Claro que sí, debido a que la finalidad del convenio de ciberdelincuencia, es ayudar a combatir los delitos informáticos y esto ayudaría muchísimo a reducir los ataques cibernéticos.

Sulca (2018) menciona que:

> Si ayudaría, porque los delitos informáticos como bien es sabido, recién empezó a tratarse en el año 2013 con una legislación que dejaba muchos cabos sueltos, siendo asi que tuvo que ser modificada nuevamente en el año 2014 tratando de que los delitos informáticos se encuentren bien definidos y saber cuáles son y que sanción tendrá, el convenio de Budapest, ayudaría bastante en la comprensión de este tema.

Sánchez (2018) menciona que:

> La DIVINDAT se ha encargado de perseguir estos tipos de delitos desde nuestra creación, hemos brindado información respecto a cómo no ser víctima de los delitos informáticos, pero aun así existe un alto número de personas que han sido víctimas de clonación de tarjetas, robo de data a empresas entre otros, por ello consideramos que si se llegara a abrir la puerta para estar dentro del convenio de Budapest, ayudaría en la mejor difusión de este tema.

Román (2018) menciona que:

> Toda ayuda es importante en el combate contra la ciberdelincuencia, el procedimiento de investigación policial es muy engorroso porque se tiene que acoger a normas existentes, nuestro país no colabora con la investigación policial y producen retardo, por ejemplo para un caso de extorsion tenemos que esperar dos o tres semanas para que salga una orden judicial que permita dar la información, cuando eso debería ser al momento, hemos tratado de concientizar a los entes que dentro de su jurisdicción tienen la facultad para poder acelerar este proceso, pero se excusan diciendo que la policía puede hacer mal uso de la información.

Análisis documental

Título: "Los factores principales que impiden la aplicación de la Ley N°30171- Lima Norte en el año 2016"

Objetivo General: Analizar cuáles son los factores principales que impiden la aplicación de la Ley N° 30171 en el sector Lima Norte en el año 2016

La ley Nº 30171, aprobada el 10 de Marzo del año 2014, en su Cuarta Disposición Complementaria Final

Señala lo siguiente, respecto a la aplicación de la Ley 30171:

> "La Cooperación Operativa se da con el objeto de garantizar el intercambio de información, los equipos de investigación, la transmisión de documentos, la interceptación, de comunicaciones y demás actividades correspondientes para dar efectividad a la presente Ley, la Policía Nacional del Perú, el Ministerio Publico, el Poder Judicial, el PERCERT (Centro de respuesta temprana del gobierno para ataques cibernéticos), la ONGEI (Oficina Nacional de Gobierno para ataques cibernético) Organismos especializados de las Fuerzas Armadas y los operadores del sector privado involucrados en la lucha contra los delitos informáticos deben establecer protocolos de cooperación operativa reformada en el plazo de 30 días desde la vigencia de la presente Ley".

Interpretación

La cuarta Disposición Complementaria de la Ley 30171, menciona que para la Cooperación Operativa contra los delitos informáticos debería lograr una efectividad para aplicar la Ley 30171, y se solicita la ayuda de la Policía Nacional del Perú, el Ministerio Publico, el Poder Judicial, el PERCET, las Fuerzas Armadas y operadores del sector privado, pero en ninguna parte de dicha disposición menciona que medidas se deben tomar para la intercomunicación rápida entre estas entidades, solo se acota el término "deben establecer protocolos de cooperación operativa reformada en el plazo de 30 días".

Objetivo Especifico 1: si la falta de capacitación de los magistrados, fiscales y PNP, es un factor principal que impide la aplicación de la ley N° 30171 en el sector Lima Norte en el año 2016

12º Congreso de las Naciones Unidas sobre Delitos Informáticos

Respecto de la capacitación a jueces, fiscales y policías menciona que:

> "Del mismo modo, debe tenerse en cuenta que el Convenio de Budapest, es como la posibilidad de obtener formación y asistencia de los Estados miembros signatarios sobre la prevención e investigación de tales crímenes y presiones tener entrenamiento y programas de entrenamiento para personas responsables del cumplimiento de la ley como jueces, fiscales y policías. También insiste en el uso de técnicas especiales de investigación como monitoreo electrónico".

Interpretación:

Aquí podemos observar cómo es que la misma ONU nos menciona sobre las ventajas que tiene el hecho de adjuntarse al convenio como son la posibilidad de obtener formación y asistencia de los Estados miembros signatarios sobre la prevención e investigación de tales crímenes y presiones tener entrenamiento y programas de entrenamiento para personas responsables del cumplimiento de la ley como jueces, fiscales y policías , entre otros tantos beneficios que consta el hecho de unirse a dicha iniciativa internacional.

