UNIVERSIDAD ANDINA DE CUSCO

FACULTAD DE DERECHO Y CIENCIAS POLÍTICAS

ESCUELA PROFESIONAL DE DERECHO Y CIENCIAS POLÍTICAS

LOS DELITOS INFORMATICOS EN PERÚ Y LA SUSCRIPCIÓN DEL CONVENIO DE BUDAPEST

Tesis para optar el título profesional de ABOGADA.

Presentado por: Bach. Marleny Yudy Huamán Cruz

Asesor: Dr. Carlos Alberto Pérez Sánchez

CUSCO – 2020

DEDICATORIA

A Dios que guía nuestro camino

A mi familia, por el amor, comprensión y el apoyo constante que me han brindado, sobre todo a mí Mamá una mujer amorosa, fuerte y luchadora que nunca se ha dado por vencida, quien pese a las dificultades de la vida ha estado a mi lado.

AGRADECIMIENTO

A mi alma mater, la Universidad Andina del Cusco

A todos los docentes que contribuyeron en mi formación profesional

A mis compañeros y amigos que han estado presente en etapa universitaria.

NOMBRE Y APELLIDOS DE JURADO DE TESIS

RIOS MAYORGA JULIO TRINIDAD (primer Dictaminante)

CHUQUIMIA HURTADO JOSE (segundo dictaminante),

JURADOS REPLICANTES:

SIXTO MADISON BARRETO JARA **(primer replicante)**

OROZ FIGUEROA ELVIS **(segundo replicante)**

INDICE

ÍNDICE DE CUADROS

ÍNDICE DE TABLAS

ÍNDICE DE IMÁGENES

RESUMEN

La presente investigación, intitulada "LOS DELITOS INFORMÁTICOS EN PERÚ Y LA SUSCRIPCIÓN DEL CONVENIO DE BUDAPEST", es realizada a partir de observar una realidad en la que los delitos informáticos van tomando mayor presencia y de conocer la postura que asume nuestro Estado para hacer frente a estos delitos; una de ellas es la suscripción del Convenio de Budapest o Convenio de Ciberdelincuencia y lo que se analiza, es la manera en que la suscripción del mencionado convenio influye en el tratamiento de los delitos informáticos, que nos lleva a plantearnos las siguientes interrogantes: ¿De qué manera la suscripción del convenio de Budapest influye en el tratamiento de los delitos informáticos? como pregunta general, y como preguntas específicas, ¿Cuál es el desarrollo legislativo de los delitos informáticos en el Perú? ¿Cuál es la problemática actual generada por los delitos informáticos en el Perú? ¿Cómo es la legislación de delitos informáticos en países sudamericanos que suscribieron el convenio de Budapest? ¿Cuáles son los efectos que produce la suscripción del convenio de Budapest?, cada una de ellas con sus respectivos objetivos.

En el Marco teórico, se pone especial énfasis en el desarrollo de nuestras categorías de estudio, siendo la primera categoría "Los Delitos Informáticos" y la segunda categoría "El Convenio de Budapest".

En el diseño metodológico se ha considerado: El enfoque de investigación cualitativo, por cuanto se orienta a la revisión y obtención de datos de carácter teórico y legislativo antes que a la obtención de datos estadísticos; como tipo de investigación: Descriptiva Jurídica y Comparativa; y el nivel de investigación: Investigación básica, al estar orientada a la revisión de conocimientos teóricos que se verán ampliados. Así como técnicas e instrumentos que han permitido obtener información doctrinaria, legislativa y de casos.

Todo ello ha permitido arribar a las siguientes conclusiones: **PRIMERA:** La suscripción del Convenio de Budapest, influye de manera relativa en el tratamiento de los delitos informáticos, al centrarse en la adecuación de nuestra normatividad a la prevista en el mencionado Convenio, como es establecer un catálogo de delitos, establecer normas procesales orientadas a salvaguardar las evidencias digitales y recurrir a la cooperación internacional para investigar la comisión de este tipo de delitos; y la principal característica que es la cooperación internacional para investigar casos trascedentes ha tenido mínima aplicación desde su suscripción. **SEGUNDA:** El desarrollo legislativo de los delitos informáticos en el Perú ha sido progresivo y rápido en un periodo de 30 años que comienza en 1991 con la tipificación de estos delitos en el artículo 207 del Código Penal, pero, sobre todo desde el año 2013 con la promulgación de la ley 30096 y las modificaciones realizadas en con la Ley 30171, hasta la suscripción del Convenio en mención, permitiendo contar en la actualidad con legislación equiparable a la legislación comparada de delitos informático. **TERCERA:** La problemática actual causada por

la comisión de delitos informáticos en el Perú es creciente; obedece al acceso y uso de diversos y novedosos medios tecnológicos por parte de los ciberdelincuentes, situación que hace difícil su identificación y ubicación. En América Latina en el año 2017 el Perú ha sido el más afectado con los programas ransomware con un 25.1% del total de casos presentado; para el 2019, nuestro país era el tercer país en América latina más afectados con programas Spyware; el mismo años se presentaron 3012 denuncias por fraude informático y 247 denuncias sobre suplantación de identidad en la Divindat); se suma a ello, el escaso presupuesto destinado a contar con tecnología de alta gama para la persecución de este tipo de delitos. **CUARTA:** La legislación sobre delitos informáticos de países sudamericanos que suscribieron el convenio de Budapest es uniforme y permite una integración generada a partir de la cooperación internacional promovida por dicho Convenio. **QUINTA:** Los efectos de suscribir el Convenio de Budapest, son positivos a nivel legislativo, porque permite contar con un catálogo integral de delitos informáticos, sin embargo, se requieren de políticas orientadas a destinar recursos económicos para el equipamiento de la tecnología informativa que permita hacer frente a los delitos informáticos.

ABSTRACT

The present investigation, entitled "COMPUTER CRIMES IN PERU AND THE SUBSCRIPTION OF THE BUDAPEST CONVENTION", is carried out based on observing a reality in which computer crimes are becoming more prevalent and knowing the position that our State assumes to face to these crimes; One of them is the signing of the Budapest Convention or Cybercrime Convention and what is analyzed is the way in which the signing of the aforementioned agreement influences the treatment of computer crimes, which leads us to ask ourselves the following questions: How does the signing of the Budapest Convention influence the treatment of cybercrime? As a general question, and as specific questions, what is the legislative development of computer crimes in Peru? What is the current problem generated by computer crimes in Peru? What is the cybercrime law like in South American countries that signed the Budapest Convention? What are the effects of the signing of the Budapest agreement? each with its respective objectives.

In the theoretical framework, special emphasis is placed on the development of our study categories, the first category being "Computer Crime" and the second category "The Budapest Convention".

For this, the methodological design has been considered: The qualitative research approach, since it is oriented to the revision and obtaining of theoretical and legislative data rather than to obtaining statistical data; as type of research: Descriptive Legal and Comparative; and the research level: Basic research, being

oriented to the revision of theoretical knowledge that will be expanded. As well as techniques and instruments that have allowed obtaining doctrinal, legislative and case information.

All this has led to the following conclusions: FIRST: The signing of the Budapest Convention has a relative influence on the treatment of computer crimes, by focusing on the adaptation of our regulations to that provided for in the aforementioned Convention, such as establishing a catalog of crimes, establishing procedural rules aimed at safeguard digital evidence and resort to international cooperation to investigate the commission of this type of crime; and the main characteristic that is international cooperation to investigate transcendent cases has had minimal application since its subscription. SECOND: The legislative development of computer crimes in Peru has been progressive and rapid in a period of 30 years that begins in 1991 with the typification of these crimes in article 207 of the Penal Code, but, especially since 2013 with the promulgation of Law 30096 and the modifications made in Law 30171, until the signing of the aforementioned Convention, currently allowing for legislation comparable to comparative legislation on computer crimes. THIRD: The current problem caused by the commission of computer crimes in Peru is growing; It is due to the access and use of diverse and innovative technological means by cyber criminals, a situation that makes their identification and location difficult. In Latin America, in 2017, Peru was the most affected by ransomware programs, with 25.1% of the total cases presented; for 2019, our country was the third country in Latin America most affected by

Spyware programs; in the same year, 3012 complaints were filed for computer fraud and 247 complaints about identity theft in the Divindat); In addition to this, the scarce budget allocated to have high-end technology for the prosecution of this type of crime. FOURTH: The legislation on cybercrime of South American countries that signed the Budapest Convention is uniform and allows integration generated from the international cooperation promoted by said Convention. FIFTH: The effects of signing the Budapest Convention are positive at the legislative level, because it allows having a comprehensive catalog of computer crimes, however, policies aimed at allocating economic resources are required to equip information technology that allows against cybercrime.

PALABRAS CLAVES

Delitos Informáticos; Convenio de Budapest; Suscripción de un Convenio Internacional; Gobierno Digital; Ciberseguridad; Ciberdelito, Ciberdelincuente.

CAPÍTULO I

EL PROBLEMA Y EL METODO DE INVESTIGACIÓN

1.1. Problema

1.1.1. Planteamiento del Problema

El Internet y el desarrollo de las nuevas tecnologías informáticas y de comunicación virtual, además de facilitar el acceso a información y a diferentes formas de comunicación, también han representado un nuevo escenario para la existencia de nuevos delitos, nos referimos a los delitos informáticos o ciberdelitos.

La tecnología cibernética, ha progresado en USA, gracias al departamento de Protección de esta nación, que "planeaba desarrollar un sistema de comunicaciones por medio de PCS conectadas en una red descentralizada (…). Esto se logró hasta 1969 con la primera red de computadoras denominada ARPANet, para en 1990 dar lugar al internet" (FRAGOSO, 2004, pág. 30)

En tanto se iba presentando éste desarrollo tecnológico, también se iban presentando casos de uso indebido de los programas computacionales o redes de ordenadores; uno de los primeros casos vincula al estudiante Kevin Mitnick, quien habría logró acceder la seguridad administrativa de su colegio, según refiere (ORANTES, 2019) también: " (…), logro acceder a los sistemas de las agencias y compañías más grandes del mundo, aparentemente impenetrables,

como Motorola, Sun Microsystems o Pacific Bell". Casos similares se iban presentando en diferentes partes del mundo, situación que ameritaba que se asuman medidas de protección y regulación.

En 1983, la Organización de Cooperación y Desarrollo Económico (creada como socio económico para la OTAN en 1947 con el apoyo de los Estados Unidos y Canadá a fin de coordinar el plan Marshall para la reconstrucción de Europa tras la Segunda Guerra Mundial), inicio un estudio a fin de aplicar y armonizar las leyes penales a nivel internacional frente al problema del uso indebido de programas de computación; en 1986 publicó un **informe de delitos de informática intitulado "Análisis de la Normativa Jurídica",** en el cual daba a conocer normas vigentes y proponía su regulación teniendo como referencia una lista de ejemplos de delitos informáticos, para que los países puedan prohibir y sancionar penalmente estas acciones.

Por su parte, la Organización Internacional de las Naciones Unidas ha publicado una descripción de **Tipos de delitos informáticos**; en esta misma línea de acciones, en 1992, la Asociación Internacional de Derecho Penal, durante el coloquio celebrado en Wurzburgo - Alemania, adoptó diversas recomendaciones respecto a los delitos informáticos, entre ellas, que en la medida que el Derecho penal no sea suficiente, deberá promoverse la modificación de la definición de los delitos existentes o la creación de otros nuevos si no basta con la adopción de otras medidas, por ejemplo, el "principio de subsidiariedad".

A las acciones realizadas por entidades internacionales, le sucedieron las acciones legislativas de diferentes Estados a fin de abordar el tema de los delitos informáticos; en Alemania en 1986 con la Ley contra la Criminalidad Económica (Espionaje de datos, estafa informática, sabotaje informático, utilización abusiva de tarjetas de crédito); Austria en diciembre de 1987 con la Ley de reforma del Código Penal (Contempla delitos como, destrucción de datos, estafa informática); Francia con la Ley número 88-19 de enero de 1988 sobre fraude informático; Estado Unidos con el Acta Federal de Abuso Computacional de 1994, que modifico el Acta de Fraude y Abuso Computacional de 1986 (En relación a los virus, se proscribe la transmisión de un programa, información, códigos o comandos que causan daño a las computadoras, al sistema informático, a las redes, información, datos o programas); entre otros países que regulan el tema de los delitos informáticos. (VELÁZQUES ELIZARRARÁS, 2007)

A nivel Latinoamericano, se ha ido implementando la legislación correspondiente, entre los primeros países se tiene a Bolivia con la Ley número 1768; Argentina con la Ley número 25326 en el año 2000; Chile con La Ley 19223 relativa a Delitos Informáticos.

En el caso del Perú, según refiere (TEMPERINI, 2013) se tiene la Ley 27309 que incorpora al Código Penal los Delitos Informáticos, a través de un artículo único que modifica el Título V del Libro Segundo del Código Penal, promulgado por Decreto Legislativo No 635, introduciendo allí los artículos

207 – A – B y C y 208. Con la Ley 28.251 se actualizó la regulación y se incorpora distintos delitos como los que afectan la integridad sexual, entre ellos, se tipifica la pornografía infantil a través de la modificación del art 183-A. Mediante la Ley 28.493 de 2005, se regula el uso del correo electrónico no solicitado (spam), que no incluye ningún tipo de sanción penal.

Entre los principales delitos informáticos o ciberdelitos regulados, se tiene: El fraude informático o Pharming, amenaza y coacción, falsificación informática, acceso e interceptación informática o Maleare, Delitos contra el honor, delitos sexuales, Interferencia de datos y sistemas, Contra la propiedad intelectual.

Son varios los delitos que se cometen bajo la denominación de delitos informáticos o ciberdelitos, y todos ellos pueden ser cometidos dentro de una red que no reconoce fronteras geográficas, es por ellos que una de las principales características de éste delito es la **transfronterización o transnacionalización,** que según (RODRÍGUEZ GARCÍA, 2019):

> Los Delitos Transnacionales son aquellas acciones u omisiones socialmente peligrosas que tienen una esfera de influencia marcada fuera del ámbito nacional, que, aunque sean reprensibles por el derecho nacional, necesitan de la colaboración internacional para su más efectiva persecución, estén o no en convenios o tratados internacionales.

Desde la perspectiva Penal, los delitos transnacionales deben ser abordados como parte del Derecho Penal Transnacional, el cual se aplica a las normas de cooperación internacional y la asistencia jurídica mutua entre Estados.

Como se puede advertir con lo señalado, los delitos informáticos han alcanzado gran presencia en la sociedad, y dado el carácter de transnacional no resulta suficiente la legislación particular que cada Estado pueda asumir, se requiere de la cooperación internacional a fin de evitar la impunidad en los casos que trascienden a la jurisdicción interna de un país.

Uno de los instrumentos internacionales que permiten la cooperación internacional y la armonización normativa para combatir el cibercrimen; en razón a que corresponde a delitos transfronterizos en la mayoría de los casos, es el Convenio de Budapest. Convenio que tiene por objeto armonizar los tipos penales vinculados a la ciberdelincuencia**,** así como, establecer determinadas reglas procesales necesarias que facilitan la investigación y procesamiento de este tipo de delitos y de aquellos cometidos mediante el uso de un sistema informático o cuyos elementos probatorios se encuentren en formato electrónico; y también busca definir algunas reglas que permitan disponer de un mecanismo rápido y eficaz de cooperación judicial internacional para contribuir a la persecución penal de ese tipo de delitos. El Convenio de Budapest, a la fecha, tienen 55 Estados parte, 43 que son miembros del Consejo

de Europa, 3 que no son miembros del Consejo de Europa y 9 que se han adherido.

En este orden de ideas, aun cuando el Convenio no constituya, en sí mismo, un tratado de derechos humanos ni desarrolle ningún derecho humano en específico, puede afirmarse que promoverá la aplicación de compromisos vinculados a la protección de derechos humanos, pero sobre todo evitara la impunidad ante la comisión de delitos informáticos o ciberdelitos.

1.1.2. Formulación del Problema

1.1.2.1. Problema principal

¿De qué manera la suscripción del convenio de Budapest influye en el tratamiento de los delitos informáticos?

1.1.2.2. Problemas secundarios

- ¿Cuál es el desarrollo legislativo de los delitos informáticos en el Perú?
- ¿Cuál es la problemática actual generada por los delitos informáticos en el Perú?
- ¿Cómo es la legislación de delitos informáticos en países sudamericanos que suscribieron el convenio de Budapest?

- ¿Cuáles son los efectos que produce la suscripción del convenio de Budapest?

1.2. Objetivos de investigación

1.2.1. Objetivo general

Explicar la manera en que la suscripción del convenio de Budapest influye en el tratamiento de los delitos informáticos.

1.2.2. Objetivos específicos

- Describir es el desarrollo legislativo de los delitos informáticos en el Perú.
- Analizar la problemática actual generada por los delitos informáticos en el Perú.
- Analizar la legislación de delitos informáticos en países sudamericanos que suscribieron el convenio de Budapest.
- Identificar los efectos que produce la suscripción del convenio de Budapest.

1.3. Justificación

El presente proyecto de investigación se justifica por las razones siguientes:

a) Conveniencia

Es conveniente realizar esta investigación, por tratarse de un problema que amerita el interés por parte del Estado, el que debe buscar un tratamiento adecuado y con cooperación internacional de los delitos informáticos o ciberdelitos en concordancia con el convenio de Budapest.

b) Relevancia Social

La presente investigación es relevante socialmente, porque afecta a toda la sociedad, debido al gran daño que producen los delitos informáticos y su carácter transnacional, por ende, todo ello desencadena en un grave problema social que necesita ser atendido de manera global.

c) Implicaciones prácticas

A través de esta investigación se busca concientizar a las personas y sobre todo al Estado para que dicte las normas adecuadas y sobre todo establezca políticas adecuadas para frenar la impunidad de los delitos informáticos.

d) Valor teórico

La información que se obtenga de este estudio, permitirá aportar al conocimiento teórico y legislativo del Derecho Penal y el Derecho Penal Transnacional, puesto que se da a conocer alcances sobre los delitos informáticos, y va a servir como base teórica para la refrendación del Convenio de Budapest, a fin de abordar de manera más completa las conductas delictivas relacionadas con el tipo penal denominado ciberdelincuencia.

e) Utilidad Metodológica

Del mismo modo, el resultado de esta investigación va a ser útil a nivel metodológico y va a dar pie a que otras personas interesadas en ampliar su contenido, se sirvan de esta investigación y tomen como un nuevo aporte a la información ya existente sobre el tema.

f) Originalidad

La presente investigación tiene originalidad, debido a que no existe en pregrado en la ciudad de Cusco otras tesis precedentes que hayan abordado la misma materia según nuestros objetivos y con la metodología elegida.

g) Viabilidad

Teniendo en consideración los objetivos trazados y la problemática a ser analizada, consideramos que es posible realizar la presente investigación

1.4. Método

1.4.1. Diseño Metodológico

El diseño de la presente investigación se precisa en el siguiente cuadro:

Cuadro N° 01

Enfoque de la investigación	**Cualitativo:** Puesto que el estudio se basa fundamentalmente en la descripción y la argumentación antes que en mediciones datos estadísticos.
Tipo de Investigación	**Jurídica Descriptiva, Comparativa:** Porque con este tipo de investigación se realizara una investigación descriptiva de los delitos informáticos a raíz de la suscripción del Convenio de Budapest, así como un estudio jurídico comparativo referido a la legislación comparada, orientada a una propuesta normativa (Según Clasificación del (Aranzamendi, 2015)
Nivel de Investigación	**Básica:** Porque se analizará y explicará el desarrollo doctrinario y legislativo de instituciones jurídicas, a fin de contribuir con el desarrollo de la ciencia del Derecho.

Fuente: Elaboración propia

1.4.2. Diseño contextual

- Unidades de estudio

La presente investigación tiene como unidades de estudio a dos categorías: Delitos Informáticos y la suscripción del Convenio de Budapest.

1.4.3. Técnicas e instrumentos de recolección de datos, procesamiento y análisis de datos

1.4.3.1. Técnicas

a. Análisis documental

Utilizar la información cualitativa de documentos escritos, recopilada en artículos científicos, libros, leyes seleccionando los aspectos que interesan a las categorías en estudio.

b. Análisis doctrinal

c. Análisis Jurisprudencial

1.4.3.2. Instrumentos

Se utilizarán los siguientes modelos de instrumento

a. Ficha de análisis documental

- Ficha bibliográfica
- Ficha de información electrónica (información extraída de medios electrónicos, por ejemplo, Internet.)

b. Ficha de análisis doctrinal

c. Ficha de análisis Jurisprudencial y normativo.

1.5. Hipótesis de trabajo

1.5.1. Hipótesis General

La suscripción del convenio de Budapest influye relativamente en el tratamiento de los delitos informáticos, dado que, la principal característica es la cooperación internacional para combatir los mencionados delitos, la misma que tiene mínima aplicación desde la suscripción.

1.5.2. Hipótesis Específicas

- El desarrollo de la legislación sobre delitos informáticos en el Perú ha sido progresivo y rápido, llegando a equipararse con legislación comparada en la materia.

- La problemática actual generada por los delitos informáticos en el Perú es cada vez más creciente, dado que los medios cibernéticos utilizados por los ciberdelincuentes son cada vez más diversos, haciendo difícil su identificación, sumado a ello, el escaso presupuesto destinado a destinado para contar con tecnología de alta gama que permita su persecución.

- Entre los efectos que produce la suscripción del convenio de Budapest, tenemos: La creación de un marco común de derecho penal

sustantivo, la estandarización de procesos penales y la cooperación internacional.

1.6. Categorías de estudio

La presente investigación es de orden cualitativa, por dicha razón y siguiendo la doctrina de la investigación científica se consignan para fines de análisis las categorías de estudios con sus respectivas sub categorías.

Cuadro N° 02

Categorías	Sub categorías
Delitos Informáticos	- Delincuencia Informática - Bien Jurídico Protegido - Sujetos del Delito - Tipos de Delitos Informáticos - Situación Internacional
Convenio de Budapest	• Contenido • Cooperación Internacional • Países suscribientes • Convención de Budapest en Chile y Argentina

Fuente: Elaboración propia

CAPÍTULO II: DESARROLLO TEMÁTICO

SUB CAPÍTULO I

DELITOS INFORMÁTICOS.

2.1. Aspectos Generales

2.1.1. Conceptos Preliminares

2.1.1.1. Informática

En 1945, no había computadores de programa guardado; en 1965, un computador costaba un millón de dólares, no obstante esto cambió por el veloz aumento de las prestaciones y el progreso tecnológico usado en la construcción de computadores y su diseño. (HENNESSY & PATTERSON, 1993).

Según, (HERNÁNDEZ MENDOZA, 2003):

> Informática es la sistematización racional de la información. Consideramos que esta definición ubica a la informática en una actitud más próxima a una ciencia y en torno a la información, pero siempre tratada ésta en forma de sistema o sistemas. Es decir, sistematizar la información es la función básica de la informática, pero deberá hacerse racionalmente, de lo contrario el uso de herramientas que van desde el papel y el lápiz hasta las computadoras más sofisticadas, dependiendo del volumen de datos que se maneje para generar la información y los procedimientos que se establezcan para el procesamiento de los datos.

Conforme se advierte, la informática está vinculada con la información que está almacenada en un computador, que, de acuerdo con la Real Academia Española, es "La máquina eléctrica dotada de una memoria de gran capacidad y de procedimiento de procedimiento de la información, capaz de solucionar inconvenientes aritméticos y lógicos debido a la implementación automática de programas registrados en ella". Un computador funciona a través de programas de ordenador, que vienen a ser las instrucciones expresadas a través de palabras, códigos, susceptibles de ser incorporadas en dispositivos de lecturas automatizadas como un ordenador, a fin de ser procesada. (ZARICH, 2005, p. 29)

2.1.1.2. Sistema Operativo

El sistema operativo es un programa de control de la computadora, que proporciona herramientas o comandos que permiten la interacción con una computadora personal o PC. Según (HERNÁNDEZ MENDOZA, 2003, p. 45): "El sistema operativo es el núcleo de toda actividad de software, monitores y controla toda la entrada y salida, así como la actividad de procesamiento dentro del sistema de computadora".

2.1.1.3. Redes de Computadoras

La red de computadoras, está referida a la interconexión que existe entre estas máquinas, en este sentido se expresa (HERNÁNDEZ MENDOZA, 2003, pp. 84-85) afirmando:

> Conforme las PC se difundieron en los negocios y aparecieron los complejos multiusuarios de software, conectar las PC se convirtió era una meta de las organizaciones. La comunicación de datos, es decir, la comunicación electrónica de información entre computadores se convirtió en el punto esencial para la industria de estas máquinas. El rápido crecimiento de la red mundial de computadoras conocida como internet hizo que la difusión de comunicación de datos se apresurara.

La primera red de computadoras se crea en 1969 y fue desarrollada por el Departamento de Defensa de los Estados Unidos y fue conocida como Arpanet, red de internet que estuvo vigente hasta 1990.

2.1.1.4. Tecnologías de Información y Comunicación

Las nuevas tecnologías de información y comunicación, se resume con las siguientes siglas NTICs. Y comprende:

Las tecnologías y procedimientos para comunicar surgidas en el entorno de la revolución información, “Revolución Telemática”, la Tercera Revolución Industrial, desenvueltas graduativamente a partir de la segunda mitad de los años 70, primordialmente en los años de 1990. La inmensa mayor parte de ellas se caracteriza por precipitar, horizontalizar y tomar menos palpable, es decir, físicamente manejable el contenido de la información, mediante la digitalización y de la comunicación en redes -medida o no por computadores- para la captación, transmisión y repartición de las informaciones: texto, imagen

estética, videos. Se considera que el advenimiento de las nuevas tecnologías y la forma como fueron utilizadas por gobiernos, empresas, individuos y sectores sociales posibilitaran el surgimiento de la "Sociedad de la Información". (VELLOSO, 2011, p. 2)

2.1.2. Conceptualización de Delito Informático

Para acércanos a una conceptualización de Delitos Informativos, debemos tomar en cuenta lo señalado por (PEÑA CABRERA F., 2011):

> "El hombre a fin de satisfacer sus necesidades más elementales y en su afán de obtención de lucro, no solo hace uso de medios lícitos, sino también se sirve de ciertos instrumentos que de forma ilegítima importa un ataque a ciertos bienes jurídicos merecedores de tutela penal. Instrumentos que en la actualidad adquieren ribetes en suma sofisticados, en ventaja al gran desarrollo alcanzando por la ciencia y tecnología, poniendo en vitrina un sistema plenamente informatizado en el funcionamiento de la información en lo cual respeta a datos y otros semejantes.

Ciertamente el avance de la tecnología, permite conocer nuevas conductas cuyas características se particularizan por el uso de medios digitales y que para su investigación requieren técnicas especiales, que en nuestro país están a cargo de la División de Investigación de Delitos de Alta Tecnología (Divindat) de la Policía Nacional.

El Perú no es ajena a esta dinámica mundial. Según (ANDINA, Agencia Peruano de Noticias, 2020): "La División de Investigación de Delitos de Alta Tecnología (Divindat) de la Policía registró 3,012 denuncias de fraudes electrónicos, pornografía infantil, suplantación de identidad y otros delitos informáticos durante el 2019". Lo que genera la necesidad de su estudio.

Según la Organización de Comercio y Desarrollo Económico, los delitos informáticos son: 'Cualquier comportamiento antijurídico, no ético o no autorizado, relacionado con el procesador automático de datos y/o transmisores de datos".

Por su parte, DAVARA RODRÍGUEZ, citado por (MOISÉS BARRIOS, 2017, p. 26) afirma:

> La denominación de delito informático, representa una acción que reuniendo las características que delimitan el concepto de delito, sea llevada a cabo utilizando un elemento informático o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software.

Como se advierte, el delito informático está referido a cualquier conducta de carácter ilegal, no ética, o no autorizada que involucra el procesamiento automático de datos y/o la transmisión de los mismos

2.1.3. Antecedentes de Delitos Informáticos

Los antecedentes de los delitos informáticos van aparejados al desarrollo de las tecnologías informáticas y de comunicación en el ciberespacio, escenario en el que los delincuentes pueden cometer delitos desde cualquier parte del mundo, únicamente accediendo a una computadora, viéndose favorecidos por el anonimato que el ciberespacio le brinda y la gran cantidad de víctimas que se hallan expuestas.

Alguno de los antecedentes facticos que posteriormente darían lugar a la comisión de los delitos en mención, se encuentran los virus informáticos, que según el periodista especializado en tecnología (YÚBAL FM., 2017) son:

1) El **CREEPER.**

   Fue el primer virus informático con carácter demostrativo en ordenadores de ARPANET (Red de computadoras utilizada como medio de comunicación, la primera comunicación con ARPANET se dio entre la Universidad UCLA de California y el instituto de investigación de Stanford el 29 de octubre de 1969), el **CREEPER** (…), fue un programa que podía recorrer una red saltando de un ordenador a otro mientras realizaba una tarea específica.

2) **RABBIR**

El primer virus informático con carácter dañino fue **RABBIR**, que se reproducía haciendo copias de sí mismo en un mismo ordenador hasta obstruir el sistema reduciendo su capacidad de rendimiento, esto provocaba que finalmente quede bloqueado.

Entre los antecedentes normativos de los delitos informáticos, tenemos:

1) **En Estados Unidos**: La propuesta legislativa del senador norteamericano Ribincolf, quien en 1977 presentó su propuesta legislativa para tipificar los delitos informáticos ante el Congreso Federal de los Estados Unidos.

2) **En Paris**: La Organización de Cooperación y Desarrollo Económico, promovió la armonización de legislación penal a nivel internacional, en 1986 realizó una publicación referida a delitos informáticos "Delitos de Informática: análisis de la normatividad jurídica", en la que alcanza su propuesta de reforma legislativa para los Estados -en la ley penal- teniendo en consideración una lista de delitos. Posteriormente, en 1992, éste comité elaboró un conjunto de normas para la seguridad de los sistemas informáticos.

3) **La ONU,** en 1990 se celebra en la Habana Cuba el Octavo Congreso sobre Prevención del Delito y Justicia Penal; se dijo "L delincuencia relacionada con la informática era consecuencia del mayor empleo del proceso de datos en las economías y burocracias de los distintos

países y que por ello se había difundido la comisión de actos delictivos" (ACURIO DEL PINO, pág. 31)

4) **La ONU**, con el Manual de las Naciones Unidas para la Prevención y Control de Delitos Informáticos, al respecto (ACURIO DEL PINO, pág. 32) señala: "Cuando el problema se eleva a la escena internacional, se magnifican los inconvenientes y las insuficiencias, por cuanto los delitos informáticos constituyen una nueva forma de crimen transnacional y su combate requiere de una eficaz cooperación internacional concertada".

2.1.4. Tipos de Delitos Informáticos

Para abordar los tipos de delitos informáticos, se ha considerado oportuno tener en consideración aquellos reconocidos por la Organización de Naciones Unidas y aquello contemplados en el Convenio de Ciberdelincuencia de Budapest:

2.1.4.1. Organización de Naciones Unidad ONU

2.1.4.2. Fraude cometido mediante manipulación de computadoras

2. Falsificaciones informáticas
3. Daño o modificaciones de programas o datos computarizados
4. Acceso no autorizado a servicios y sistemas informáticos

2.1.4.3. Convenio de Ciberdelincuencia o Convenio de Budapest

Título 1- Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos:

- Artículo 2 Acceso ilícito

- Artículo 3 Interceptación ilícita
- Artículo 4 Ataque a la integridad de datos
- Artículo 5 Ataques a la integridad del sistema
- Artículo 6 Abuso de los dispositivos

Título 2 Delitos informáticos

- **Artículo 7 Falsificación informática**
- **Artículo 8 Fraude Informático**

Título 3 Delitos relacionados con el contenido

- Artículo 9 Delitos relacionados con la pornografía infantil

Título 4 Delitos relacionados con infracción de la propiedad intelectual y de los derechos afines

- Artículo 10 Delitos relacionados con infracciones de la propiedad intelectual y de derechos afines.

Precisada la clasificación de delitos reconocidos por la ONU y aquellos contemplado en el Convenio de Ciberdelincuencia, nos corresponde referirnos a los mismos -**delitos informáticos-**, por ser materia de análisis de la presente investigación.

Tipos de delitos informáticos según la ONU

- **Fraude cometido mediante manipulación de computadoras**
- **Falsificaciones informáticas**
- Daño o modificaciones de programas o datos computarizados
- Acceso no autorizado a servicios y sistemas informáticos

Tipos de delitos informáticos según el Convenio de Budapest (Título 2 Delitos informáticos).

- **Artículo 7 Falsificación informática**
- **Artículo 8 Fraude Informático**

2.1.4.4. Falsificación Informática

Referido a: "(…), la introducción, alteración, borrado o supresión deliberados e ilegítimos de datos informáticos que genere datos no auténticos, con independencia de que los datos sean legibles e inteligibles directamente. (artículo 7 del Convenio de Budapest).

Según la ONU, la falsificación informática cuenta con una sub clasificación:

> Falsificación informática como objeto. Cuando se alteran datos de los documentos almacenados en forma computarizada.
>
> Falsificación informática como instrumento. Cuando se efectúan falsificaciones de documentos de uso comercial haciendo uso de las computadoras.

Por citar un ejemplo se tiene la legislación francesa, que prevé la falsificación de documentos informáticos en el artículo 462 -5, el dicho artículo se sanciona a quien de cualquier modo falsifique documentos informatizados con intensión de causar un perjuicio a otro.

2.1.4.5. Fraude Informático o Pharming

Referido a: "(…), los actos deliberados e ilegítimos que causen perjuicio patrimonial a otra persona mediante: a) La introducción, alteración, borrado o supresión de datos informáticos; b) Cualquier interferencia en el

funcionamiento de un sistema informático" (artículo 8 del Convenio de Budapest).

El **Pharming**, asociado al lhishing, es:

> Un tipo de fraude informático que ha aparecido desde mediados de la década pasada, cuya finalidad común es la de apoderarse de información personal de un usuario de Internet, para acceder a sus cuentas de correo o de redes sociales y obtener adicionalmente datos de sus contactos virtuales, a fin de comercializarlos ilícitamente, o bien, conseguir claves de "e-banking" para de este modo ingresar a las cuentas corrientes bancarias de los titulares y disponer del dinero que en ellas se encuentra, realizando una operación de transferencia de activos a un tercero que se denomina "mule". (OXMAN, 2013, pág. 216)

Según lo previsto por la Organización de Naciones Unidas que reconoce como delito al fraude cometido mediante manipulación de computadoras, el fraude puede ser cometido:

> Mediante manipulación de computadoras. Conocido también como sustracción de datos, representa el delito informático más común ya que es fácil de cometer y fácil de descubrir. Este delito no requiere de conocimientos técnicos de informática y puede realizarlo cualquier persona que tenga acceso a las funciones normales de procesamiento de datos en la fase de adquisición de los mismos. (HALL, s.f.)

> Manipulación de Programas: (…). Consiste en modificar los programas existentes en el sistema de computadoras o en insertar nuevos programas o

nuevas rutinas. Un método común utilizado por las personas que tienen conocimientos especializados en programación informática es del denominado Caballo de Troya, que consiste en insertar instrucciones de computadora de forma encubierta en un programa informático para que pueda realizar una función no autorizada al mismo tiempo que su función normal. (HALL, s.f.)

Manipulación de datos de salida. Se efectúa fijando un objetivo al funcionamiento del sistema informático. El ejemplo más común es el fraude de que se hace objeto a los cajeros automáticos mediante la falsificación de instrucciones para la computadora en la fase de adquisición de datos. Tradicionalmente esos fraudes se hacían a base de tarjetas bancarias robadas; sin embargo, en la actualidad se usan ampliamente equipos y programa de computadora especializados para codificar información electrónica falsificada en las bandas magnéticas de las tarjetas bancarias y las tarjetas de crédito.

Por su parte, (KATERIN, 2019) agrega los delitos informáticos específicos, entre los que se tiene al **sexting,** consiste en enviar mensajes, fotos o videos de contenido erótico y sexual a través del dispositivo móvil mediante redes sociales o una aplicación de mensajería instantánea. El **Grooming,** delito que consiste en realizar acciones y conductas realizadas por un adulto, que actuando en anonimato busca a tomar videos o imágenes de un menor de edad. Las **Extorciones**, Delito que consiste en obligar a una persona, utilizando la violencia, amenaza e intimidación, a realizar u omitir realizar un negocio jurídico con ánimo de lucro y generar perjuicio. El **Pheraking**, delito que

consiste en acceder a redes sociales utilizando cuentas ajenas para realizar llamadas telefónicas.

Como ejemplo en legislación comparada, el profesor español (ACURIO DEL PINO, pág. 41) refiriéndose a la legislación ecuatoriana señala:

> El nuevo Código Penal introduce el concepto de fraude informático, consistente en la manipulación informática o artificio similar que, concurriendo ánimo de lucro, consiga una transferencia no consentida de cualquier activo patrimonial en perjuicio de tercero. El Código Penal anterior exigía la concurrencia de engaño en una persona, lo cual excluía cualquier forma de comisión basada en el engaño a una máquina. Los Arts. 248 y siguientes establecen una pena de prisión de 6 meses a 4 años para los reos del delito de estafa, pudiendo llegar a 6 años si el perjuicio causado reviste especial gravedad.

2.1.5. Bien Jurídico Protegido

A fin de identificar el Bien Jurídico Protegido en los Delitos Informáticos, tomaremos en cuenta lo descrito por (VILLAVICENCIO TERREROS, 2014):

> El bien jurídico tutelado en los delitos informáticos se concibe en los planos de manera conjunta y concatenada; 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 a través de este tipo de delitos como son la indemnidad sexual, intimidad, etcétera (…).

> En este tipo de delitos no se puede establecer a la información como el único bien jurídico afectado, por ser el principal y el más importante; sino a un conjunto de bienes que son afectados, debido a la característica de la conducta típica en esta modalidad delictiva que colisiona con diversos intereses colectivos. En ese sentido que coincidimos con María Luz Gutiérrez Francés, quien señala que es un delito pluriofensivo, sin perjuicio de que uno de tales bienes este independientemente tutelado por otro tipo penal.

En efecto, los bienes jurídicos afectados son diversos por ser un delito de tipo pluriofensivo, lo que significa tener cuidado en la descripción de cada conducta ilícita señala en la normativa pertinente.

2.1.6. Sujetos del Delito

2.1.6.1. Sujeto Activo

Para los delitos informáticos no se requiere de una cualidad especial para ser considerado sujeto activo; a decir de (PEÑA CABRERA FREYRE, 2011):

> Basta con que se cuente con ciertos conocimientos propios de la informática para realizar la conducta prohibida. Resulta admisible apreciar una autoría mediata, cuando el hombre de atrás se aprovecha de la buena fe del hombre de adelante, del instrumento quien, sin dolo, desconociendo la naturaleza de los actos que está cometiendo, ingresa de forma indebida a una red o base de datos.

Cabe recalcar que no se puede considerar como sujeto activo a personas jurídicas solo naturales; pero que, sin embargo, si está implicado una persona jurídica esta puede ser pasible de consecuencias accesorias descritas en el Código Penal en el artículo 105°.

2.1.6.2. Sujeto Pasivo

Puede considerarse cualquier persona, sea natural o jurídica, estatales o privados.

A decir de (VILLAVICENCIO TERREROS, Delitos Informáticos, 2014), citando a Gutiérrez Francés señala que: "El sujeto pasivo por excelencia del ilícito informático es la persona jurídica, debido al tráfico económico en el que desarrollan sus actividades, por ello son los sectores más afectados por la criminalidad mediante computadoras. Y entre ellos están: la banca, las instituciones públicas, la industria de transformación, etcétera".