Quinta Disposición Complementaria Final no derogado, de la Ley N° 30096 "Ley de delitos Informáticos", publicada en el año 2013

Las instituciones públicas involucradas en la prevención y represión de los delitos informáticos deben impartir cursos de capacitación destinados a optimizar la formación profesional de su personal -especialmente de la Policía Nacional del Perú, el Ministerio Público y el Poder Judicial- en el procedimiento de los delitos previstos en la presente Ley.

Interpretación

Esta disposición complementaria final menciona que las instituciones públicas conocedoras de los delitos informáticos deben impartir cursos de capacitación para educar al personal de la PNP, el Ministerio Publico y el Poder Judicial, respecto del tratamiento de estos delitos ya mencionados.

Objetivo Especifico 2: Determinar si la falta de adhesión al convenio de Budapest es un factor principal que impide la aplicación de la ley N° 30171 en el sector Lima Norte en el año 2016

El proyecto de Dictamen Nº2807-2017, presentado por el Poder Ejecutivo donde se propone la aprobación del "Convenio de Ciberdelincuencia" en la ciudad de Budapest

Señala lo siguiente respecto a la adhesión a este convenio:

> **"**Es importante y necesaria la adhesión del Perú al convenio de Budapest , ya que ayudaría a prevenir los actos que pongan en peligro la confidencialidad ,la integridad, y la disponibilidad de los sistemas ,redes y datos informáticos, garantiza la tipificación del delito ,facilita su detección , investigación y sanción , en el ámbito nacional e internacional ,así como , la cooperación judicial internacional"

Interpretación:

Aquí el poder legislativo por medio de la comisión de relaciones exteriores nos habla porque sería la decisión más óptima, el adherirnos al convenio de Budapest debido a que ayudaría a

prevenir los actos que pongan en peligro la confidencialidad ,la integridad, y la disponibilidad de los sistemas ,redes y datos informáticos, garantiza la tipificación del delito ,facilita su detección , investigación y sanción , en el ámbito nacional e internacional ,así como , la cooperación judicial internacional, entre otras ventajas que dicho acuerdo de la comunidad internacional otorga, recalca adicionalmente la importancia de que le Perú forme parte de la ya mencionada dando así solución a muchos problemas de nuestra legislación en este tema.

IV. DISCUSION

A continuación se pasara a realizar la discusión de los resultados, tal como se sabe mediante el método de análisis de datos discutiendo los trabajos previos de esta investigación, así como también contrastando con todos los resultados obtenidos gracias a los instrumentos de recolección de datos utilizados, teniendo por ultimo una discusión desde mi posición personal para conocer que se han logrado alcanzar con los objetivos trazados en esta tesis.

Objetivo General: Analizar cuáles son los factores principales que impiden la aplicación de la Ley N° 30171 en el sector Lima Norte en el año 2016

Supuesto General: Los factores principales que impidieron la correcta aplicación de la Ley N° 30171 en el sector Lima Norte, fueron: La falta de capacitación a los magistrados, fiscales y PNP, respecto a los delitos informáticos y la falta de adhesión al convenio de Budapest en el sector Lima Norte en el año 2016

1. Francia, Acosta y Robles (2018), manifiestan lo siguiente:

La Ley es muy amplia y genérica, tiene que capacitarse a los jueces, fiscales, abogados y a todos los que intervengan en estos casos, la misma policía no está capacitada para detectar a los que roban mediante tarjetas de consumo. Existen factores que no permiten la aplicación de dicha Ley, uno de ellos podemos pensar que es el atraso tecnológico que existe en nuestro país. Pero también hay una gran variedad de factores, como puede ser el mismo pensamiento nacional influenciado por las costumbres, entre otros.

2. Minaya, Salazar, Urbina (2018), manifiestan lo siguiente:

Como factor principal requeriría el registro inequívoco del delito (es decir que se pueda probar) y de otra parte que pueda imputarse el autor o autores del mismo, toda vez que se trata de información virtual y que desde el punto de vista informático puede ser fácilmente manipulada. Por ello de existir factores que impiden la aplicación de la Ley N° 30171, considero que entre los más resaltantes factores seria la falta de capacitación o información a las autoridades encargadas de estos temas, además cabe señalar que siempre es deber del Estado velar por el correcto cumplimiento y evitar que se obstaculicen la aplicación por factores como: la carencia de conocimientos de los funcionarios encargados o de indumentaria necesaria.

3. Sulca y Sánchez (2018) mencionan que:

Sin duda alguna, si se puede ver diversos factores que dificulten la aplicación de dicha Ley, que pueden ser, la falta de conocimiento en todos sus ámbitos (técnico, informático o jurídico) de jueces y fiscales y todos los encargados, así como también la falta de cooperación internacional. La DIVINDAT como ente encargado de perseguir y desarticular crímenes informáticos, desde su perspectiva uno de esos factores vienen a ser desde las políticas estatales hasta la poca atención en este ámbito.