2.1.7. Legislación de delitos informáticos en países de Sudamérica

2.1.7.1. Chile

En relación a la situación de delitos informáticos en el país de Chile, consideramos el estudio realizado por (CARO MARTÍNEZ, 2010), quien señala:

Chile fue el primer país latinoamericano en sancionar una Ley contra Delitos Informáticos. La Ley 19223, publicada en el Diario Oficial el 7 de junio de 1993, en un corto articulado tipifica y sanciona la destrucción o inutilización de un sistema de tratamiento de información.

Le Ley pretende proteger un nuevo bien jurídico surgido en el uso de las modernas tecnologías computacionales: calidad, la pureza e idoneidad de la información en cuanto tal, contenida en un sistema automatizando de tratamiento de ésta, y de los productos que de su operación se obtengan.

No obstante, no sólo se protege ese bien, sino que además concurren otros, tales como: el patrimonio, la privacidad, la intimidad y la confidencialidad; la seguridad y fiabilidad y tráfico jurídico y probatorio; el derecho de propiedad sobre la información y sobre los elementos físicos.

La Ley contempla cuatro artículos que, si bien corresponden cada uno a un tipo de conducta distinta, se pueden clasificar en dos grandes figuras delictivas: el sabotaje informático y el espionaje informático.

El sabotaje informático (artículo 1° y 3°) comprende aquellas conductas tipificadas atendiendo al objeto que se afecta o atenta con la acción delictual, y que puede ser un sistema de tratamiento de la información o a sus partes componentes, en funcionamiento de un sistema de tratamiento de la información, o los datos contenidos en un sistema automatizado de tratamiento

de la información. El atentado a estos objetos puede ser a través de su destrucción, inutilización, obstaculización o modificación.

El espionaje informático (artículo 2° y 4°) comprende aquellas figuras delictivas que atienden al modo operativo ejecutable y pueden ser, en primer lugar, delitos de apoderamiento, uso o conocimientos indebidos de la información, cometidos interfiriendo, interceptando o meramente accediendo al sistema de tratamiento de datos. Estas figuras corresponden a lo conocido comúnmente como hacking. En segundo lugar, comprende también delitos revelación indebida y difusión de datos contenidos en un sistema de tratamiento de la información.

2.1.7.2. Colombia

Al respecto, (CARO MARTÍNEZ, 2010), señala:

> En la década pasada se consideraba, tanto en el campo nacional como en el universal, que la inseguridad jurídica respecto del costo probatorio de los mensajes de datos era el primordial inconveniente para el desarrollo del negocio electrónico y que su regulación, por consiguiente, era un tema de suma trascendencia. La expedición de la ley 527 de 1999 obedeció a esta necesidad jurídica a las transacciones electrónicas.

En la regulación de los medios electrónicos para la ley 527 el legislador, con fines de adaptar el régimen jurídico existente a las nuevas realidades, creó el

criterio del equivalente funcional. Dicho criterio puede ser enunciado como sigue:

> Si un mensaje da datos cumple con los mismos objetivos y tiene las mismas funciones que un medio tradicional o físico de transmisión de información, dicho mensaje tendrá los mismos efectos jurídicos que dicho medio físico". En ese sentido, no pueden negarse efectos jurídicos, validez o fuerza a cierta información por el solo hecho de que esté en forma de mensaje de datos. (…).

El delito informático en Colombia no está tipificado expresamente como una categoría delictiva individual y autónoma. El Código Penal de Colombia cuenta con un exclusivo artículo, el 195, que bajo el epígrafe de "acceso abusivo de un sistema informático" (hanking en otras legislaciones), instituye una sanción multa, sin especificar la cuantía, para quienes abusivamente se introduzcan en un sistema informático salvaguardado con medida de estabilidad o se mantenga contra la voluntad de quien tiene derecho a excluirlo.

Es fundamental considerar que, sin perjuicio de existir o no una definición de qué es o qué no es un delito informático, el Código Penal trae definidos, delimitados y regulados muchísimos delitos propensos de ser realizados en un ámbito informático. Y, es allí precisamente, donde el juzgador y los investigadores deben encontrar relación, con fines de evitar la impunidad en cuanto a la ciberdelincuencia.

2.1.7.3. Argentina

El 4 de junio de 2008 mediante Ley 26388 se modificó el Código Penal Argentino para incluir delitos informáticos sus respectivas penas, teniendo en su contenido temas como: Distribución y tenencia con fines de distribución de pornografía infantil; violación de correos electrónicos; acceso ilegítimo a sistemas informáticos; daño informático y distribución de códigos maliciosos; interrupción de comunicaciones o DoS.

Posteriormente, el 4 de diciembre de 2013 se publicó la Ley Grooming, Ley N° 26904, que responde a una necesidad de proteger a menores de edad en la comunicación cibernética; siendo así, se incorporó en el Código Penal artículo 131, que sanciona a personas que, por medio de comunicaciones electrónicas, telecomunicaciones o cualquier otra tecnología de transmisión de datos, contacta a una persona menor de edad, con el propósito de cometer cualquier delito contra la integridad sexual de la misma.

2.1.8. Naciones Unidas y Delitos Informáticos (Manual de las Naciones Unidas para la Prevención y Control de Delitos Informáticos)

En 1994, la Organización de las Naciones Unidas aprueba el Manual sobre la prevención y control de delitos informáticos, en cuyo contenido se aprecia cinco modalidades más comunes de delitos informáticos, i) El fraude por manipulación; ii) La falsificación informática; iii) Los daños o modificaciones de los datos informáticos o programas, o sabotaje informático;

iv) Acceso no autorizado a sistemas informáticos y de servicio; v) Reproducción no autorizada de programas informáticos legalmente protegidos.

En atención a éste manual, la Organización de Naciones Unidas estableció que los Estados asuman mecanismos de control social y de poder a fin de prevenir, disminuir la criminalidad asociada a delitos informáticos.

Según refiere el profesor chileno (OXMAN, 2013):

> En el Manual de las Naciones Unidas sobre Prevención y Control de Delitos Informáticos se señaló que el potencial de la delincuencia informática es tan amplio como el de los propios sistemas internacionales de telecomunicaciones. Como era de esperar, la palabra "Internet" aparecía solo una vez en el Manual y la palabra "ciberdelincuencia" no se utilizó; sin embargo, las conclusiones demostraron una gran visión de futuro.

Agrega el autor citado, "Si bien el Manual centró su atención en el concepto de "delito informático", es bien sabido que hoy en día la "ciberdelincuencia" recurre efectivamente a las tecnologías globalizadas de la información y las comunicaciones, en particular a Internet, para la comisión de actos delictivos de alcance transnacional"

En el Manual en mención se advierte que desde 1994 la Organización de las Naciones Unidas preveía algunos tipos de delitos informáticos que el Internet traía consigo; a la postre aparecerían además otros tipos de delitos informáticos, dando surgimiento a la denominación de "ciberdelincuencias",

que sin ser propiamente jurídica ha permitido comprender a los diferentes tipos de delitos informático.

SUB CAPÍTULO II

CONVENIO DE BUDAPEST.

2.2. Convenio de Budapest

2.2.1. Antecedentes

Ante el panorama de cibercriminalidad la comunidad internacional reaccionó con una serie de conferencias, convenciones, congresos y eventos internacionales, que derivaron en acuerdos, criterios, principios y medidas a fin de dar solución a los problemas generados por las nuevas conductas delictivas, ya que por el carácter transnacional de estos delitos y la posibilidad de cometerlos desde cualquier parte del mundo, ya sea porque son cometidos por personas que operan en diferentes países, porque las víctimas están en un país distinto o porque la prueba está alojada en servidores ubicados en países distintos al que lleva adelante la investigación lo que provoca una serie de problemas como son los de la legislación y la jurisdicción aplicable al caso.

A su vez, esto dio impulso a que hayan surgido iniciativas de regulación por parte de organismos internacionales. En este sentido, la idea se remonta a 1989, una vez que el Consejo del continente Europeo divulgó una secuencia de sugerencias sobre la necesidad de que el derecho penal sustantivo para penalizar las conductas dañinas realizados por medio de redes informáticas. En 1997 el Consejo del continente Europeo conformó un Comité de Profesionales sobre la delincuencia en el ciberespacio para escribir una convención para facilitar la cooperación de los Estados en la indagación y persecución de los delitos informáticos y para conceder una solución a los inconvenientes de la delincuencia cibernética por medio de la adopción de una herramienta jurídico mundial.

Ya en su 109 junta la junta de Ministros del Consejo del continente Europeo, determinaron aprobar el 23 de noviembre del año 2001 el "Convenio de Budapest" la cual se promovió con miras a la prevención de la cibercriminalidad en el ciberespacio, en especial mediante una legislación idónea y uniforme, de manera tal que las conductas sancionables sean pasibles de ser investigadas por cualquier persona de los Estados integrante, y el 1 de marzo de 2006 entró en vigor el Protocolo Adicional a la Convención sobre el delito cibernético. Los estados que lo han ratificado deben penalizar la difusión de propaganda racista y xenófoba a través de los sistemas informáticos, así como amenazas racistas y xenófobos cometidos mediante medios informáticos.

Es así que, por medios del reconocimiento de la necesidad de cooperación entre Estados para la lucha contra la cibercriminalidad, a fin de proteger los intereses de la sociedad ligado al desarrollo de las tecnologías de información se planteó como objetivo en el convenio la introducción de las conductas pasibles de sanción penal como ilícitas, así como adoptar procedimientos idóneos para la investigación y sanción de dichos ilícitos.

En conclusión, La Convención de Budapest, es actualmente el único instrumento internacional que aborda de manera específica el tema de cibercrimen y hace frente a los delitos informáticos y los delitos en Internet mediante la armonización de leyes entre naciones para procesar a los delincuentes cibernéticos y representa un importante intento de regular el ciberespacio.

2.2.2. Definición

La penetración de las redes informáticas trajo consigo los ciberataques que hoy, de acuerdo con el Informe de Riesgos Mundiales 2019, se encuentran entre las amenazas globales más graves del planeta (Banco Interamericano de Desarrollo, 2016).

De ahí que el concepto de ciberdelincuencia se convirtiera en una preocupación para los gobiernos de todo el mundo, Cabe señalar que el convenio no define explícitamente el concepto de ciberdelincuencia, pero sí establece los tipos de cibercrimen que los países deben tipificar en sus

legislaciones. Entre estos, son de gran importancia por su impacto y frecuencia, los delitos informáticos reseñados en el Titulo II:

Falsificación informática: hace referencia a la introducción, alteración, borrado o supresión, deliberada y de forma ilegítima, de datos informáticos que dé lugar a datos no auténticos, "con la intención de que sean tenidos en cuenta o utilizados a efectos legales como si se tratara de datos auténticos".

Fraude informático: son los actos deliberados e ilegítimos que causen perjuicio patrimonial a otro mediante la introducción, alteración, borrado o supresión de datos; o causándole interferencias en el funcionamiento de sus sistemas informáticos.

Los delitos informáticos mencionados líneas arriba son de gran importancia, sin embargo, de alguna manera ya han sido tratados en la legislación peruana, por otro lado, hay temas novedosos para nuestra legislación como la estandarización de procesos penales y la cooperación internacional.

2.2.3. Contenido

El Convenio contiene un Preámbulo y un total de cuarenta y ocho artículos distribuidos en cuatro capítulos, divididos en secciones y títulos, de la siguiente forma: (convenio, 2001)

- Preámbulo

- Capítulo I – Terminología
- Capitulo II – Medidas Que Deben Adoptarse A Nivel Nacional
    - Sección 1 – Derecho Penal Sustantivo
        - Titulo 1 - Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos
        - Titulo 2 - Delitos Informáticos
        - Titulo 3- Delitos relacionados con el contenido
        - Titulo 4 - Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines
        - Titulo 5 - oras formas de responsabilidad y de sacian
    - Sección 2 – Derecho Procesal
        - Titulo 1 - Disposiciones Comunes
        - Titulo 2 - Conservación rápida de datos informáticos almacenados
        - Titulo 3 - Orden de Presentación

- Titulo 4 - Registro y confiscación de datos informáticos almacenados
- Titulo 5 - Obtención en tiempo real de datos informáticos

- Sección 3- Jurisdicción

- Capitulo III– Cooperación Internacional
  - Sección 1 – Principios Generales
    - Titulo 1 - Principios Generales Relativos a la cooperación Internacional
    - Titulo 2 - Principios relativos a la extradición
    - Titulo 3 - Principios relativos a la asistencia mutua
    - Titulo 4 - Procedimientos relativos a la solicitud de asistencia mutua en ausencia de acuerdos internacionales aplicables
  - Sección 2 – disposiciones Específicas
    - Titulo 1 - Asistencia mutua en materia de medidas provisionales

- Titulo 2 - Red 24/7
- Titulo 3 - Asistencia mutua en relación con los poderes de investigación.

- Capitulo IV – Clausulas Finales Firma Y Entrada En Vigor

El primer capítulo tan únicamente comprende un precepto, referido a la terminología utilizada en el escrito; El capítulo segundo «Medidas que deberán adoptarse a grado nacional», incluye recursos tanto de Derecho material (responsabilidad penal, tentativa, complicidad) como procesal (procedimiento, salvaguardas, datos, registros, jurisdicción); El tercer capítulo tiene las reglas de cooperación mundial, que son normas de cooperación para averiguar cualquier delito, ya sean delitos clásicos o informáticos. Incluye, entre otras, disposiciones acerca de la localización de sospechosos, recolección o envío de evidencia digital, e incluso lo referente a extradición; El cuarto Capitulo trata de Formalidades para la firma y entrada en vigor, la adhesión, las reservas, la solución de controversias y la denuncia del tratado, entre otros.

2.2.4. Temas regulados en el Convenio de Ciberdelincuencia o

Los temas que forman parte del Convenio son:

Los delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos (Capítulo II). El Artículo 2, se refiere al acceso ilícito; el Artículo 3, se refiere a la Interceptación ilícita; el Artículo 4, referido

al ataque a la integridad de datos; en el Artículo 5, se prevé los ataques a la integridad del sistema; el Artículo 6, está referido al Abuso de los dispositivos

También, se precisan los Delitos informáticos, en el artículo 7 la Falsificación informática, y en el artículo 8 el Fraude Informático. Por su parte, el Título 3 contempla los delitos relacionados con el contenido, entre los que se encuentran los delitos relacionados a pornografía infantil (Artículo 9); los delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines (Artículo 10); En el artículo 11 se prevé la tentativa y la complicidad, en el artículo 12 la responsabilidad de las personas jurídicas.

En los artículos 16 y 17 se prevé la conservación rápida de los datos informáticos almacenados por las autoridades competentes de cada Estado; los artículos 19 y 20 se refieren al registro y confiscación de datos informáticos almacenado y a la obtención en tiempo real de datos relativos al tráfico, respectivamente.

En el Capítulo III pudimos encontrar los principios en general relativos a la cooperación universal en el artículo 23; la extradición en el artículo 24; principios relativos a la ayuda recíproca en el artículo 25; en el artículo 27 se prevé lo relativo al método frente a demandas de ayuda recíproca en ausencia de consenso universal aplicable; en el artículo 35 se hace mención a la Red 24/7 con el objeto de: "(…), asegurar una ayuda instantánea para indagaciones que se relacionan con delitos vinculados a sistemas y datos informáticos, (…)". Al

final, en el artículo 39 se hace mención a los efectos del pacto, como: Si 2 o más piezas han celebrado ya un convenio o tratado relativo a las preguntas contempladas en el presente acuerdo, o si lo realizan el en futuro, lo harán en consecuencia no sea incompatible con las metas y inicios del convenio. Nada de lo dispuesto en el Convenio afectará a otros derechos, restricciones, obligaciones y responsabilidades de cada parte.

2.2.5. Países suscribientes

El Convenio de Budapest (COUNCIL OF EUROPE PORTAL, 2020) sobre la Ciberdelincuencia fue redactado por los 43 países miembros del Consejo de Europa, a la fecha cuenta con 65 Estados Parte (total de ratificaciones), provenientes de todos los continentes como refleja en los siguientes cuadros:

Cuadro N° 03

Estados miembros del Consejo de Europa

NRO	Estado	Firma	Ratificación	Entrada en Vigor
1	Albania	23/11/2001	20/06/2002	01/07/2004
2	Andorra	23/04/2013	16/11/2016	01/03/2017
3	Armenia	23/11/2001	12/10/2006	01/02/2007
4	Austria	23/11/2001	13/06/2012	01/10/2012
5	Azerbaiyán	30/06/2008	15/03/2010	01/07/2010
6	Bélgica	23/11/2001	20/08/2012	01/12/2012
7	Bosnia y Herzegovina	09/02/2005	19/05/2006	01/09/2006
8	Bulgaria	23/11/2001	07/04/2005	01/08/2005
9	Croacia	23/11/2001	17/10/2002	01/07/2004

10	Chipre	23/11/2001	19/01/2005	01/05/2005
11	República Checa	09/02/2005	22/08/2013	01/12/2013
12	Dinamarca	22/04/2003	21/06/2005	01/10/2005
13	Estonia	23/11/2001	12/05/2003	01/07/2004
14	Finlandia	23/11/2001	24/05/2007	01/09/2007
15	Francia	23/11/2001	10/01/2006	01/05/2006
16	Georgia	01/04/2008	06/06/2012	01/10/2012
17	Alemania	23/11/2001	09/03/2009	01/07/2009
18	Grecia	23/11/2001	25/01/2017	01/05/2017
19	Hungría	23/11/2001	04/12/2003	01/07/2004
20	Islandia	30/11/2001	29/01/2007	01/05/2007
21	Italia	23/11/2001	05/06/2008	01/10/2008
22	Letonia	05/05/2004	14/02/2007	01/06/2007
23	Liechtenstein	17/11/2008	27/01/2016	01/05/2016
24	Lituania	23/06/2003	18/03/2004	01/07/2004
25	Luxemburgo	28/01/2003	16/10/2014	01/02/2015
26	Malta	17/01/2002	12/04/2012	01/08/2012
27	Mónaco	02/05/2013	17/03/2017	01/07/2017
28	Montenegro	07/04/2005	03/03/2010	01/07/2010
29	Países Bajos	23/11/2001	16/11/2006	01/03/2007
30	Noruega	23/11/2001	30/06/2006	01/10/2006
31	Polonia	23/11/2001	20/02/2015	01/06/2015
32	Portugal	23/11/2001	24/03/2010	01/07/2010
33	República de Moldavia	23/11/2001	12/05/2009	01/09/2009
34	Rumania	23/11/2001	12/05/2004	01/09/2004
35	Serbia	07/04/2005	14/04/2009	01/08/2009
36	República Eslovaca	04/02/2005	08/01/2008	01/05/2008
37	Eslovenia	24/07/2002	08/09/2004	01/01/2005
38	España	23/11/2001	03/06/2010	01/10/2010
39	Suiza	23/11/2001	21/09/2011	01/01/2012
40	República de Macedonia	23/11/2001	15/09/2004	01/01/2005
41	Turquía	10/11/2010	29/09/2014	01/01/2015
42	Ucrania	23/11/2001	10/03/2006	01/07/2006
43	Reino Unido	23/11/2001	25/05/2011	01/09/2011

Fuente:https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=oJ83l4Km

Por otro lado, el Convenio permite que los Estados que no son parte del Consejo de Europa, puedan adherirse al mismo, para que puedan enfrentar a las amenazas a la seguridad informática.

Siguiendo el ejemplo del punto anterior, enumero en el siguiente cuadro a los estados no miembros del Consejo de Europa que se han adherido al convenio de Budapest.