4. Escobar y Román (2018) mencionan que:

No existen factores que impidan la aplicación de la Ley 30171, debido a que toda Ley es de carácter imperativa. Lo que existe es poca ayuda brindada a la DIVINDAT, por parte del Ministerio del Interior, ya sea en apoyo técnico o de conocimiento procedimental, como legal,

5. Respecto al análisis documental podemos señalar como el más importante a la cuarta disposición Complementaria de la Ley 30171 el cual señala lo siguiente: La Cooperación Operativa se da […] para dar efectividad a la presente Ley**,** por ello la Policía Nacional del Perú, el Ministerio Publico, el Poder Judicial, el PERCERT (Centro de respuesta temprana del gobierno para ataques cibernéticos), la ONGEI (Oficina Nacional de Gobierno para ataques cibernético), Organismos especializados de las Fuerzas Armadas y los operadores del sector privado involucrados en la lucha contra los delitos informáticos deben establecer protocolos de cooperación operativa.

6. Al respecto Puelles (2014) en su trabajo de investigación titulada *"Luces y sombras en la lucha contra la delincuencia informática en el Perú"*, llega a la conclusión de que: [..] Si bien es cierto nuestro Legislador se preocupó por penalizar este tipo de delitos o conductas ilícitas y algunas entidades como la Policía Nacional (PNP) realizaron intentos para poder luchar contra el cibercriminal por medio de la especialización de sus divisiones y efectivos, si se puede llegar a un concepto seria que muchas instituciones como el Ministerio Público y el Poder Judicial han quedado rezagadas por lo que de igual forma deberían abrir las puertas a la modernización de sus equipos y especializar a sus operadores jurídicos pues las

técnicas que se requieren para la investigación y persecución de esta actividad delictiva no es igual a la de los delitos que comúnmente se conocen.

7. Además según Poinst (2003) señala que son delitos informáticos aquellos comportamientos ilícitos efectuados por medio de procesos electrónicos, que su ilicitud recaía en bienes que presentaban una configuración predeterminada en el desarrollo o también sobre nuevos objetos tales como software y hardware

Cabe señalar que los delitos informáticos a pesar de estar configurados en una ley, han tenido dificultades para poder ser aplicada dentro de nuestra sociedad.

De acuerdo a los resultados obtenidos a través de las entrevistas, análisis documental, antecedentes y marco teórico, se puede decir que los delitos informáticos no logran aplicarse correctamente, debido a que como lo han señalado muchas personalidades existe la ley, existe las exigencias que se requiera para su aplicación, pero no existe indumentaria, no hay capacitaciones a los entes encargados, a pesar de existir una disposición dentro de la Ley para la cooperación operativa, que permita de esta manera lograr que se pueda castigar estos delitos, no han sido efectivas y quizás estos problemas pudiesen ser resueltos si nos adherimos al Convenio de Budapest, pero como se ha visto hasta la actualidad, el Estado no se ha preocupado por este tema a pesar de ser importante, ya que una estafa virtual, clonación de tarjetas, extorsión, son temas muy graves que afectan nuestra sociedad, pero el ejecutivo no se ha preocupado porque esta Ley existente se aplique correctamente.

Objetivo Especifico 1: Determinar si la falta de capacitación de los magistrados, fiscales y PNP, es un factor principal que impide la aplicación de la ley N° 30171 en el sector Lima Norte en el año 2016

Supuesto Especifico 1: La Falta de capacitación de los magistrados, fiscales Y PNP respecto a los delitos informáticos, es un factor principal que impidió la correcta aplicación de la ley N°30171 en el sector Lima Norte en el año 2016

1. Francia, Robles y Escobar (2018), mencionan que:

Debe haber una capacitación totalmente integral, pero además es necesario un equipo experto en informática, porque los abogados solo estamos preparados en leyes y nada más, el resto de cosas solo podremos conocerlas a grandes rasgos pero en sí, se requiere la ayuda

de un experto en informática para la realización de las capacitaciones. Es obligación del Estado ayudar y promover instrumentos que faciliten la impartición de justicia en especial sobre una ley que especifica un tema tan latente, como lo es los delitos informáticos. Además es necesario la capacitación a los magistrados, fiscales para su conocimiento e instrucción a su personal, para poder manejar de manera eficiente los casos por delitos informáticos.

Además cabe mencionar que es imperativo que se otorgue toda clase de información a los funcionarios públicos que tienen como misión la aplicación de la justicia. A criterio personal, la falta de información a las autoridades que se encargan del seguimiento y de la administración del justicia, es un factor determinante, ya que los magistrados son los encargados de hacer cumplir lo que dicta la norma, y el desconocimiento en este asunto impediría la función de igual forma, y de la misma manera sucedería con los demás servidores públicos.