Cuadro N° 04

Estados no miembros del Consejo de Europa

NRO	Estado	Firma	Ratificación	Entrada en Vigor
1	Argentina		05/06/2018	01/10/2018
2	Australia		30/11/2012	01/03/2013
3	Behin			
4	Brasil			
5	Bukina faso			
6	Cabo Verde		19/06/2018	01/10/2018
7	Canadá	23/11/2001	08/07/2015	01/11/2015
8	Chile		20/04/2017	01/08/2017
9	Colombia	22 /06/2018		
10	Costa Rica		22/09/2017	01/01/2018
11	Dominica		07/02/2013	01/06/2013
12	Ghana			
13	Guatemala			
14	Israel		09/05/2016	01/09/2016
15	Japón	23/11/2001	03/07/2012	01/11/2012
16	Mauricio		15/11/2013	01/03/2014
17	Marruecos		26/06/2018	01/10/2018
18	México			

19	Níger			
20	Nigeria			
21	Panamá		05/03/2014	01/07/2014
22	Paraguay		30/07/2018	01/11/2018
23	Perú		01/12/2020	01/12/2020
24	Filipinas		28/03/2018	01/07/2018
25	Senegal		16/12/2016	01/04/2017
26	Sudáfrica			
27	Sri Lanka		29/05/2015	01/09/2015
28	Tonga		09/05/2017	01/09/2017
29	Túnez			
30	Estados Unidos	23/11/2001	29/09/2006	01/01/2007

Fuente:https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=oJ83l4Km

2.2.6. Convención de Budapest y América Latina

En relación a las naciones del territorio de Latinoamérica, al 1 de noviembre de 2018, el Acuerdo ya ha sido ratificado y entró en vigor para los Estados de Argentina, Chile, Costa Rica, República Dominicana, Panamá y Paraguay; y ha sido ratificado y entrará en vigor a comienzos del año 2019 para Colombia. Los países mencionados previamente adecuaron su legislación interna, en los casos que fue requerido, y cumplieron con los procedimientos establecidos por el Convenio para su adhesión. Un caso a resaltar es el de Argentina, territorio invitado por el Consejo del continente Europeo el 27 de septiembre de 2017 para unirse al Pacto, y que para quincena de diciembre del mismo año su congreso ya había aprobado la incorporación al Pacto, para al final pegarse con el depósito del instrumento que corresponde el 5 de junio de 2018. A partir del 1 de octubre de 2018 el Pacto está en vigor para aquel

territorio. Por otra parte, Brasil fue invitado el 10 de mayo de 2017, encontrándose en proceso de cumplir los requisitos para la adhesión; México no tiene avances en la adhesión por intereses internos que no le permiten dar el paso para modernizar su legislación nacional; Bolivia, Ecuador, Venezuela y otros países aún no han mostrado interés o avances para una futura adhesión al Convenio de Budapest sobre la Ciberdelincuencia.

Por otro lado, el 30 de enero de 2019, el Pleno del Congreso del Perú, de manera unánime, aprobó la suscripción del Acuerdo de Budapest, el cual ha sido Aprobado el por medio de Resolución Legislativa N°30913, del 12 de febrero de 2019; para que en lo subsiguiente el señor Mandatario de la República ratificara por medio del Decreto Supremo N° 010-2019-RE, del 9 de marzo de 2019.

2.2.7. Influencia del Convenio de Budapest en Perú

El Convenio de Budapest sobre la Ciberdelincuencia trae una secuencia de relevantes beneficios para los Estados Parte que hicieron constancia mundial de su consentimiento a obligarse por esta herramienta mundial. Con base a lo estipulado en el Pacto, se rescata los primordiales beneficios para los Estados Parte del Acuerdo son los próximos.

- Ejercer una política penal común con objeto de defender a la sociedad ante la ciberdelincuencia, por medio de la adopción de una legislación correcta.
- Utilizar herramientas establecidas en el mismo Acuerdo para prevenir delitos que pongan en peligro o abusen de sistemas y datos informáticos.
- Conseguir cooperación en materia penal instantánea y fiable, lo cual fortalecerá las habilidades de detección, averiguación y sanción de los Estados Parte para la contienda positiva contra los delitos previstos en los artículos del capítulo II del Acuerdo.

Ahora que el Perú ha ratificado el acuerdo Budapest, seria parte de las ventajas descritos líneas arriba, además iniciaría con el proceso de utilización del Pacto, como ha ocurrido ya en otros territorios, por esto resulta fundamental desarrollar el efecto que esta van a tener en el cumplimiento de sus fines, y cabe preguntarnos de qué forma o forma el acuerdo perjudicara en la ley de los delitos informáticos del Perú, y si ello mejorará el procedimiento de los delitos informáticos.

Para eso nos centraremos en desarrollar las metas que tiene el acuerdo de Budapest; (1) el implantar una política penal común para defender a la sociedad mundial ante la cibercriminalidad, (2) conseguir una legislación específica, (3) la construcción de nuevos mecanismos de cooperación multinacional ante los delitos cibernéticos.

2.2.7.1.Marco Común De Derecho Penal Sustantivo

En todos los casos en los cuales el Pacto de Budapest ha elaborado propuestas de tipificación, se han desarrollado o modificado reglas en el territorio en relación con el mismo objetivo. Por lo general, las reglas peruanas poseen una redacción parecida, incluyendo puntos clave como la necesidad de que los delitos sean realizados "deliberada e ilegítimamente" e inclusive usando los mismos verbos rectores (infringir, generar, dar a conocer, alterar, suprimir, etcétera.). En realidad, lo que se observa es más bien una ampliación de términos pues en varios delitos se agregan acciones más allá de lo sugerido por el Convenio (introducir, clonar, etc.).

Además, la Ley N° 30096 introduce en la categoría de delitos informáticos otras conductas que no estuvieron contempladas en el texto final de Budapest, pero que han sido desarrolladas posteriormente a través de sus protocolos. Este es la situación de: Proposiciones a chicos, chicas y jóvenes con objetivos sexuales por medios tecnológicos (grooming), tráfico ilegal de datos individuales y la modificación de los artículos 162 (Interferencia telefónica) y 323 (Discriminación e incitación a la discriminación) del Código Penal para que incluyan como agravante la utilización de medios informáticos o Internet. Esto último no está exento de determinada disputa, sin embargo en términos prácticos no perjudica en nada la futura utilización del Acuerdo, toda vez que entre los recientes adherentes se discuten protocolos para tipificar nuevos

delitos como el discurso de odio y la xenofobia por medio de medios informáticos.

Podría decirse entonces que la creación de un marco común de derecho penal sustantivo es una tarea bastante avanzada en el Perú, pero haber llegado a dicha situación ha requerido superar varios obstáculos. Al menos a partir de 2010, el interés por regular las situaciones en relación a los delitos informáticos produjo diversas iniciativas legislativas que fueron materia de enormes debates entre los actores del ecosistema digital. La definición misma de "delitos informáticos" es problemática en tanto que no existe acuerdo en si esta debe comprender solo a los delitos en donde el bien jurídico es la información o bien informático o integrar además a los delitos habituales realizados por medio de medios informáticos. Ejemplificando, no en todos los casos se había cuidado la redacción y se castigaba conductas usuales en Internet como la construcción de bases de datos o actividades inofensivas y potencialmente beneficiosas como el ethical hacking. Diferentes expertos criticaron estos problemas en su momento y señalaron la distancia que existía en perjuicio del país entre dicha norma y el estándar propuesto por el Convenio de Budapest. Recién con las modificaciones introducidas por la Ley N° 30171 publicada en 2014 se mejoró la redacción y se modificaron o eliminaron las posiciones problemáticas.

Lo cual Significa esto que contamos con una legislación conforme al estándar de Budapest, sin embargo consideramos que el grado de aplicación efectivo de parte de los operadores del sistema de justicia es incierto. En comienzo, no existe información pública disponible sobre la ocurrencia de esta clase de delitos, salvo por la continua y constante confirmación de actores privados de existente un riesgo inminente y que buscan dar productos de estabilidad. Consecuentemente tampoco se sabe el número de razones que sobrepasan la averiguación policial y se formalizan en un proceso penal, llegan a juicio y reciben una sentencia. Al no existir cifras públicas ni otros medios para conocer el escenario presente, existe la sensación de que los diferentes actores interesados trabajan a ciegas o de manera descoordinada, a pesar de disponer de una legislación adaptada al uso universal. Prueba de ello son las diferentes iniciativas sectoriales que son impulsadas actualmente y que, en la mayoría de los casos, son contradictorias entre sí. Peor todavía, hay otras que ya han reclamado la vulneración de diferentes derechos con el objetivo de facilitar la labor de sus operadores ignorando procesos anteriores largamente consensuados.

Por ejemplo, pese a que existe desde hace varios años un protocolo en el Código Procesal Penal para la intervención legal de las comunicaciones, en 2015 se aprobó el Decreto Legislativo N° 1182 que creó un mecanismo por fuera de esta ley, que permitía a la policía acceder a datos de geolocalización sin orden judicial. Esto último compromete la legalidad de ciertas medidas de

acceso y retención y precariza la posición peruana frente a la implementación del Convenio.

2.2.7.2. Estandarización De Procesos Penales

Junto con las reglas penales, en su Segundo Capítulo el Acuerdo de Budapest recomienda diferentes medidas procesales a fin de viabilizar la persecución penal y facilitar la informática forense, o sea la acumulación de pruebas que permitan mostrar la comisión de los delitos informáticos, detectar a sus autores y conducirlos a juicio. Estas medidas tienen la posibilidad de dividir en propuestas sobre garantías procesales y propuestas sobre obligaciones de vigilancia. Las primeras son: el ámbito de aplicación del marco penal común, las condiciones y salvaguardias y los límites a la jurisdicción. Las otras abarcan diferentes obligaciones de conservación de datos informáticos, la revelación de dichos datos en tiempo real, su interceptación y los procedimientos para el registro y confiscación.

La legislación peruana en materia procesal aplicable a los delitos informáticos no ha sido pensada teniendo al Acuerdo de Budapest como relacionado. Por otro lado, la reforma del anterior Código Procesal Penal que condujo a la redacción y aceptación en 2004 del Nuevo Código Procesal Penal (NCPP) estuvo casi exclusivamente enfocada en renovar el sistema de queja penal e meter instituciones novedosas con el objetivo de adecuar y determinar los papeles de los actores en cada una de los periodos del proceso penal. No

obstante, por su misma naturaleza, este corpus de normas también es susceptible de modificaciones a través de leyes específicas. Con respecto a las propuestas sobre garantías procesales no encontramos que sean necesarias grandes modificaciones en la legislación peruana. Las posiciones usuales del Pacto de Budapest proponen un marco para la aplicación de medidas procesales especiales para los delitos informáticos, un apartado sobre las garantías y al final el entorno de la jurisdicción aplicable. En estos tres aspectos, actualmente se aplican normas del NCPP de orden general relacionadas a la legalidad de la obtención y uso de las pruebas, el debido proceso y el ámbito de la competencia territorial respectivamente.

En una evaluación inicial, las reglas procesales peruanas vigentes parecen ajustarse bien a lo postulado por el Acuerdo de Budapest, por lo menos en lo sustancial, por lo cual no parece primordial una reforma importante. El Pacto de Budapest sugiere medidas en relación a la recolección, interceptación, disposición y conservación de datos informáticos, lo cual incluye no solo la información del tráfico de datos sino además el contenido de los mismos y los dispositivos donde permanecen almacenados, algunas veces en tiempo real. Este tipo de medidas han sido introducidas principalmente por las modificaciones de la Ley N° 30096 al artículo N° 230 del NCPP relacionado a la intervención de las comunicaciones. Ahí se establecen mecanismos de cooperación y obligaciones para los concesionarios de servicios de telecomunicación. Sin embargo, hasta la fecha no se ha desarrollado de forma

específica su modo de aplicación, lo que parece haberse dejado para los manuales y protocolos de investigación del Ministerio Público, que es el encargado de solicitar estas medidas al Poder Judicial. No obstante, existe otra regla habilitante para adoptar dichos mecanismos que ha sido aprobada en 2015: el Decreto Legislativo 1182, que se superpone al NCPP y crea un sistema particular para la geolocalización de dispositivos móviles, además de (volver) a obligar obligaciones de recolección, conservación y entrega a las compañías de telecomunicación. Este Decreto además otorga facultades a la Policía sin requerir un mandato judicial para hacer estos pedidos, lo que pone en riesgo la constitucionalidad de dicha medida y la validez de las pruebas. Debería tenerse presente que esto puede ser problemático para la utilización del Pacto de Budapest puesto que la coexistencia de las dos reglas puede elaborar resultados inválidos.

2.2.7.3.Cooperación Internacional

Al final, en el Tercer Capítulo, el Pacto de Budapest instituye una secuencia de obligaciones mínimas y posiciones habituales para hacer posible la cooperación entre sus miembros. Estas obligaciones permanecen referidas primordialmente a la habituación de la legislación en temas de extradición, la ayuda recíproca y la construcción de un artefacto de contestación a emergencias. En el primer caso, la iniciativa del Acuerdo de Budapest es hacer viable la extradición constantemente que se cometa un delito informático y las naciones envueltos lo hayan tipificado en su norma penal. Para ello propone

adicionar los delitos informáticos en tratados previos de extradición y, de no existir, emplear el Convenio como base legal para que estos puedan ser ejecutados. En lo que respecta a la asistencia mutua, se propone que los resultados producto de las medidas propuestas en la sección de procesos penales puedan ser compartidos entre los miembros en situaciones específicas, con el fin de ampliar la eficacia de la persecución penal.

En este aspecto el Perú no cuenta con una legislación conforme al estándar de Budapest, en temas de cooperación universal, la cual busca logar una alianza más estrecha entre sus miembros e intensificar la cooperación entre las naciones.

En ese sentido, el Perú tiene una gran oportunidad de poder mejorar su regulación interna y, además, poder tener el apoyo y la cooperación de otros Estados. Finalmente, se propone un modelo de cooperación basado en la designación de puntos de contacto para atender solicitudes de emergencia que pueden o no estar relacionadas al contenido de los pedidos de asistencia mutua.

Ahora que el Perú ratifico el acuerdo, el Poder Ejecutivo tendrá que generar un conjunto laboral multisectorial con el objeto de evaluar el proceso de utilización del Acuerdo de Budapest. Este conjunto laboral debería estar formado mínimamente por: Un representante de la Secretaría de Regimen Digital, un representante del Ministerio de Interrelaciones Exteriores, un representante del Ministerio de Justicia y Derechos Humanos, un representante

del Ministerio de Transporte y Comunicaciones, un representante del Ministerio del Interior, un representante del Ministerio de Custodia y otras entidades que se estime correcto, incluso fuera del sector público.

El objetivo del grupo de trabajo será realizar un análisis de la situación de cara a la implementación del Convenio de Budapest y propondrá reformas en todos los niveles del Estado para lograr una adecuación exitosa.

Una vez desarrollado el objetivo de cooperación internacional cabe precisar que este objetivo trae consigo grandes cambios y beneficios para brindar una mejor asistencia en cuanto a delitos informáticos se trate, para ello enumero a continuación algunos de puntos en las que influirá de manera positiva en el Perú.

- En la vulnerabilidad de nuestro ecosistema digital ante ciberataques o incluso frente al riesgo de convertirnos en un campo de experimentación para los terroristas digitales.

- En facilitar las investigaciones judiciales sobre hechos delictivos de carácter transnacional a través de la formalización de los canales de intercambio de información con los países miembros.

- También en el país espera avanzar en los temas de evidencia digital y participar en las estrategias conjuntas en materia de ciberdelincuencia.

- con respecto la pandemia global del coronavirus (COVID-19) impacta a todos los ámbitos de una sociedad y en ese contexto la aplicación de cooperación internación representa un esfuerzo valioso para mantener el espacio cibernético a salvo.

La utilización del Pacto de Budapest implicará la manera de comenzar un proceso de revisión y de los 3 fines declarados del Acuerdo de Budapest: Producir un marco común de derecho penal sustantivo, estandarizar los procedimientos procesales y la informática forense e promover la cooperación mundial; y habiendo examinado el caso del territorio, debemos concluir que la utilización del Acuerdo no necesitará más grandes cambios. Probablemente en donde se presenten las mejores oportunidades de formular políticas públicas en materia de ciberseguridad serán en el ámbito de la cooperación internacional, lo que abrirá la puerta para una inserción mayor del país en los espacios de discusión que el Convenio habilita para sus miembros.

Habiendo examinado el caso en la que está el territorio, todo parece indicar que, en temas de adecuación, es poco lo cual debe modificarse de manera sustantiva para llevar a cabo el Pacto de Budapest. Sin embargo, sí hay varias medidas que merecen particular atención y sin las cuales el cumplimiento de las metas del Acuerdo no va a poder ser abordados de manera exitosa. Estas acciones están principalmente orientadas a viabilizar la implementación del Convenio y explotar sus beneficios, especialmente los relacionados a la adecuación normativa y la cooperación internacional.

Sin embargo el efecto de la utilización (El convenio Budapest en America Latina, 2018) del Convenio de Budapest variable y es dependiente en gran medida de la relación entre la formulación de políticas públicas, el grado de involucramiento de los actores y los papeles que puedan consumar, así como el grado de respeto de los derechos humanos relacionados en cada una de los periodos.

En conclusión, debemos asumir algunos de los escenarios que a veces son positivos, pero también negativos en relación al ecosistema digital peruano. La forma cómo esto evolucione depende del compromiso que organizaciones de todos los sectores asuman. Es por esto que esperamos que los debates acerca de la implementación se den en espacios abiertos y transparentes.

SUB CAPÍTULO III

DELITOS INFORMÁTICOS Y LA SUSCRIPCIÓN DEL CONVENIO DE BUDAPEST EN EL PERÚ

2.3.1. Problemática de la delincuencia informática en el Perú

El uso y acceso cada vez más frecuente de los dispositivos electrónicos en el ciberespacio y las telecomunicaciones, así como, el acceso a navegar en internet, contar con correos electrónicos, utilizar mensajes de texto, acceder a redes sociales, realizar compras on line, celebrar contratos, hacer uso de programas, apps, entre otros, ha conllevado a facilitar las actividades del ser humano, sin embargo, representa un espacio cómodo para los ciberdelincuentes, quienes encuentran un mundo sin fronteras para la comisión de delitos informáticos.

Teniendo en consideración lo señalado por la (ORGANIZACIÓN DE LAS NACIONES UNIDAS, Abril de 2015): Uno de los principales elementos impulsores de la ciberdelincuencia contemporánea y del uso creciente de pruebas digitales es el desarrollo de la conectividad electrónica global. (…) El veloz incremento de Internet y de la tecnología informática ha facilitado el aumento económico y un más grande ingreso a servicios fundamentales como la educacion, la atención de salud y la gobernanza electrónica, empero además ha desarrollado novedosas maneras para la actividad delictiva.

A ello se suma, que algunos instrumentos de ciberdelincuencia pueden construir redes globales de dispositivos infectados con programas informáticos maliciosos controlados a distancia por delincuentes, que el uso de páginas web se utiliza para cometer actos de hostigamiento, amenazas, extorción e difusión de información privada; el fraude en línea con tarjetas de crédito, robo y suplantación de identidad, entre otros casos.

Perú, no es ajeno a la ciberdelincuencia, y aun cuando la regulación penal contenida en la Ley N° 30096, sanciona la comisión de los siguientes delitos informáticos:

> (CAPÍTULO II) DELITOS CONTRA DATOS Y SISTEMAS INFORMÁTICOS
>
> Artículo 2 acceso ilícito; Artículo 3. Atentado a la integridad de datos informáticos; Artículo 4. Atentado a la integridad de sistemas informáticos
>
> (CAPÍTULO III) DELITOS INFORMÁTICOS CONTRA LA INDEMNIDAD Y LIBERTAD SEXUAL

Artículo 5 Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos.