2. Salazar, Urbina, y Sulca (2018) mencionan que:

Siempre es algo positivo reforzar los alcances que puedan tener nuestros funcionarios públicos y con mayor razón a quienes manejan temas tan delicados como la lucha contra la ciberdelincuencia. Es parte de las funciones del Estado renovar y proveer de nuevo y mejores recursos, tanto intelectuales en el caso de boletines informáticos, talleres y capacitaciones como en recursos técnicos, como los son: los materiales de trabajo para darle el tratamiento adecuado para esta modalidad. Por tanto el Estado en su afán de querer mejorar la inseguridad que muchas normas provocan debería brindar a los funcionarios encargados mayores alcances para que desempeñen sus funciones de manera óptima

3. Sánchez y Román (2018) mencionan que:

Todo apoyo en forma de capacitación a los efectivos como otras formas preparación más que una acción particular vendría a convertirse más, en un apoyo a la propia sociedad, por parte del Estado para poder desempeñarse con mayor efectividad. No se discute que con algo más de preparación se puede realizar un mejor rendimiento por una parte, no solo de la DIVINDAT, sino también al Poder Judicial y el Ministerio Público, también se requiere de la cooperación operativa para en conjunto lograr afrontar estos delitos.

4. Acosta y Minaya (2018) afirman que:

El Estado tiene la obligación de dar todos los alcances necesarios para el cumplimiento de las funciones de las entidades estatales, pero no solo en forma de capacitaciones. Sería deseable en todo caso, aunque desde el punto de vista profesional se entiende que deben de existir o crearse instituciones o departamentos *ad. Hoc* con agentes especializados. La falta de información que el Estado no brinda, no determina, toda vez que magistrados, fiscales y la PNP pueden obtener asesoría especializada que garantice la correcta implementación para la aplicación de la ley.

5. Respecto al análisis documental en el 12vo congreso de las naciones unidas sobre delitos informáticos nos menciona que estar dentro del Convenio de Budapest, es la posibilidad de obtener formación y asistencia de los Estados miembros, acerca de la prevención e investigación de los delitos informáticos, además de tener entrenamiento para los responsables del cumplimiento de la ley como jueces, fiscales y policías,

6. Al respecto Díaz (2014) en su investigación titulada *"Delitos Informáticos como combatirlos"*, mencionó que para poder combatir a los delitos informáticos se requiere de fortalecer la legislación, entablar alianzas internacionales, especializar a la policía y autoridades judiciales, así como también informar a los ciudadanos y recibir cooperación de las instituciones privadas y públicas.

7. Cabe mencionar que en el caso peruano en la quinta disposición complementaria final no derogada de la Ley Nº 30096, nos menciona que las instituciones públicas que conocen del tema de los delitos informáticos deben capacitar profesionalmente al personal de la PNP, el Ministerio Publico y el Poder Judicial, sobre estos temas

Cabe señalar que tal como mencionan los sujetos de la investigación las capacitaciones son un factor importante para la correcta aplicación de la ley los delitos informáticos, pero además mencionan que estas capacitaciones no bastan con hacerlas a la ligera, sino que se debe realizar con asistencia profesional de expertos que sepan de estos asuntos, asimismo son necesarias para poder realizar un tratamiento adecuado a estos delitos.

Por otro lado el tema de las capacitaciones sobre delitos informáticos hacia las autoridades competentes se ha venido tratando desde la aparición de la primera ley de delitos informáticos, estando regulado este aspecto en la quinta disposición complementaria final,

que no ha sido derogado, el problema es que esta disposición no obliga a las instituciones públicas a realizar dichas capacitaciones, solo lo consideran como un deber

Objetivo Específico 2: Determinar si la falta de adhesión al convenio de Budapest es un factor principal que impide la aplicación de la ley N° 30171 en el sector Lima Norte en el año 2016.

Supuesto Especifico 2: La falta de adhesión al convenio de Budapest es un factor principal que impidió la correcta aplicación de la ley N° 30171 en el sector Lima Norte en el año 2016.

1. Acosta, Robles y Escobar (2018) mencionan que:

El Estado tiene la obligación de dar todos los alcances necesarios para el cumplimiento de las funciones de las entidades estatales, por ende sería una oportunidad relevante. De existir ya una tratativa de carácter internacional es de suma importancia, debido a que entre nuestras fuentes del derecho se encuentras los tratados internacionales como fuente para regular criterios que se acepten a nuestra realidad. No estar adscritos al convenio de Budapest, es un factor que impide la aplicación de la Ley de delitos informáticos, debido a que atrasa la captura al delincuente cibernético, y además es un claro reflejo de que nuestra legislación aun no cumple con los estándares internacionales, para encontrarse dentro de dicho convenio.