(CAPÍTULO IV) INFORMACIÓN CONTRA LA INTIMIDAD Y EL SECRETO DE LAS COMUNICACIONES

Interceptación de datos informáticos

(CAPÍTULO V) DELITOS INFORMATICOS CONTRA EL PATRIMONIO

Artículo 8 Fraude Informático

(CAPÍTULO VI) DELITOS INFORMÁTICOS CONTRA LA FÉ PÚBLICA,

Artículo 9 Suplantación de Identidad

La realidad nos muestra la frecuencia con que estos se viene cometiendo, así, según el portal (ANDINA, 2018) son tres las principales modalidades de delitos informáticos que afectan a usuarios y empresas en el Perú, estos son, **ransomware, phishing y cryptojacking**:

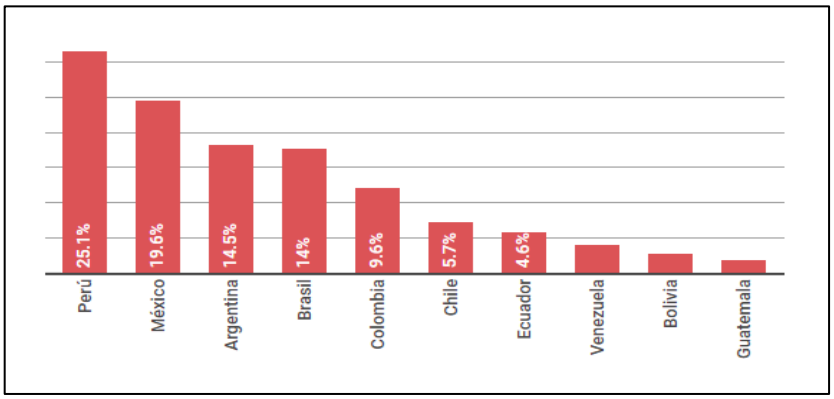
2.3.1.1. Ransomware

> El **ransomware**, Es un programa de software malicioso que infecta tu computadora y muestra mensajes que exigen el pago de dinero para restablecer el funcionamiento del sistema (…), tiene capacidad de bloquear la pantalla de una computadora o cifrar archivos importantes predeterminados con una contraseña. (AO Kaspersky Lab., 2020)

El Ransomware, se adecua a los supuestos previstos por el artículo 4 de la Ley 30069, que sanciona el *Atentado a la integridad de sistemas informáticos* (Delito de acceso ilícito).

Esta forma de software es utilizada para bloquear archivos o dispositivos del usuario, secuestrar datos de la computadora y luego reclama el pago de una suma de dinero en línea para liberar o devolver los archivos; este tipo de delitos en el año 2017 ha representado la cifra más alta en América latina, y con un 25.1 % Perú se ubica en primer lugar, sucedido por México, Argentina, Brasil, Colombia, Chile, Ecuador, Venezuela, Bolivia y Guatemala, así:

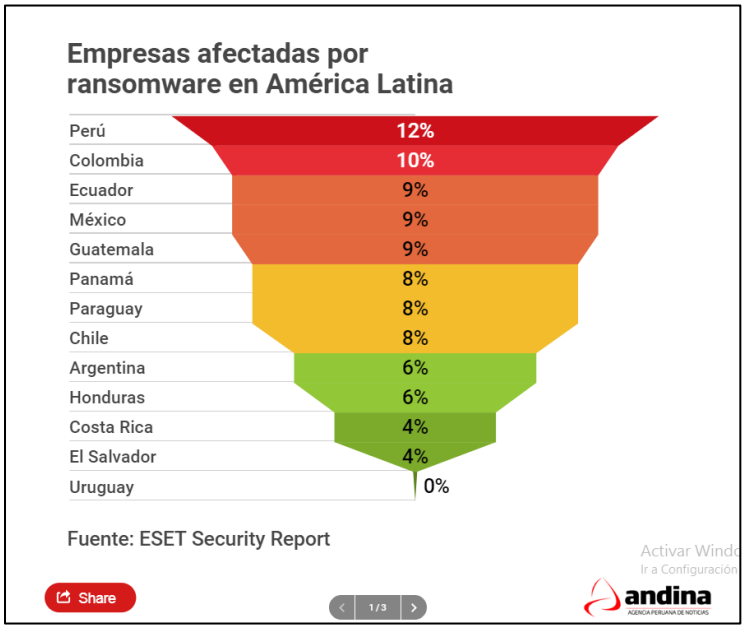
Tabla N° 01



Fuente:https://portal.andina.pe/edpespeciales/2018/ciberataques-peru/index.html

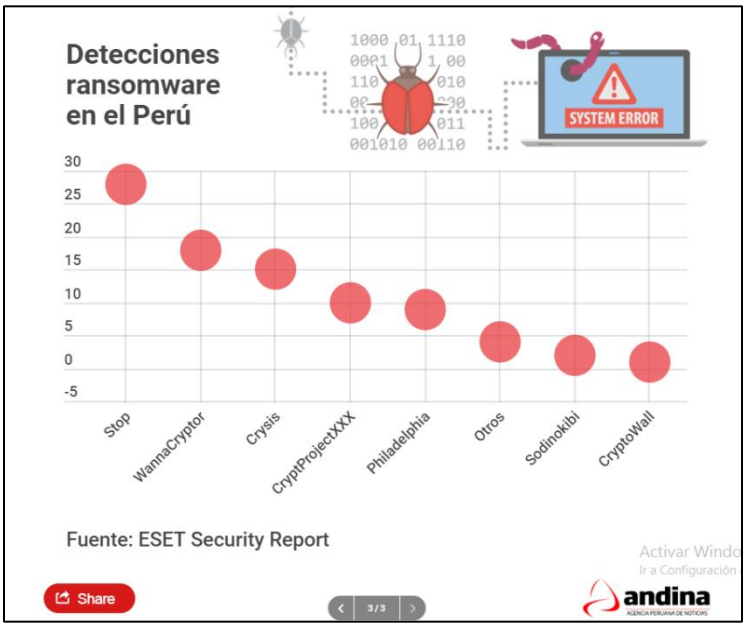
Para el 2018, la empresa ESET Segurity Report citada por (ANDINA AGENCIA DE NOTICIAS, andina.pe, 2019) nos presenta información que detalla que Perú se ubica en primer lugar en América Latina, como país que reporta ataques de ransomware informático, siendo los sectores los sectores más afectados el de tecnología, educación y salud.

Tabla N° 02



Fuente:https://infogram.com/detecciones-de-ransomware-1hxr4zzjlejq4yo

Tabla N° 03



Fuente: https://infogram.com/detecciones-de-ransomware-1hxr4zzjlejq4yo

Eset Security Report Latinoamérica, señalo en el 2019 que Perú es el país que menos implementa políticas para gestionar la ciberseguridad de las empresas; esto, representa uno de los factores por los cuales el Perú se encuentra en primera ubicación.

En relación al **phishing**, denominada también como ingeniería social, utilizada para cometer fraude electrónico y estafas en línea; tiene como principal víctima a los usuarios más que a las empresas, porque roba información financiera a través de redes sociales y correos electrónicos.

El phishing, se adecua a los supuestos previsto por el artículo 8 de la Ley 30069, que sanciona el *Fraude Informático* (Delito informático contra el patrimonio).

El **cryptojacking**, orientado a ataques invisibles, se presenta cuando: "los usuarios ingresan a un portal y se ejecuta algoritmos criptografiados para crear criptomonedas como bitcoin, etherium y ripple, con valores superiores a los 5000 dólares dependiendo del mercado"

Según la empresa pionera en protección antivirus (CYBERSEGURITY EXPERTS YOUR SIDE ESET, 2019) también se presentan otros incidentes de seguridad de la información, como son: a) **Infección con códigos malicioso**, b) **Acceso indebido a sistemas**, c) **Uso inapropiado de la infraestructura**, d) **Robo de información**, e) **Privación y/o Secuestro de información**, g) A**taques de ingeniería social o phishing.**

Estos actos, se adecuan a los supuestos previstos en la Ley 30069:

La **Infección con códigos maliciosos** y el **uso inapropiado de la infraestructura**, se adecua a los supuestos previstos por el artículo 3 y 4 de la Ley 30069, que sanciona el *Atentado a la integridad de los datos y de los sistemas informáticos.*

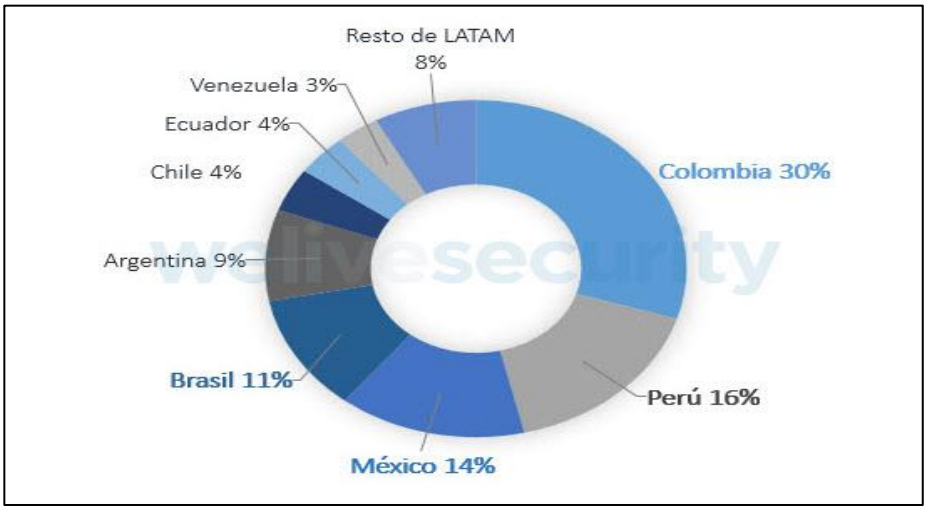
El **Acceso indebido a sistemas** se adecua a los supuestos previstos por el artículo 4 y 9 de la Ley 30069, que sanciona el *Atentado a la integridad de los sistemas informáticos, y la suplantación de identidad.*

El **Robo de información**, se adecua a los supuestos previstos por el artículo 8 la Ley 30069, que sanciona el *Fraude informático. (Delitos Informáticos contra el patrimonio)*

La **Privación y/o Secuestro de información**, se adecua a los supuestos previsto por el artículo 7 la Ley 30069, que sanciona el *Interceptación de datos informáticos. (Delitos informáticos contra la intimidad y el secreto de las comunicaciones)*

La empresa se ciberseguridad (CYBERSEGURITY EXPERTS YOUR SIDE ESET, 2019) advierte que: “El 40% de las empresas de América Latina sufrió una infección con malware el último años”, afirma que **nuestro país cerró el 2018 ocupando el segundo lugar con propagaciones ransomware** por debajo de Colombia.

Tabla N° 04

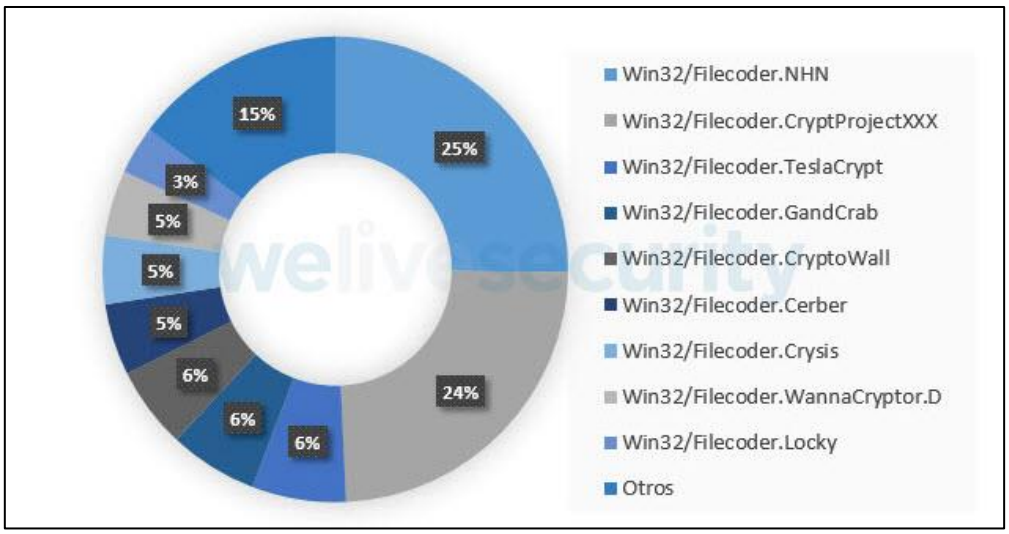


Fuente: https://www.welivesecurity.com/la-es/2019/01/04/paises-mas-afectados-ransomware-latinoamerica-durante-2018/#single-post-fancybox-1

ESET, recomienda como tecnologías a aplicar para hacer frente a estos casos, las siguientes: a) Backup de la información, b) Firewall, c) Soluciones de seguridad para móviles, d) Herramientas de detección/prevención de intrusiones (IDS/IPS), e) Sofware antivirus, f) Tecnología de cifrado, g) Soluciones de doble autenticidad, h) Administración de parches y actualización de software.

En Perú, se ha desarrollado un microsistema de ronsomware, dominado por dos familias, la CryptProjectxxx () y el Filcoder NHN; el ronsomware presenta las siguientes variantes:

Tabla N° 05



Fuente: https://www.welivesecurity.com/la-es/2019/01/04/paises-mas-afectados-ransomware-latinoamerica-durante-2018/#single-post-fancybox-6

2.3.1.2. Spyware

> **Spyware** es un tipo de maleare que intenta mantenerse oculto mientras registra información en secreto y sigue sus actividades en línea, tanto en equipos como en dispositivos móviles. Puede supervisar y copiar todo lo que escribe, carga, descarga y almacena. Algunas cepas de spyware también son capaces de activar cámaras y micrófonos para verlo y escucharlo sin que usted se dé cuenta. (Seguin, 2020)

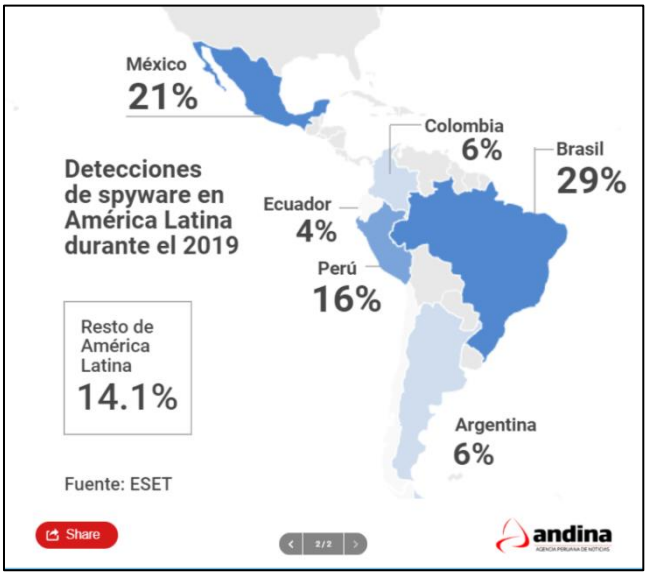
El Spyware comprende programas espías, representa una de las modalidades utilizadas por los cibercriminales para robar información sensible de una computadora.

El Spyware, se adecua a los supuestos previstos por el artículo 3 y 4 de la Ley 30069, que sanciona el *Atentado a la integridad de datos informático e integridad de sistemas informáticos.*

Entre los spyware más comunes están, el troyano Emotet, tiene como objetivo el robo de credenciales bancarias y datos financieros, es enviado mediante correos electrónicos falsos a manera de promociones de tiendas virtuales; el Mekotio, caracterizado por suplantar la identidad de compañías de servicios mediante correos electrónicos en el cual envían un enlace para descargar una supuesta factura, pero en realidad es un archivo que contiene un troyano. (ANDINA AGENCIA DE NOTICIAS, 2019)

Nuestro país, es el **tercer país más afectado con los programas Spyware**, después de Brasil y México:

Tabla N° 06

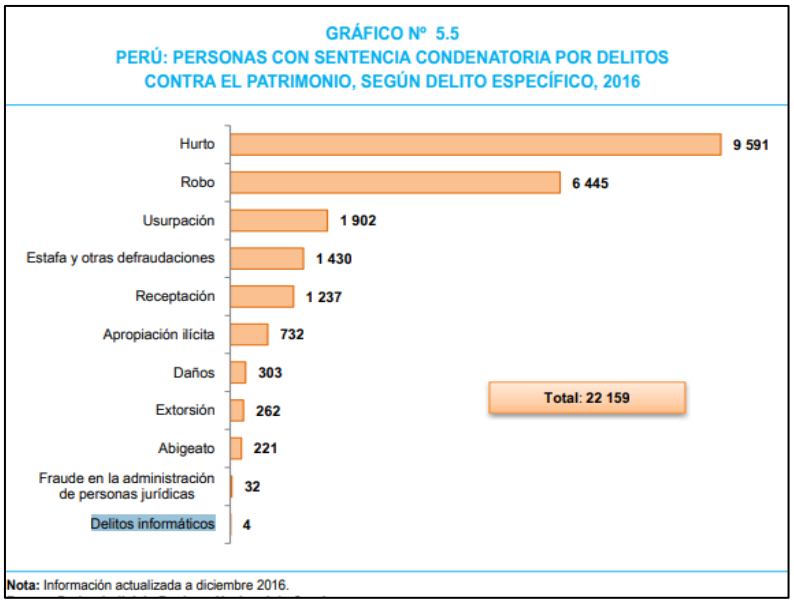


Fuente:https://infogram.com/nuevas-variantes-de-spyware-por-plataforma-en-2019-1ho16v0m8pwx4nq

Por otro lado, tenemos los datos proporcionados por (INSTITUTO NACIONAL DE ESTADISTICA E INFORMÁTICA, 2017) que nos da a conocer que en el caso de delitos informáticos contra el patrimonio según delito específico, en el año 2016 se sentenció a 04 personas, y para el año 2017, el Poder Judicial únicamente sentencio a 02 personas.

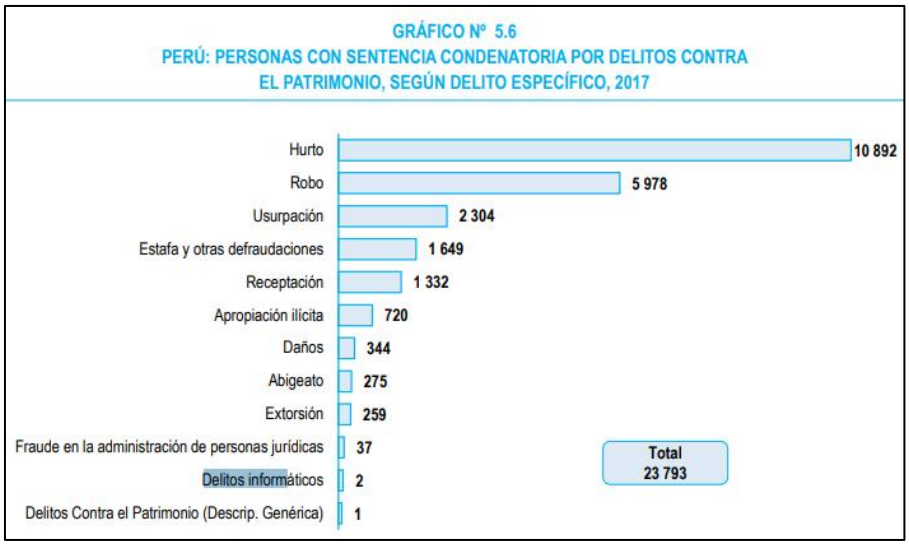
Resulta ínfimo la cantidad de personas sentenciadas para finales de 2017, debido a que los datos que anteceden muestran un escenario que ubica a nuestro país con porcentajes elevados para la comisión de delitos informáticos.