Tanto con la cooperación internacional para la captura del delincuente cibernético, como para la seguridad de la información como bien jurídico protegido de los delitos informáticos. Influiría de manera positiva estar adheridos a dicho convenio, en muchos ámbitos tanto en la cooperación internacional como en la capacitación al personal encargado.

2. Salazar, Urbina y Sulca (2018) mencionan que:

La adhesión al convenio de Budapest lo cambia todo, ya que acarrearía muchas cosas positivas para nuestro sistema y el hecho de que aún no estemos dentro del convenio si es un factor de que algo no anda bien en nuestra legislación. Tomando en cuenta que un convenio internacional se crea para resolver un problema común que afecta a todos, y por

ello significa que ese problema lo tienen otros países, y que por sí solos no pueden hacer frente, por diferentes motivos, en cambio sí se agrupan para optar medidas que ayuden a dar solución al problema, eso sí podría funcionar, y si el Perú aún no está incluido, es Ahí donde encontramos la falla de una mala ejecución de nuestras normas y sistema siendo este un factor detonante. Se cuenta actualmente con una normativa que regula la clase de delitos, sin embargo, no está respaldada por un tratado o convenio y al no respaldado por otra forma, se dificulta la aplicación de la ley actual. Nuestro sistema legal, mejoraría de la manera más evidente al contar con ayuda internacional, entre otras posibilidades como disminuir el crecimiento delincuencial

3. Francia, Minaya,

La adhesión al Convenio de Budapest, se conduciría a buscar como siempre el equilibrio en las acciones penales y los derechos humanos que nos asisten, porque se implementaría la Ley de modo correcto con acceso a informática forense, que en la actualidad aún no tenemos, de esta manera Permitiría, ser un bloque homogéneo contra la CIBERDELINCUENCIA, habría una capacitación mayor y muy seria

4. Sánchez y Román (2018)

La DIVINDAT se ha encargado de perseguir estos tipos de delitos desde su creación, han brindado información respecto a cómo no ser víctima de los delitos informáticos, pero aun así existe un alto número de personas que han sido víctimas de clonación de tarjetas, robo de data a empresas entre otros, por ello si se llegara a estar dentro del convenio de Budapest, ayudaría en la difusión de este tema.

Toda ayuda es importante en el combate contra la ciberdelincuencia, el procedimiento de investigación policial es muy engorroso porque se tiene que acoger a normas existentes, no hay cooperación con la investigación policial y producen retardo, por ejemplo para un caso de extorsión, hay que esperar dos o tres semanas para que salga una orden judicial que permita dar la información, cuando eso debería ser al momento, se ha tratado de concientizar a los entes que dentro de su jurisdicción tienen la facultad para poder acelerar este proceso, pero se excusan diciendo que la policía puede hacer mal uso de la información.

5. Con respecto al análisis documental se debe resaltar al proyecto de Dictamen Nº2807-2017, presentado por el Poder Ejecutivo, donde se propone la aprobación del “Convenio de

Ciberdelincuencia" en el cual se señala que es importante y necesaria la adhesión del Perú al convenio de Budapest , ya que ayudaría a prevenir los actos que pongan en peligro la confidencialidad ,la integridad, y la disponibilidad de los sistemas ,redes y datos informáticos, además de garantizar la tipificación del delito, facilitar su detección , investigación y sanción, en el ámbito nacional e internacional ,así como , la cooperación judicial internacional, por tanto vemos que el Perú, esta con miras a llegar a formar parte del Convenio de Budapest.

6. De la misma manera Iglesias (2010) en su investigación "*análisis al convenio de Budapest*" menciona que: El Convenio de Budapest obliga a recolectar y guardar información sobre comunicaciones, así como también a acceso a otros países firmantes que la soliciten.

7. Además Prado (2008) menciona que el convenio de Budapest se dio en el consejo europeo, en el 2001 buscaba homogenizar las legislaciones de sus miembros y de los países observadores para apoyar la lucha contra los crímenes en el sistema digital, en la actualidad cuenta con 45 miembros adicionales a los europeos

Cabe señalar que en cuanto a la Adhesión del Perú al Convenio de Budapest, o también llamado al convenio Internacional de Cibercriminalidad, según los expertos en el tema, mencionan que no estar dentro de dicho convenio es un factor que puede retardar el proceso de captura y sanción a los delincuentes informáticos, asimismo hablan de la cooperación internacional que este convenio nos podría generar, además es importante destacar que el convenio de Budapest viene combatiendo estos delitos desde el año 2001 y ya cuenta con 45 países miembros.

V. CONCLUSIONES

Las conclusiones son la parte en donde finaliza el trabajo o cualquier proceso de investigación que se transforma en una tesis, debido a que en ese punto el investigador o tesista debe por medio de la sintonización señalar lo más importante en todo el trabajo, en concreto se indica la demostración o negación de las hipótesis investigadas o la corroboración del objetivo planteado (Sevilla, 2008.p75).