Tabla N° 07



Fuente: Poder Judicial – Registro Nacional de Condenas
Elaborado: Instituto Nacional de Estadística e Informática

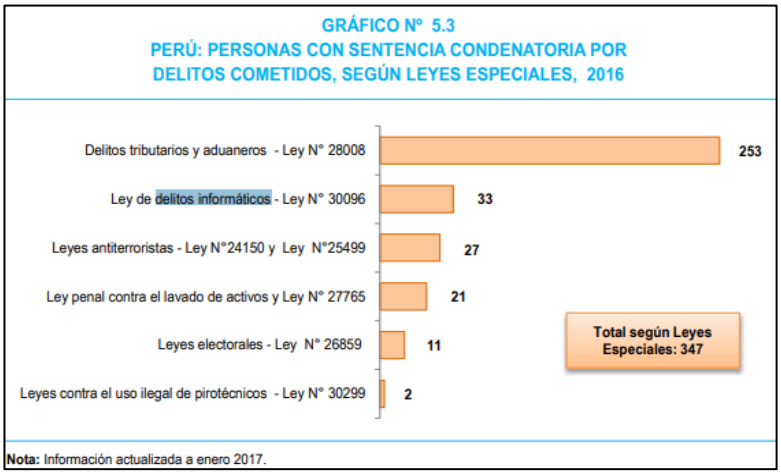
Tabla N° 08



Fuente: Poder Judicial – Registro Nacional de Condenas
Elaborado: Instituto Nacional de Estadística e Informática

El (INSTITUTO NACIONAL DE ESTADISTICA E INFORMÁTICA, 2017) nos da a conocer que las sentencias emitidas en el caso de delitos informáticos cometidos según ley especial, asciende a 33.

Tabla N° 09



Fuente: Poder Judicial Registro Nacional de Condenas
Elaborado: Instituto Nacional de Estadística e Informática

Tabla N° 10

CUADRO Nº 5.6
PERÚ: PERSONAS CON SENTENCIA CONDENATORIA, POR COMISIÓN DE DELITOS CONTRA EL PATRIMONIO, SEGÚN DELITO ESPECÍFICO, 2012 - 2016

Delito específico	2012		2013		2014		2015		2016	
	Total	%	Total	%	Total	%	Total	%	Total	%
Total	**15 115**	**100,0**	**17 239**	**100,0**	**14 858**	**100,0**	**15 252**	**100,0**	**22 159**	**100,0**
Hurto	5 577	36,9	6 583	38,2	5 779	38,9	5 771	37,8	9 591	43,3
Robo	5 513	36,5	5 774	33,5	4 765	32,1	4 931	32,3	6 445	29,1
Usurpación	1 109	7,3	1 472	8,5	1 266	8,5	1 264	8,3	1 902	8,6
Estafa y otras defraudaciones	1 191	7,9	1 302	7,6	1 229	8,3	1 254	8,2	1 430	6,5
Receptación	649	4,3	797	4,6	735	4,9	872	5,7	1 237	5,6
Apropiación ilícita	566	3,7	665	3,9	540	3,6	526	3,4	732	3,3
Daños	220	1,5	260	1,5	213	1,4	264	1,7	303	1,4
Abigeato	150	1,0	155	0,9	140	0,9	178	1,2	221	1,0
Extorsión	109	0,7	188	1,1	145	1,0	169	1,1	262	1,2
Fraude en la administración de personas jurídicas	25	0,2	37	0,2	30	0,2	21	0,1	32	0,1
Delitos informáticos	6	0,0	6	0,0	16	0,1	2	0,0	4	0,0

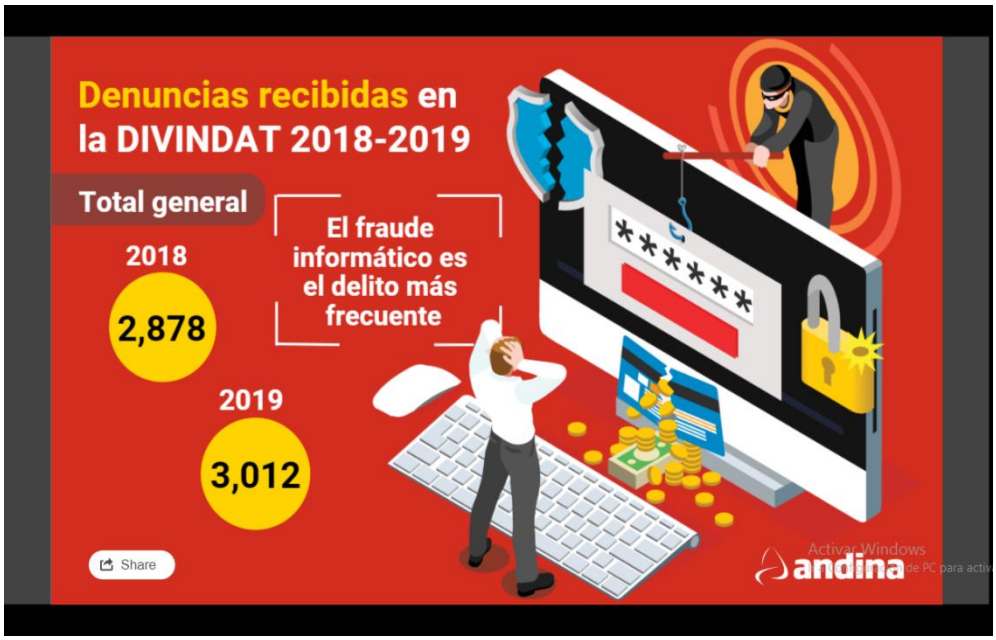
Nota: Información actualizada a diciembre de 2016.

Fuente: Poder Judicial Registro Nacional de Condenas
Elaborado: Instituto Nacional de Estadística e Informática

En el gráfico que antecedes se aprecia la variación en cantidad de personas sentenciadas por la comisión de delitos informáticos contra el patrimonio desde el año 2012 al 2017, siendo el 2014 el año en que se sanciono a más delincuentes (16).

Datos actuales, brindados por (ANDINA AGENCIA DE NOTICIAS, 2020) evidencia que se han presentado un número importante de denuncias referidas a delitos informáticos, número que se ha ido incrementando desde 2018:

Tabla N° 11



Fuente:https://infogram.com/denuncias-de-delitos-informaticos-1h7g6kgdpmko4oy

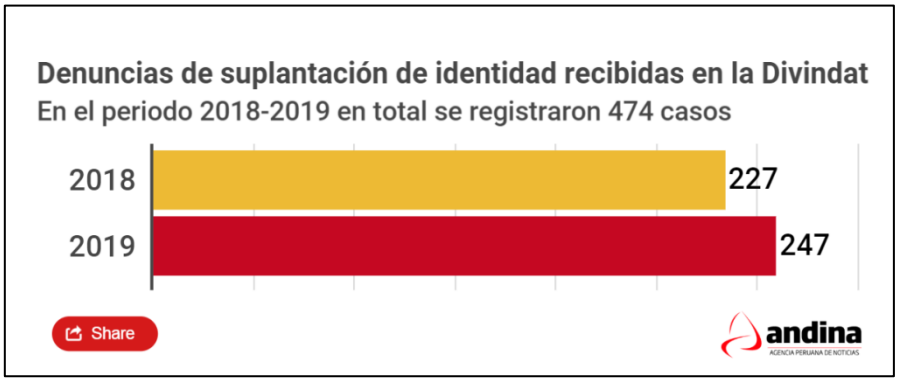
Teniendo en consideración los datos contenidos en la tabla N° 09 y 10, se espera que la proyección de personas sentenciadas se eleve para el 2020.

Algunos ejemplos de delitos informáticos más frecuentes en nuestro país son: La suplantación de identidad, con la creación y uso de perfiles falsos de cuentas de Facebook (véase el grafico N° 11) y Phishing.

Al respecto, el (DIARIO OFICIAL EL PERUANO, 2020) evidencia que: Crecen **denuncias de perfiles falsos**. En el 2019 se incrementaron las denuncias de suplantación de identidad en redes sociales y plataformas de internet pasando de 227 a 247 casos registrados por la Policía Nacional del Perú". El Coronel de la Policía Nacional del Perú Orlando Mendieta, jefe de la División de Investigación de Alta Tecnología (Divindat), explico (…). Los

Usuarios podrían encontrar sus fotos en perfiles con nombres falsos que son utilizados para chantajes o acosos sexuales. También se suplanta la identidad del usuario, incluyendo información real. Los ciber delincuentes crean perfiles falsos y se hacen pasar por la víctima para pedir dinero a sus amistades.

Tabla N° 12



Fuente: https://infogram.com/suplantacion-de-identidad-1ho16vkexp782nq

La problemática que enfrenta el Perú es sin duda delicada, según el Contralmirante Enrique Arnáez Braschi entrevistado por (BUSINESS ALLIANCE FOR SECURE COMMERCE CAPÍTULO PERÚ, 2019), en la Comandancia de Ciberdefensa de la Marina de Guerra del Perú, creada en 1999: Diariamente se recibe distintos tipos de ataques provenientes de muchas partes del mundo. Normalmente los ataques buscan robar información, identidades o crédito para venderlos en el mercado negro de internet; sin embargo, también actúan en el ciberespacio organizaciones criminales internacionales y hasta Estados.

Agrega que la más frecuente técnica utilizada es la **PHISHING**, "que consiste en penetrar una red a través de la seducción a algún usuario para hacer click en un link o en un archivo que le otorga, al atacante, el acceso libre a su computadora".

Culmina la entrevista precisando: En palabras más sencillas, nosotros, los seres humanos, somos el vector de ataque más fácil, por experiencia a nivel mundial, el eslabón más débil y más vulnerable de toda organización es la persona (…). Para este efecto recomienda las siguientes medidas:

- Verificar el origen y contenido de los correos electrónicos que reciba chequeando que la dirección del promotor no sea una falsa.
- Establecer contraseñas robustas, no compartirlas y cambiarlas periódicamente.
- No instalar software no autorizado por la empresa, y menos se es pirata.
- Cifrar información sensible con los métodos que trae el propio procesador de texto u hoja de cálculo que emplee.
- Analizar con un antivirus los archivos que descarguemos desde internet, correo electrónico o cualquier dispositivo externo como USBs, DVDs o discos duros externos, entre otros; este análisis debe realizarse antes de abrir el archivo.
- Bloquear la sesión de su computador cundo no se encuentre presente

- Controlar con responsabilidad en el uso de los dispositivos asignados, de la información que contienen y de los accesos a redes especialmente a las públicas.

Aun cuando la problemática expuesta en este acápite es reciente, no quiere decir que nuestro país este expuesto de forma deliberada; actualmente se cuenta con un marco jurídico penal importante, el cual regula diferentes tipos de delitos informáticos desde 1991, y ha ido experimentando modificaciones desde entonces.

2.3.2. Regulación de delitos informáticos en el Perú

Nuestra normativa ha sufrido más de una modificación en cuanto a las conductas ilícitas relacionadas a delitos informáticos, a decir de (VILLAVICENCIO TERREROS, 2014), de los antecedentes de los citados delitos señala:

El delito informático en un principio estaba tipificado en el artículo 186, inciso 3, segundo párrafo del Código Penal de 1991. Actualmente, los delitos informáticos permanecen previstos en el Capítulo X (13) del Código Penal: los artículos 207-A (interferencia, ingreso o réplica ilícita contenida con base de datos), 207-B (alteración, mal o devastación de base de datos), 207-C (circunstancias cualificantes agravantes), 207-D (tráfico ilegal de datos), y en las leyes penales especiales.

Entre estas leyes penales especiales, se encuentra la Ley 30096 (Ley de Delitos Informáticos). Esta Ley de Delitos Informáticos está constituida por 7 capítulos que se estructuran de la siguiente forma: finalidad y objeto de la ley (Capítulo I), delitos contra datos y sistemas informáticos (Capítulo II), delitos informáticos contra la indemnidad y libertad sexual (Capítulo III), delitos informáticos contra la intimidad y el secreto de las comunicaciones (Capítulo IV), delitos informáticos contra el patrimonio (Capítulo V), delitos informáticos contra la fe pública (Capítulo VI) y las disposiciones comunes (Capítulo VII). Posteriormente se promulgó la Ley 30171 (Ley que modifica la Ley 30096, Ley de Delitos Informáticos). La finalidad de esta ley fue adecuar la Ley 30096 a los estándares legales del convenio sobre la cibercriminalidad (Convenio de Budapest), al incorporar en la redacción típica de los artículos 2, 3, 4, 7, 8 y 10 de la referida Ley la posibilidad de cometer el delito deliberada e ilegítimamente. Las modificaciones de la Ley 30171 (10 de marzo de 2014), con respecto a los delitos informáticos, son las siguientes: - Artículo 1; Modificación de los artículos 2, 3, 4, 5, 7, 8 y 10 de la Ley 30096 Ley de Delitos Informáticos. - Artículo 2; Modificación de la tercera, cuarta y undécima disposiciones complementarias finales de la Ley 30096 Ley de Delitos Informáticos.

Artículo 3; Incorporación del artículo 12 a la Ley 30096 Ley de Delitos Informáticos. - Artículo 4; Modificación de los artículos 158, 162 y 323 del Código Penal. - Artículo 5; Incorporación de los artículos 154-A y 183-B del

Código Penal. - Única Disposición Complementaria Derogatoria; Deroga el artículo 6 de la Ley 30096 Ley de Delitos Informáticos.

A manera de resumen, los delitos informáticos previstos en la Ley 30096 a la fecha son:

- **DELITOS CONTRA DATOS Y SISTEMAS INFORMÁTICOS**, que comprende: Artículo 2 referido al **acceso ilícito**. "El que deliberada e ilegalmente accede a todo o parte de un sistema informático, siempre que se realice con vulneración de medidas de seguridad establecidas para impedirlo, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días multa. Será reprimido con la misma pena, el que accede a un sistema informático excediendo lo autorizado". Artículo 3. **atentado a la integridad de datos informáticos**. "El que deliberadamente daña, introduce, borra, deteriora, altera, suprime o hace inaccesibles datos informáticos, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días multa". Artículo 4. **Atentado a la integridad de sistemas informáticos**. "El que deliberada e ilegítimamente utiliza, total o parcialmente, un sistema informático, impide el acceso a este, entorpece o imposibilita su funcionamiento o la prestación de sus servicios, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días multa."
- **DELITOS INFORMÁTICOS CONTRA LA INDEMNIDAD Y LIBERTAD SEXUAL,** que comprende: Artículo 5 **Proposiciones a**

niños, niñas y adolescentes con fines sexuales por medios tecnológicos. "El que a través de internet u otro medio análogo contacta con un menor de catorce años para solicitar u obtener de él material pornográfico, o para proponerle llevar a cabo cualquier acto de connotación sexual con él o con tercero, será reprimido con una pena privativa de libertad no menor de cuatro ni mayor de ocho años e inhabilitación conforme a los numerales 1, 2, 4 y 9 del artículo 36 del Código Penal. Cuando la víctima tiene entre catorce y menos de dieciocho años de edad y medie engaño, la pena será no menor de tres ni mayor de seis años e inhabilitación conforme a los numerales 1,2,4 9 del artículo 36 del Código Penal"

- **INFORMACIÓN CONTRA LA INTIMIDAD Y EL SECRETO DE LAS COMUNICACIONES**, que comprende: Artículo 7 **Interceptación de datos informáticos.** "El que deliberada e ilegítimamente intercepta datos informáticos en transmisiones no públicas, dirigidos a un sistema informático originados en un sistema informático o efectuado dentro de mismo, incluidas las emisiones electromagnéticas provenientes de un sistema informático que transporte dichos datos informáticos, será reprimido con una pena privativa de libertad no menor de tres ni mayor de seis años (…)."
- **DELITOS INFORMATICOS CONTRA EL PATRIMONIO,** que comprende: Artículo 8. **Fraude Informático.** "El que deliberada e ilegítimamente procura para sí o para otro un provecho ilícito en perjuicio de tercero mediante el diseño, introducción, alteración, borrado, supresión, donación de datos informáticos o cualquier interferencia o manipulación en el funcionamiento de un sistema informático, será reprimido con una pena

privativa de libertad no menor de tres ni mayor de ocho años y con sesenta a ciento veinte días multa. La pena será privativa de libertad no menor de cinco ni mayor de diez años y de ochenta a ciento cuarenta días multa cuando se afecte el patrimonio del Estado destinado a fines asistenciales o programas de apoyo social"

- **DELITOS INFORMÁTICOS CONTRA LA FÉ PÚBLICA,** comprende: Artículo 9 **Suplantación de Identidad.** "El que, mediante las tecnologías de la información o de la comunicación suplanta la identidad de una persona natural o jurídica, siempre que de dicha conducta resulte algún perjuicio, material o moral, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años"

2.3.2.1. DIVINDAT División de Investigación de Delitos de Alta Tecnología

La División de Investigación de Delitos de Alta Tecnología, forma parte de la Dirección de Investigación Criminal y Apoyo a la Justicia (DIRINCRI), esta institución se encarga de:

Prevención: Mediante campañas en Medios de Comunicación, en la ASBANC, en empresas dedicadas al rubro de medios de pago y empresas y comercios que prestan colaboración a instituciones del Estado.

Evalúa legislación a fin de proponer modificaciones.

Presta colaboración a instituciones del Estado.

Apoya a organismos no gubernamentales en la lucha contra la ciberdelincuencia y criminalidad (trata de personas, prostitución, pornografía,

tráfico de órganos, etc.) (DIVISIÓN DE INVESTIGACIÓN DE DELITOS DE ALTA TECNOLOGÍA)

Dirección:
Piso 9 de la Av. España N° 323, Cercado de Lima
Correo:
www.policiinformatica.gop.pe
En facebook
@división de investigación de delitos de alta tecnología

2.3.2.2. Perú y el Gobierno Digital

La transformación digital no podía únicamente quedar al alcance de las personas usuarias o las empresas privadas, también los Estados han ido implementando procesos de innovación tecnológica y de transformación digital; nuestro país cuanta con una Secretaría de Gobierno Digital como ente rector del Sistema Nacional de Transformación Digital y administradora de las plataformas digitales del Estado Peruano.

El marco jurídico que da sustento al Gobierno Digital es el Decreto Legislativo N° 1412 de septiembre de 2018, que permite adecuar la gestión de identidad digital, servicios digitales, arquitectura digital, interoperabilidad, seguridad digital y datos (Secretaría de Gobierno Digital, 2020).

Este decreto, tiene por objeto establecer el marco de gobernanza del gobierno digital, que según el artículo 2, es de aplicación a toda entidad que forma parte de la Administración Pública a que se refiere el artículo I del Título

Preliminar del Texto Único Ordenado de la Ley N° 27444 Ley de Procedimiento Administrativo General.

El artículo 6 del decreto en mención, prescribe:

> **El gobierno digital**, es el uso de las tecnologías digitales y datos en la Administración Pública para la creación de valor público. Se sustenta en un ecosistema compuesto por actores del sector público, ciudadanos y otros interesados, quienes apoyan en la implementación de iniciativas y acciones de diseño, creación de servicios digitales y contenidos, **asegurando el pleno respeto de los derechos de los ciudadanos y personas en general en el entorno digital.** (El sombreado nos corresponde)

El Decreto Legislativo N° 1412, regula diferentes aspectos referidos a un gobierno digital, entre los que se puede precisar están:

- El ente rector es la presidencia del Consejo de Ministros (Artículo 8).
- Entre sus finalidades esta, mejorar la prestación y acceso a servicios digitales seguros y promover la colaboración entre entidades (Artículo 4).
- Rige principios como la cooperación digital (Prima el intercambio de datos e información, la interoperabilidad de los sistemas y soluciones para la prestación conjunta de servicios digitales) y de Nivel de protección adecuado para los datos (El tratamiento de los datos

personales debe realizarse conforme a lo establecido en la Ley de Protección de Datos Personales y su Reglamento) Artículo 5.