En el presente trabajo de investigación, en la etapa final de todo el desarrollo de la tesis, se llegó a conseguir el objetivo general y los específicos planteados, que estos a su vez han ayudado a fundamentar los supuestos jurídicos general y los específicos, planteados en el primer capítulo, en ese contexto se ha podido concluir lo siguiente:

1. Los factores principales que han impedido la aplicación de la Ley Nº 30171 han sido: la falta de capacitaciones a los magistrados, fiscales y PNP y la falta de cooperación operativa, la cual se podría lograr mediante la adhesión al Convenio de Budapest.

2. La falta de capacitación de los magistrados, fiscales y PNP, es un factor principal que impide la correcta aplicación de la Ley Nº 30171, ya que las capacitaciones a estas autoridades no bastan con hacerlas a la ligera, sino que se debe realizar con asistencia profesional de expertos que sepan de estos asuntos y con el material necesario, en la quinta disposición complementaria final no derogada de la Ley Nº 30096, nos habla del tema de las "Capacitaciones", pero lamentablemente de acuerdo al resultado obtenido en la presente investigación se verifica que en la práctica no se viene aplicando, ya que en dicha disposición las capacitaciones mencionan que son un deber realizarlas, mas no brinda un carácter de obligación a las instituciones públicas encargadas.

3. La falta de adhesión al Convenio de Budapest es un factor principal que impidió la correcta aplicación de la Ley Nº 30171 o también llamado al convenio Internacional de Cibercriminalidad, los expertos consultados mencionan que no ser partícipe de dicho convenio es un factor que puede retardar el proceso de captura y sanción a los delincuentes informáticos, además es muy importante la cooperación internacional que este convenio nos podría generar.

VI. RECOMENDACIONES

Las recomendaciones son instrumentos de ayuda para asociarse lógicamente con las conclusiones establecidas, para poder interponer sugerencias para implementar o realizar la solución planteada, proponen el logro de una situación favorable e ideal establecida, desde la óptica del tema abordado en el trabajo de investigación, por tanto se harán únicamente del tema referido en la investigación (Palella, 2004, p.78).

PRIMERO: Los factores que impiden la correcta aplicación de la Ley 30171, como ya se mencionó líneas arriba son: La falta de capacitación de la PNP, Jueces y fiscales y la falta de adhesión de nuestro país al convenio internacional de Budapest, por tanto con respecto a estos dos factores las autoridades competentes deberían realizar una preparación constante, permanente y fortalecer nuestra legislación tanto a las capacitaciones como a la cooperación operativa nacional, para poder adherirnos definitivamente al convenio de Budapest.

SEGUNDO: En cuanto que la falta de capacitaciones a la PNP, jueces y fiscales, son un factor principal para poder aplicar correctamente la Ley 30171, las entidades encargadas según la Ley tienen que empezar a realizar estas capacitaciones de manera frecuente y obligatoria con profesionales expertos en la materia de delitos informáticos, de la misma manera reformar la Ley 30096 en el ámbito de las capacitaciones, que no solo sea un deber sino una obligación realizarlas.

TERCERO: Otro factor principal es la adhesión al Convenio de Budapest, un gran número de expertos coinciden que adherirnos a un convenio internacional, que viene combatiendo los delitos informáticos muchos años en cooperación con otros países del mundo es una gran oportunidad para el país, porque de esa manera podemos hacer frente a estos delitos que muchas veces no han podido llegar a ser resueltos, por la falta de entrenamiento y cooperación operativa en la investigación, por tanto, el Estado debe normar las legislaciones correspondientes de forma adecuada para poder ser aptos en formar parte del convenio de Budapest.

REFERENCIAS

Referencias metodológicas:

Bobadilla, M. (2009). "*Metodología de la investigación científica*". (1º Ed) Huaraz: Editorial Imprenta Bobadilla C.C "Inversiones Lima".

Carrasco, S. (2013). "*Metodología de la investigación científica*. Pautas metodológicas para diseñar y elaborar el proyecto de investigación". (5.º Ed) Lima: Editorial San Marcos.

Cotrina, P, Pacheco A. y Moretti K. (2012). *Referencias estilo APA adaptación de la norma de la American Psycological Association.* Lima: Fondo editorial de la Universidad César Vallejo.

Orbegoso,T (2008).*La metodología dentro de un trabajo de investigación.* Lima: Editorial de la Universidad Nacional Mayor de San Marcos.

Benites, R (2005) *La esencia de la investigación científica* .Madrid: Editorial ESIC.

Figueroa, H (2009) *Bases de la investigación cualitativa*. Barcelona: Editorial MORATA S.L.