- La Identidad digital, que es aquel conjunto de atributos que individualiza y permite identificar a una persona en entornos digitales. (Artículo 10)

- Obtención y uso del Documento Nacional de Identidad electrónico -DNIe- (Artículo 16 y 17)

- Gobernanza de datos. Los datos son la representación dimensionada y descifrable de hechos, información o concepto, expresada en cualquier forma apropiada para su procesamiento, almacenamiento, comunicación e interpretación. Las entidades de la Administración Pública administran sus datos como un activo estratégico, garantizando que estos se recopilen, procesen, publiquen, almacenen y pongan a disposición durante el tiempo que sea necesario y cuando sea apropiado, considerando las necesidades de información, riesgo y la normatividad vigente en materia de gobierno digital, seguridad digital, transparencia, protección de datos personales y cualquier otra vinculante. (Artículo 23)

- La seguridad jurídica es el estado de confianza en el entorno digital que resultan de la gestión y aplicación de un conjunto de medidas proactivas y reactivas frente a los riesgos que afectan la seguridad de las personas (…). (Artículo 30)

- El Marco de seguridad digital del Estado, el artículo 32. precisa que se cuenta con ámbitos como: a) Defensa, al respecto se precisa: "El Ministerio de Defensa (MINDEF) en el marco de sus funciones y competencias dirige, **supervisa y evalúa las normas en materia de ciberdefensa**". b) "La Dirección Nacional de Inteligencia (DINI) como autoridad técnica normativa en el marco de sus funciones **emite, supervisa y evalúa las normas en materia de inteligencia, contrainteligencia y seguridad digital en el ámbito de esta competencia**". c) El Ministerio de Justicia y Derechos Humanos (MINJUS), el Ministerio del Interior (MININTER), la Policía Nacional del Perú (PNP), el Ministerio Púbico y el Poder Judicial (PJ) **en el marco de sus funciones y competencias dirigen, supervisan y evalúan las normas en materia de ciberdelincuencia**.

Del contenido desarrollado en el artículo 6 del Decreto Legislativo en mención, el gobierno digital es el uso estratégico de las tecnologías digitales y datos en la Administración Pública para la creación de valor público (…); de ésta manera, nuestro país adopta un modelo de gobierno digitalizado, de manera que, se integra a un sistema de informática y de interconexión mediante el ciberespacio.

2.3.2.3. Perú y Ciberdefensa

Esta decisión, conlleva a adoptar medidas de ciberseguridad a fin de cautelar la información que el Estado tiene a su cargo y asegurar el pleno respeto

de los derechos de los ciudadanos y personas en general, y de evitar la posible comisión de delitos informáticos previstos en el Convenio de Budapest.

Se ha previsto que la Dirección Nacional de Inteligencia (DINI) **emita, supervise y evalúe las normas en materia de inteligencia, contrainteligencia y seguridad digital en el ámbito de esta competencia,** y que **entidades como** El Ministerio de Defensa (MINDEF), el Ministerio de Justicia y Derechos Humanos (MINJUS), el Ministerio del Interior (MININTER), la Policía Nacional del Perú (PNP), el Ministerio Púbico y el Poder Judicial (PJ) dirijan, supervisen y evalúen las normas en materia de ciberdelincuencia.

Con posterioridad, en agosto de 2019 se promulga la Ley N° 30999 "Ley de Ciberdefensa", que prescribe:

> La ciberdefensa es considerada como una capacidad militar que le permite a las Fuerzas Armadas del Perú actuar en defensa de las secciones digitales de sus activos, que pueden tener ramificaciones tan profundas que un ataque puede comprometer sistemas, bienes y/o servicios de carácter estratégico. (WATSON, 2019)

De acuerdo al artículo 1 de la ley en mención, esta tiene por objeto establecer el marco normativo en materia de ciberdefensa del Estado peruano, regulando las operaciones militares en y mediante el ciberespacio a cargo de los órganos ejecutores del Ministerio de Defensa dentro de su ámbito de competencia, conforma ley.

En el artículo 5 se precisa que las Fuerzas Armadas, constituidas por el Ejército, la Marina de Guerra, las Fuerzas Aéreas y el Comando Conjunto de las Fuerzas Armadas son instituciones con calidad de órganos ejecutores del Ministerio de Defensa. Por su parte, en el artículo 7 se precisa el empleo de capacidades de ciberdefensa por parte de los órganos ejecutores antes mencionados ante amenazas o ataques en y mediante el ciberespacio en defensa de la seguridad nacional. En el artículo 9, se establece que el uso de la fuerza por parte de las Fuerzas Armadas mediante el ciberespacio se realiza teniendo en consideración lo regulado en el artículo 51 de la Carta de las Naciones Unidas.

2.3.3. Aspectos generales de la suscripción realizada por Perú del Convenio de Budapest

El convenio de Budapest, representa un instrumento de cooperación entre los Estado miembros del Consejo de Europa y las economías firmantes, su finalidad es proteger a la sociedad ante los actos de ciberdelincuencia, para ello promueve la adopción de legislación compatible y adecuada, así como la cooperación internacional frente a los actos en mención.

La ratificación del convenio, ha seguido el siguiente procedimiento:

- El Poder ejecutivo, representado por el Presidente de la República Martin Vizcarra Cornejo presenta la propuesta de adhesión del Perú al Convenio de Budapest.

- El Congreso de la República, aprobó el dictamen del proyecto de ley que aprueba el Convenio sobre Ciberdelincuencia con 85 votos a favor y ningún voto en contra ni abstención.

- La Resolución legislativa que aprueba el Convenio sobre Ciberdelincuencia es la 30913

- En la (Resolución Legislativa N° 30913, 2019), se realiza las siguientes reservas:

  a. De conformidad con lo dispuesto en el párrafo 3 del artículo 6 del Convenio sobre la Ciberdelincuencia, la República del Perú se reserva el derecho de no aplicar el artículo 6, párrafo 1, literal b del Convenio.

  b. De conformidad con el numeral 4 del artículo 9 del Convenio sobre la Ciberdelincuencia, la República del Perú considera que el bien jurídico tutelado en el derecho interno con respecto a la pornografía infantil es la libertad y/o indemnidad sexual de un menor, por lo que formula una reserva a los literales b) y c) del párrafo 2 del citado artículo, debido a que las conductas contempladas en dichas disposiciones no involucran la participación de un menor de edad.

  c. Conforme al numeral 4 del artículo 29 del Convenio sobre la Ciberdelincuencia, la República del Perú se reserva el derecho a denegar la solicitud de conservación en virtud de dicho artículo en el caso que

tenga motivos para creer que, en el momento de la revelación de los datos, no se cumplirá con la condición de la doble tipificación penal.

2.3.4. Casos

El portal web (MADE FOR MINDS, 2019), se mencionan seis casos de ataques cibernéticos, entre los cuales las víctimas han sido algunos Estados.

2014. Presunto ataque de Corea del Norte a Sony

En noviembre de 2014, Sony Pictures sufrió un ataque cibernético después de que un grupo de hackers que se llamaban a sí mismos Guardianes de la Paz obtuvieran acceso a la red de computadoras de la compañía. Corea del Norte negó su responsabilidad, sin embargo explico el ataque como una "acción justa" en respuesta a la película de Sony "La entrevista", una comedia que explico la muerte violenta de Kim Jong-un de Corea del Norte.

2015. Ataque a red eléctrica de Ucrania

En diciembre de 2015, unas 230.000 personas quedaron hasta seis horas en la oscuridad después de que piratas informáticos se infiltraran en tres compañías de energía y cerraran temporalmente los generadores en tres regiones de Ucrania.

El servicio de seguridad de Ucrania culpó al Régimen ruso por el ataque. Se estima que este ataque es la primera ocasión que piratas

informáticos tienen la posibilidad de atacar exitosamente una red de repartición de electricidad.

2016. Elecciones presidenciales en Estados Unidos

Piratas informáticos filtraron miles de correos electrónicos del Comité Nacional Demócrata (DNC), la junta directiva del Partido Demócrata, durante las elecciones presidenciales de 2016. La filtración avergonzó al liderazgo del partido, quien expresó su desdén en algunos correos electrónicos por la campaña de Bernie Sanders, un candidato que había competido con Hillary Clinton para convertirse en el candidato presidencial del partido. El Departamento de Justicia de Estados Unidos acusó más tarde a 12 rusos –que se cree son agentes de la agencia de inteligencia militar de Rusia.

2017. WannaCry

Un ataque con un ransomware conocido como WannaCry infectó a unas 300.000 computadoras en 150 países en mayo de 2017. El software cifró los archivos y exigió a los usuarios entregar cientos de dólares a cambio de claves para descifrar los archivos.

El ataque afectó a hospitales, incluidos muchos pertenecientes al Servicio Nacional de Salud (NHS) del Reino Unido, bancos y otras empresas. La compañía FedEx dijo que había perdido cientos de millones de dólares como resultado del ataque. Estados Unidos y Reino Unido culparon a Corea del Norte, una acusación que Pyongyang negó y que calificó de "grave provocación política".

2019. Ataque del Bundestag alemán

En enero de 2019, la Oficina Federal de Seguridad de la Información de Alemania (BSI) dijo que estaba investigando un ataque cibernético contra cientos de políticos, incluida la canciller alemana, Angela Merkel. El ataque cibernético se dirigió a todos los partidos en el Parlamento alemán, excepto al partido de extrema derecha Alternativa para Alemania (AfD).

CAPÍTULO III: RESULTADO Y ANÁLISIS DE LOS HALLAZGOS

3.2. Resultados del estudio

3.2.1. Casos en el Perú

Caso Clonación de tarjetas. Para el Hurto de Fondos

Imagen N° 01

Fuente: http://190.117.81.252/files/criminalistica/delito.pdf

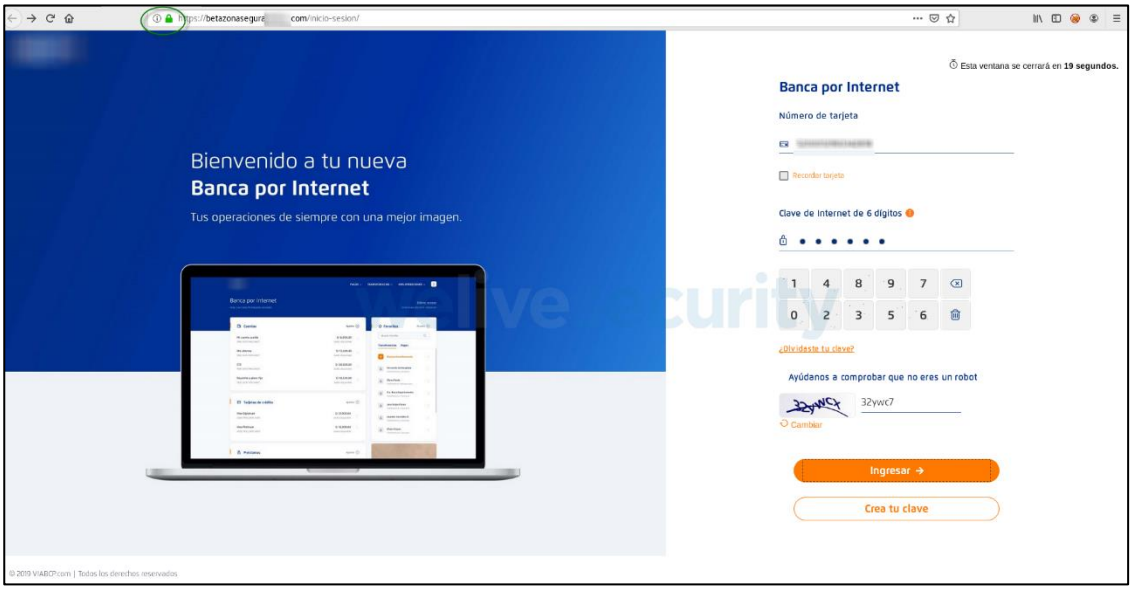
Caso Phishing:

Cuando llega al móvil o correo electrónico un mensaje de una entidad financiera, que también ve perjudicada su imagen.

Imagen N° 02

Fuente: http://190.117.81.252/files/criminalistica/delito.pdf

Imagen N° 03



Fuente: https://www.welivesecurity.com/la-es/2019/12/13/phishing-apunta-clientes-banco-bcp-peru-robar-informacion-financiera/

La figura N° 03 corresponde a un caso acontecido en 2018, como consecuencia de un ataque informático que sufrió el BCP, el cual, permitió a terceros acceder a datos de identificación personal de un grupo de clientes, números de tarjetas, cuentas y saldos.

El caso es que un sitio phishing **suplantaba** la identidad del BCP, a fin de robar los datos de tarjetas de crédito y debido y del número de DNI.

En el Perú el Phishing, esta está penalizada hasta con cuatro años de pena privativa de la libertad por el artículo 2 de la Ley 30096 señala:

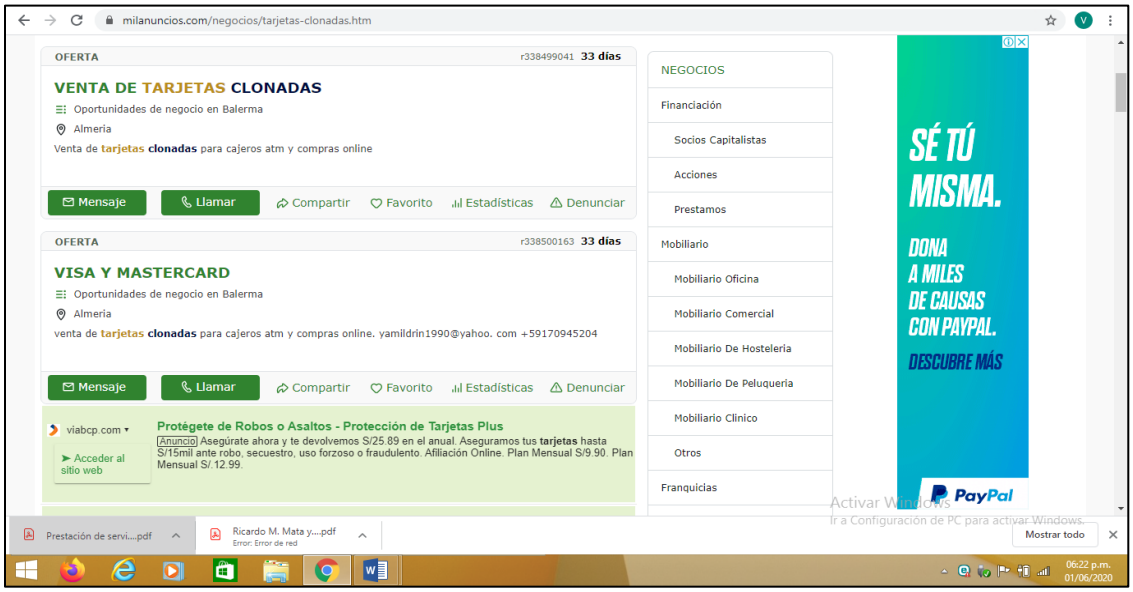
> El que accede sin autorización a todo o parte de un sistema informático, siempre que se realice con vulneración de medidas de seguridad establecidas para impedirlo, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días multa.
>
> Será reprimido con la misma pena el que accede a un medio informático excediendo lo autorizado

Imagen N° 04

Fuente: https://www.welivesecurity.com/la-es/2019/12/13/phishing-apunta-clientes-banco-bcp-peru-robar-informacion-financiera/

Caso de tarjetas clonada que es vendida en Internet.

Imagem N° 05



Fuente: https://www.milanuncios.com/negocios/tarjetas-clonadas.htm

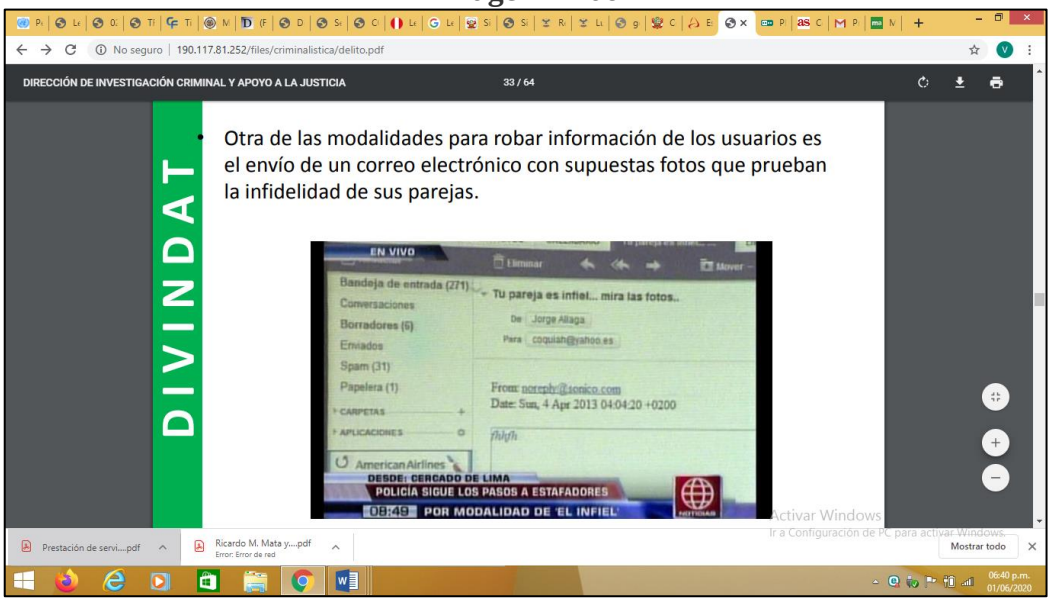
Para el caso de la figura número 01 y número 04, la clonación de tarjetas:

Sucede cuando se duplica una tarjeta mediante la falsificación de la banda magnética. Los estafadores copian la banda magnética de tu tarjeta pasándola por un sakimmer (deposito que almacena los datos de la banda magnética). Además, se encarga de conocer tu clave secreta. (scotiabank, 2020)

La Clonación de tarjetas esta conducta está penalizada por el Artículo 8. Fraude informático de la Ley 30096 que señala, El que, a través de las tecnologías de la información o de la comunicación, procura para sí o para otro un provecho ilícito en perjuicio de tercero mediante el diseño, introducción, alteración, borrado, supresión, clonación de datos informáticos o cualquier interferencia o manipulación en el funcionamiento de un sistema informático, será reprimido con una pena privativa de libertad no menor de tres ni mayor de ocho años y con sesenta a ciento veinte días multa. La pena será privativa de libertad no menor de cinco ni mayor de diez años y de ochenta a ciento cuarenta días multa cuando se afecte el patrimonio del Estado destinado a fines asistenciales o a programas de apoyo social

Caso de vírus Troyano

Imagen N° 06



Fuente: http://190.117.81.252/files/criminalistica/delito.pdf

Esta conducta está penalizada por Artículo 3. de la ley 30096, referido al **atentado a la integridad de datos informáticos**. "El que deliberadamente daña, introduce, borra, deteriora, altera, suprime o hace inaccesibles datos informáticos, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días multa".

Caso Suplantación de identidad de beneficiarios de bono universal familiar (2020).

Imagen N° 07

Fuente: https://infomercado.pe/hackers-roban-en-web-de-bono-familiar-universal-casi-un-millon-de-soles/

Esta conducta (Figura 4 y 7) está penalizada por Artículo 9. de la ley 30096, referido a la **Suplantación de Identidad.** "El que, mediante las tecnologías de la información o de la comunicación suplanta la identidad de una persona natural o jurídica, siempre que de dicha conducta resulte algún perjuicio, material o moral, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años"

Precisando que el presente caso se encuentra en investigación. Se trataría de un caso en que Hakers suplantaron la identidad de los verdaderos beneficiarios del bono familiar universal de 760 soles a fin de hacerse del dinero. Esto fue advertido por 2 especialistas Mauricio y Camilo, que habrían advertido el caso y las evidencias fueron puestas en conocimiento de la Fiscalía.