Referencias temáticas:

Acurio, L. (2006) "*Delitos Informáticos*", Lima: academia cielo.

Alejos, P. (2016) "*Convenio de Ciberdelincuencia comentarios*", Lima: lyos.

Cabrera, R. (2014) "*Delitos Informáticos*", Lima: Ediciones san marcos

Callegari, L. (2008), "*Delitos informáticos*", Lima: Legis

Fernández, C. (2015). *Delitos Informáticos*. Lima: Legis

Garrido, G. (1993) "*Delitos informáticos en tiempos modernos*", Lima, Editorial Leyes

Legislación Nacional

Código Penal Peruano.

Ley 30096 "*Ley de delitos Informáticos*"

Ley 30171 "*Ley de delitos Informáticos*".

Tesis Internacional

Rincón, J. (2015). *El delito en la ciber sociedad y la justicia penal internacional.* Madrid: Universidad Complutense de Madrid.

Díaz (2014) *Delitos informáticos, como combatirlos.* México: Gles.

Iglesias (2010) *Análisis al Convenio de Budapest*. México: Universidad Autónoma de México.

Código Penal Alemán de 1987.

Acta Federal de Estados Unidos de 1994 Ley N°8819.

Código Penal de Austria de 1987.

Ley de Ciberdelincuencia N° 19223 de Chile Código Penal Español de 1995.

XV Congreso de la Organización de las Naciones Unidas en el año 2013.

Tesis Nacional

Mamani, C. (2017). *Delitos Informáticos*. Lima: Egacal Mazuelos, A. (2014). *Delitos Informáticos*. (3.a ed.). Lima: PUCP.

Rivero, T. (2008) "*Delitos Informáticos*" Lima: PUCP.

Rodríguez, I. (1989) "*Delitos Informáticos*", Lima: LKN.

Villavicencio, F. (2015) *"Criminalidad informática*" Lima: PUCP.

Páginas Web

Ceresole, A. y Oyarzábal, S. (2014). *Los delitos informáticos*. (Tesis de maestría en Derecho).Recuperada de: https://www.terragjurista.com.ar/doctrina/Delitos_informaticos.pdf

Montaño, A. (2008). *La problemática jurídica en la regulación de los delitos informáticos*. Recuperada de: http://www.scielo.org.mx/scielo.php?script= arttext&pid=S0041-86332012000300002.

Portal de la DIVINDAD, recuperado de: https://www.mininter.gob.pe/content/ciberpolicí-contra-delitos-informáticos

Puelles, E. (abril 2014). Luces y sombras en la lucha contra la delincuencia informática en el Perú. Revista Jus- Doctrina. Recuperado xddehttp://portal.mpfn.gob.pe/ncpp/files/c12171_articulo%20dr.%20sas.pdf

ANEXOS

Anexo. 01

Matriz de Consistencia para la investigación

Estudiante: Santiago Ricardo Juan Cotrina Yucra
Línea de Investigación: Derecho Penal
Facultad/Escuela: Derecho

Título del Trabajo de Investigación	"Los factores principales que impiden la aplicación de la ley N°30171- Lima Norte en el año 2016"
Problema General	¿Cuáles son los factores principales que impiden la aplicación de la Ley N° 30171 en el sector Lima Norte en el año 2016?
Problema Específico 1	¿Porque la falta de capacitación de los magistrados, fiscales y PNP, es un factor principal que impide la aplicación de la ley N° 30171 en el sector Lima Norte en el año 2016?
Problema Específico 2	¿Porque la falta de adhesión al convenio de Budapest es un factor principal que impide la aplicación de la ley N° 30171 en el sector Lima Norte en el año 2016?
Objetivo General	Analizar cuáles son los factores principales que impiden la aplicación de la Ley N° 30171 en el sector Lima Norte en el año 2016
Objetivo Específico 1	Determinar si la falta de capacitación de los magistrados, fiscales y PNP, es un factor principal que impide la aplicación de la ley N° 30171 en el sector Lima Norte en el año 2016
Objetivo Específico 2	Determinar si la falta de adhesión al convenio de Budapest es un factor principal que impide la aplicación de la ley N° 30171 en el sector Lima Norte en el año 2016
Supuesto General	Los factores principales que impidieron la correcta aplicación de la Ley N° 30171 en el sector Lima Norte, fueron: La falta de capacitación a los magistrados, fiscales y PNP, respecto a los delitos informáticos y la falta de adhesión al convenio de Budapest en el sector Lima Norte en el año 2016

Supuesto Específico 1	La falta de capacitación de los magistrados, fiscales y PNP respecto a los delitos informáticos, es un factor principal que impidió la correcta aplicación de la ley N°30171 en el sector Lima Norte en el año 2016
Supuesto Específico 2	La falta de adhesión al convenio de Budapest es un factor principal que impidió la correcta aplicación de la ley N° 30171 en el sector Lima Norte en el año 2016
Diseño del Estudio	Teoría Fundamentada
Técnicas e Instrumentos de Recolección de Datos	Técnica: Análisis documental, Instrumento: La Guía de análisis Documental Técnica: La entrevista, Instrumento: La Guía de Entrevista
Categorías **Subcategorías**	Aplicación de la Ley N° 30171 Capacitación a la PNP, jueces y fiscales Adhesión al Convenio de Budapest La Ley N° 30171 Delitos Informáticos Elementos del delito La ley 30096

UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE DERECHO

ESCUELA PROFESIONAL DE DERECHO

"Los Ausentes principales por Impedir la aplicación de la Ley N°30771- Lima Norte en el año 2016"

TESIS PARA OBTENER EL TITULO PROFESIONAL DE ABOGADO

AUTOR:

ASESOR:

TEMÁTICO: Mg.

METODOLÓGICO: Mg.

LÍNEA DE INVESTIGACIÓN:

UCV UNIVERSIDAD CÉSAR VALLEJO	AUTORIZACIÓN DE PUBLICACIÓN DE TESIS EN REPOSITORIO INSTITUCIONAL UCV	Código : F08-PP-PR-02.02 Versión : 09 Fecha : 23-03-2018 Página : 1 de 1

Yo Santiago Ricardo Juan Catrina Yucra identificado con DNI Nº 76404576,
egresado de la Escuela Profesional de Derecho de la Universidad César Vallejo, autorizo (X), No autorizo ( ) la divulgación y comunicación pública de mi trabajo de investigación titulado "Los factores principales que impiden la aplicación de la Ley N° 30171 Lima Norte, 2018"; en el Repositorio Institucional de la UCV (http://repositorio.ucv.edu.pe/), según lo estipulado en el Decreto Legislativo 822, Ley sobre Derechos de Autor, Art. 23 y Art. 33

Fundamentación en caso de no autorización:

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

FIRMA

DNI: .....

FECHA: ..... de ..... del 201....

Elaboró	Dirección de Investigación	Revisó	Responsable de SGC	Aprobó	Vicerrectorado de Investigación

UNIVERSIDAD CÉSAR VALLEJO

AUTORIZACIÓN DE LA VERSIÓN FINAL DEL TRABAJO DE INVESTIGACIÓN

CONSTE POR EL PRESENTE EL VISTO BUENO QUE OTORGA EL ENCARGADO DE INVESTIGACIÓN DE

MAGDA MEJIA BARTOLO

A LA VERSIÓN FINAL DEL TRABAJO DE INVESTIGACIÓN QUE PRESENTA:

SANTIAGO RICARDO JUAN COTRINA YUCRA

INFORME TÍTULADO:

LOS FACTORES PRINCIPALES QUE IMPIDAN LA APLICACIÓN DE LA LEY 30171 EN LIMA NORTE EN EL AÑO 2016

PARA OBTENER EL TÍTULO O GRADO DE: ABOGADO (A)

ABOGADO

SUSTENTADO EN FECHA: **09 DE JULIO DEL 2018**

NOTA O MENCIÓN: 16

UCV OFICINA DE INVESTIGACIÓN V°B° EAP DE DERECHO

FIRMA DEL ENCARGADO DE INVESTIGACIÓN

DR. MAGDA MEJIA BARTOLO

UCV UNIVERSIDAD CÉSAR VALLEJO	ACTA DE APROBACIÓN DE ORIGINALIDAD DE TESIS	Código : F06-PP-PR-02.02 Versión : 09 Fecha : 23-03-2018 Página : 1 de 1

Yo, LUCA ACETO,
docente de la Facultad Derecho y Escuela Profesional de Derecho de la Universidad César Vallejo LIMA NORTE. (precisar filial o sede), revisor(a) de la tesis titulada

"LOS FACTORES PRINCIPALES QUE IMPIDEN LA APLICACION DE LA LEY N° 30171 – LIMA NORTE EN EL AÑO 2016"

del (de la) estudiante SANTIAGO RICARDO JUAN COTRINA YUCRA, constato que la investigación tiene un índice de similitud de 30 % verificable en el reporte de originalidad del programa Turnitin.

El/la suscrito (a) analizó dicho reporte y concluyó que cada una de las coincidencias detectadas no constituyen plagio. A mi leal saber y entender la tesis cumple con todas las normas para el uso de citas y referencias establecidas por la Universidad César Vallejo.

Lugar y fecha LIMA 23/3/2018

Firma

Nombres y apellidos del (de la) docente

DNI: 48074953

Elaboró	Dirección de Investigación	Revisó	Responsable de SGC	Aprobó	Vicerrectorado de Investigación