3.3. Discusión y contrastación teórica de los hallazgos

En la parte final del presente trabajo, corresponde contrastar los aspectos desarrollados sobre los delitos informáticos en el Perú y la suscripción del Convenio de Budapest, con los problemas y objetivos

Para ello es oportuno tener presente nuestros problemas y lo objetivos, así:

General.	**General.**
¿De qué manera la suscripción del convenio de Budapest influye en el tratamiento de los delitos informáticos?	Explicar la manera en que la suscripción del convenio de Budapest influye en el tratamiento de los delitos informáticos

Específicos.	**Específicos.**
¿Cuál es el desarrollo legislativo de los delitos informáticos en el Perú? ¿Cuál es la problemática actual generada por los delitos informáticos en el Perú? ¿Cómo es la legislación de delitos informáticos en países sudamericanos que suscribieron el convenio de Budapest? ¿Cuáles son los efectos que produce suscripción del convenio de Budapest?	- Describir es el desarrollo legislativo de los delitos informáticos en el Perú - Analizar la problemática actual generada por los delitos informáticos en el Perú - Analizar la legislación de delitos informáticos en países sudamericanos que suscribieron el convenio de Budapest - Identificar los efectos que produce suscrición del convenio de Budapest

Correspondiendo analizar el problema general y el objetivo general, para luego articularlos con los problemas y objetivos específicos en base a las categorías de estudio para finalmente llegar a exponer las conclusiones

3.3.1. Influencia de la Suscripción de Convenio de Budapest en el tratamiento de los delitos informáticos

El problema general formulado viene a ser: ¿De qué manera la suscripción del convenio de Budapest influye en el tratamiento de los delitos informáticos?, al que le corresponde el objetivo general, que es, Explicar la manera en que la suscripción del convenio de Budapest influye en el tratamiento de los delitos informáticos.

La influencia de la Suscripción del Convenio de Budapest en el tratamiento de los delitos informáticos en el Perú ha sido relativa, por cuanto, no ha trascendido más allá de la adecuación normativa de nuestro país en relación a los delitos informáticos y la promoción de desarrollar tecnología informática. conforme se encuentra descrito a lo largo del Desarrollo Temático, para cuyo fin se ha recurrido a la doctrina, legislación comparada y el propio convenio; precisando que, aun cuando su influencia en el tratamiento de los delitos informáticos es relativa, debe entenderse que esta influencia resulta positiva, al permitido asumir un compromiso de acortar las brechas tecnológicas y dificultades técnicas por parte del Estado, gracias a que existe la posibilidad de recurrir a la cooperación internacional.

La influencia de la suscripción del Convenio de Budapest, se puede advertir en la parte referida a la complementación a nuestra legislación. Así como la implementación de políticas de Gobierno Digital, de políticas de

ciberseguridad con una autoridad competente que descansa en la Presidencia del Consejo de Ministros.

Sin embargo, en el tratamiento mismo de los delitos informáticos, no se ha percibido una clara influencia, por cuanto aún no se han visto casos de cooperación internacional frente a la comisión de algún delito informático que haya merituado recurrir a dicha cooperación. Por cuanto, los delitos informáticos que se cometen en nuestro país, resulta tener mayor trascendencia a nivel interno.

3.2.1. Desarrollo legislativo de los delitos informáticos en el Perú

El primer problema específico formulado viene a ser: ¿Cuál es el desarrollo legislativo de los delitos informáticos en el Perú? al que le corresponde el primer objetivo general, que es, Describir es el desarrollo legislativo de los delitos informáticos en el Perú.

El desarrollo legislativo de los delitos informáticos en el Perú, ha sido abordado en el numeral 2.3.1. del sub capítulo III del Desarrollo Temático, el cual describe: Que la regulación de delitos informáticos en el Perú se ha desarrollado desde que, en 1991, el Código Penal tipifico en el artículo 186, inciso 3, segundo párrafo los delitos informáticos. Posteriormente, se promulgo la Ley 30096 (Ley de Delitos Informáticos). Esta Ley de Delitos Informáticos está conformada por siete capítulos que se estructuran de la siguiente manera: finalidad y objeto de la ley (Capítulo I), delitos contra datos

y sistemas informáticos (Capítulo II), delitos informáticos contra la indemnidad y libertad sexual (Capítulo III), delitos informáticos contra la intimidad y el secreto de las comunicaciones (Capítulo IV), delitos informáticos contra el patrimonio (Capítulo V), delitos informáticos contra la fe pública (Capítulo VI) y las disposiciones comunes (Capítulo VII). Posteriormente se promulgó la Ley 30171 (Ley que modifica la Ley 30096, Ley de Delitos Informáticos). Para finalmente, suscribir el convenio sobre la cibercriminalidad (Convenio de Budapest) en 2019.

Actualmente, la legislación referida a delitos informáticos comprende la siguiente tipificación:

- DELITOS CONTRA DATOS Y SISTEMAS INFORMÁTICOS
- DELITOS INFORMÁTICOS CONTRA LA INDEMNIDAD Y LIBERTAD SEXUAL
- INFORMACIÓN CONTRA LA INTIMIDAD Y EL SECRETO DE LAS COMUNICACIONES
- DELITOS INFORMATICOS CONTRA EL PATRIMONIO
- DELITOS INFORMÁTICOS CONTRA LA FÉ PÚBLICA

3.2.2. Problemática actual generada por los delitos informáticos en el Perú

El segundo problema general formulado viene a ser: ¿Cuál es la problemática actual generada por los delitos informáticos en el Perú? al que le corresponde el segundo objetivo general, que es, Describir la problemática actual generada por los delitos informáticos en el Perú.

La problemática actual generada por los delitos informáticos en el Perú, ha sido desarrollada en el numeral 2.3.5. de Desarrollo Temático, cuyo análisis viene a ser:

Ante, el uso y acceso cada vez más frecuente de los dispositivos electrónicos en el ciberespacio, a las telecomunicaciones, y el acceso a internet, ha permitido facilitar las actividades del ser humano, sin embargo, representa un espacio cómodo y propicio para los ciberdelincuentes.

La realidad nos muestra la frecuencia con que estos se viene cometiendo; según el portal (ANDINA AGENCIA DE NOTICIAS, 2018) son tres las principales modalidades de delitos informáticos que afectan a usuarios y empresas en el Perú, estos son, **ransomware, phishing y cryptojacking**; que, ha sido corroborado por la empresa ESET Segurity Report citada por (ANDINA AGENCIA DE NOTICIAS, 2019) que advierte, que al menos 57% de las empresas peruanas sufrieron un ataque de ransomware y entre los sectores afectados están el sector de tecnología, educación y salud.

La empresa antes mencionada, ha señalo en el 2019 que Perú es el país que menos implementa políticas para gestionar la ciberseguridad de las empresas; esto, representa uno de los factores por los cuales el Perú se encuentra en primera ubicación en Latinoamérica, de manera que, los datos reflejan una situación de vulnerabilidad ante ciertos delitos informáticos.

Otros incidentes de seguridad de la información, que se presentan en nuestro país son: a) Infección con códigos malicioso, b) Acceso indebido a sistemas, c) Uso inapropiado de la infraestructura, d) Robo de información, e) Privación y/o Secuestro de información, g) Ataques de ingeniería social o phishing. Esto ubica al Perú, como el tercer país más afectado con los programas Spyware, después de Brasil y México:

En el escenario judicial, según los datos proporcionados por (INSTITUTO NACIONAL DE ESTADISTICA E INFORMÁTICA, 2017), las sentencias emitidas por la comisión de delitos informáticos contra el patrimonio según delito específico, en el año 2016 asciende a 04, y para el año 2017 se sentenciaron a 02 personas. Sin embargo, se han emitido 33 sentencias por la comisión de delitos informáticos cometidos según ley especial.

A manera de ejemplo, él (DIARIO OFICIAL EL PERUANO, 2020) nos brinda datos de los casos más frecuentes presentados en el 2019, precisa que las denuncias están referidas a la **suplantación de identidad en redes sociales y plataformas de internet, mediante la creación de perfiles falsos;** denuncias que en el 2018 ascendieron 227 y en el 2019 alcanzaron a 247 denuncias registrados por la Policía Nacional del Perú.

La problemática que enfrenta el Perú es sin duda delicada; normalmente los ataques buscan robar información, identidades o crédito, generar fraude, afectar sistemas informáticos, atentar contra la integridad sexual de menores de

edad, atentar contra la administración pública, entre otros; siendo el eslabón más débil y más vulnerable de toda organización es la persona.

3.2.3. Legislación de delitos informáticos en países sudamericanos que suscribieron el convenio de Budapest

El tercer problema general formulado viene a ser: ¿Cómo es la legislación de delitos informáticos en países sudamericanos que suscribieron el convenio de Budapest?, al que le corresponde el tercer objetivo general, que es, Analizar la legislación de delitos informáticos en países sudamericanos que suscribieron el convenio de Budapest.

La legislación de delitos informáticos en países sudamericanos que han suscrito el Convenio ha sido uniformizada en atención al contenido del mencionado Convenio; se arriba a una uniformización, por cuanto cada país tenía una regulación particular. esto se ha señalado en los numerales 2.2.7.4; 2.2.7.5; 2.2.7.6, del Desarrollo Temático, cuando nos hemos referido a países como: **Chile**, que fue el primer país latinoamericano en sancionar una Ley contra Delitos Informáticos. La Ley N° 19223 fue publicada en el Diario Oficial el 7 de junio de 1993, que en un corto articulado tipifica y sanciona la destrucción o inutilización de un sistema de tratamiento de información. Actualmente su legislación se encuentra adecuada de conformidad a lo regulado en el Convenio de Ciberdelincuencia de Budapest. En **Colombia**, la expedición de la ley 527 de 1999 obedeció a la necesidad jurídica de las

transacciones electrónicas; el Código Penal colombiano cuenta con un único artículo, el 195, que bajo el epígrafe de "acceso abusivo de un sistema informático" (hanking en otras legislaciones), Y actualmente se alinea a lo regulado en el Convenio de Ciberdelincuencia de Budapest. Finalmente, **Argentina** el 4 de junio de 2008 promulga Ley 26388 que modificó el Código Penal para incluir delitos informáticos, teniendo en su contenido temas como: Distribución y tenencia con fines de distribución de pornografía infantil; violación de correos electrónicos; acceso ilegítimo a sistemas informáticos; daño informático y distribución de códigos maliciosos; interrupción de comunicaciones o DoS. El 4 de diciembre de 2013 se publicó la Ley Grooming, Ley N° 26904, que responde a una necesidad de proteger a menores de edad en la comunicación cibernética; siendo así, se incorporó en el Código Penal artículo 131. Actualmente su legislación se alineó a lo regulado en el Convenio de Ciberdelincuencia de Budapest.

3.2.4. Efectos que produce suscripción del Convenio de Budapest

El cuarto problema general formulado viene a ser: ¿Cuáles son los efectos que produce suscripción del convenio de Budapest?, al que le corresponde el cuarto objetivo general, que es, Identificar los efectos que produce suscrición del convenio de Budapest.

Los efectos que produce la suscripción del Convenio de Budapest, han sido identificados y precisado en el sub capítulo II del desarrollo temático, específicamente en el numeral 2.2.7. precisando que estos son:

Permite aplicar una política penal común con objeto de proteger a la sociedad frente a la ciberdelincuencia, mediante la adopción de una legislación adecuada.

Por otro lado, la suscripción de Convenio ha motivado el desarrollo de tecnologías de la información, usar herramientas establecidas en el mismo Convenio para prevenir delitos que pongan en riesgo o abusen de sistemas y datos informáticos.

Lograr cooperación en materia penal rápida y fiable, lo que fortalecerá las capacidades de detección, investigación y sanción de los Estados Parte para la lucha efectiva contra los delitos previstos en los artículos del capítulo II del Convenio. Conseguir la aplicación de programas técnicos y de capacitación sobre la ciberdelincuencia y temas afines patrocinados por el Consejo de Europa y otras organizaciones internacionales. y permitir la participación de actores clave de suma importancia para una mejor lucha contra la ciberdelincuencia como son: otros Estados, agencias, el sector privado y la sociedad civil.

CONCLUSIONES

PRIMERA: La suscripción del Convenio de Budapest, influye de manera relativa en el tratamiento de los delitos informáticos, al centrarse en la adecuación de nuestra normatividad a la prevista en el mencionado Convenio, como es establecer un catálogo de delitos, establecer normas procesales orientadas a salvaguardar las evidencias digitales y recurrir a la cooperación internacional para investigar la comisión de este tipo de delitos; y la principal característica que es la cooperación internacional para investigar casos trascedentes, la cual ha tenido mínima aplicación desde su suscripción.

SEGUNDA: El desarrollo legislativo de los delitos informáticos en el Perú ha sido progresivo y rápido en un periodo de 30 años que comienza en 1991 con la tipificación de estos delitos en el artículo 207 del Código Penal, pero, sobre todo desde el año 2013 con la promulgación de la ley 30096 y las modificaciones realizadas en con la Ley 30171, hasta la suscripción del Convenio en mención, permitiendo contar en la actualidad con legislación equiparable a la legislación comparada de delitos informático.

TERCERA: La problemática actual causada por la comisión de delitos informáticos en el Perú es creciente; obedece al acceso y uso de diversos y novedosos medios tecnológicos por parte de los ciberdelincuentes, situación que hace difícil su identificación y ubicación. En América Latina en el año 2017 el Perú ha sido el más afectado con los programas ransomware con un 25.1% del total de casos presentado; para el 2019, nuestro país era el tercer país en América latina más afectados con programas Spyware; el mismo años se presentaron 3012 denuncias por fraude informático y 247 denuncias sobre suplantación de identidad en la Divindat); se suma a ello, el escaso presupuesto destinado a contar con tecnología de alta gama para la persecución de este tipo de delitos.

CUARTA: La legislación sobre delitos informáticos de países sudamericanos que suscribieron el convenio de Budapest es uniforme y permite una integración generada a partir de la cooperación internacional promovida por dicho Convenio

QUINTA: Los efectos de suscribir el Convenio de Budapest, son positivos a nivel legislativo, porque permite contar con un catálogo integral de delitos informáticos, sin embargo, se requieren de políticas orientadas a destinar recursos económicos para el equipamiento de la tecnología informativa que permita hacer frente a los delitos informáticos.

RECOMENDACIONES

PRIMERA: Utilizar la cooperación internacional habilitada por el Convenio de Budapest para investigar la comisión de delitos informáticos transnacionales que tengan incidencia en nuestro país.

SEGUNDA: Al contar con una legislación de delitos informáticos orientada por la Convención y equiparable a la legislación comparada, sería oportuno establecer políticas de difusión destinadas a dar a conocer e informar a los estudiantes del nivel secundario de los procedimientos y mecanismos de ciberseguridad que deben considerar a fin de reducir el nivel de riesgo potencial en el que se encuentran.

TERCERA: A fin de abordar la problemática causada por la comisión de delitos informáticos, se recomienda equipar las instituciones encargadas de la investigación y seguimiento de los delitos informáticos, con los instrumentos y la tecnología informática que resulte más óptima la persecución de estos delitos y evitar la impunidad ante su comisión.

CUARTA: Invitar a los países Sudamericanos que aún han no han suscrito el Convenio de Budapest a ratificarlo a fin de contar con un bloque sudamericano de cooperación internacional para hacer frente a los ciberdelincuentes que cometen estos los delitos informáticos, más aún por tratarse de un asunto de seguridad nacional.

QUINTA: Que el Ministerio de Economía asigne un presupuesto considerables destinado para la ciberseguridad de nuestro país.

BIBLIOGRAFÍA

ANDINA, Agencia Peruano de Noticias (16 de enero de 2020). Recuperado el 3 de abril de 2020, de https://andina.pe/agencia/noticia-estos-son-los-delitos-informaticos-mas-frecuentes-el-peru-segun-policia-781320.aspx

ACURIO DEL PINO, S. (s.f.). *oas.org/juridico.* Recuperado el 14 de Abril de 2020, de oas.org/juridico: https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

ANDINA. (4 de Junio de 2018). *portal.andina.pe*. Obtenido de portal.andina.pe: https://portal.andina.pe/edpespeciales/2018/ciberataques-peru/index.html

ANDINA AGENCIA DE NOTICIAS. (7 de Noviembre de 2019). *andina.pe*. Obtenido de andina.pe: https://andina.pe/agencia/noticia-ransomware-es-uno-de-ciberataques-mas-afecta-a-peruanos-772229.aspx

ANDINA AGENCIA DE NOTICIAS. (23 de Octubre de 2019). *andina.pe/agencia/noticia-peru-*. Obtenido de andina.pe/agencia/noticia-peru-: https://andina.pe/agencia/noticia-peru-entre-los-paises-mas-victimas-programas-maliciosos-espia-770616.aspx?fbclid=IwAR3fFiRAZFP_DJwLXyIE9LnhgktwTxorwQDoax9YxyPk7ImoIAebp-E2edc

AO KASPERSKY LAB. (2020). *latam.kaspersky.com*. Obtenido de latam.kaspersky.com: https://latam.kaspersky.com/resource-center/definitions/what-is-ransomware

BANCO INTERAMERICANO DE DESARROLLO. (2016). Obtenido de https://publications.iadb.org/es/publications/spanish/document/Ciberseguridad-%C2%BFEstamos-preparados-en-Am%C3%A9rica-Latina-y-el-Caribe.pdf

BUSINESS ALLIANCE FOR SECURE COMMERCE CAPÍTULO PERÚ. (2019). Marina de Guerra del Perú crea la Comandancia de Ciber defensa. *Cargo SECURITY N° 38*, 16-17. Obtenido de https://www.bascperu.org/pdf/principales/REVISTA-38_opt.pdf

CONVENIO DE CIBERDELINCUENCIA DE BUDAPEST. (2001). Obtenido de https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

COUNCIL OF EUROPE PORTAL. (26 de 05 de 2020). Obtenido de https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=oJ83l4Km

CYBERSEGURITY EXPERTS YOUR SIDE ESET. (2019). *security-report.eset-la.com/*. Obtenido de security-report.eset-la.com/: https://security-report.eset-la.com/

DIARIO OFICIAL EL PERUANO. (26 de Enero de 2020). *elperuano.pe/noticia.* Obtenido de elperuano.pe/noticia: https://www.elperuano.pe/noticia-crecen-denuncias-perfiles-falsos-89076.aspx

DIMUCCIO, B. (23 de enero de 2019). *Glosario de Terminos Informáticos.* Aragua - Venezuela: Ministerio de Educación. Obtenido de https://es.slideshare.net/giovainina/glosario-informatico-pdf

DIVISIÓN DE INVESTIGACIÓN DE DELITOS DE ALTA TECNOLOGÍA. (s.f.). Recuperado el 28 de Mayo de 2020, de http://190.117.81.252/files/criminalistica/delito.pdf

EL CONVENIO BUDAPEST EN AMERICA LATIN*a*. (Marzo de 2018). Obtenido de https://adc.org.ar/wp-content/uploads/2019/06/035-la-convencion-de-cibercrimen-de-budapest-y-america-latina-vol-1-03-2018.pdf

FRAGOSO, E. (2004). Un poc de historia de a Internet y. *Revista CONAMED*, 30-35.

HALL, A. (s.f.). *gestiondelriesgo.com*. Recuperado el 23 de Mayo de 2020, de gestiondelriesgo.com: http://www.gestiondelriesgo.com/artic/discipl/disc_4016.htm

HENNESSY, J., & PATTERSON, D. (1993). *Arquitectura de Computadores Un Enfoque Cuantitativo.* Madrid: McGraw Hill.

HERNÁNDEZ MENDOZA, F. (2003). *Apuntes para la Asignatura Informática I.* Ciudad de México: Fondo Editorial F.C.A.

HERNANDEZ SAMPIERI, R., Fernández Collado, C., & Baptista Lucio, P. (2014). *Metodología de la Investigación.* México: MgGRAYW HILL / INTERAMERICANA EDITORES S.A.

INSTITUTO NACIONAL DE ESTADISTICA E INFORMÁTICA. (2017). Personas con sentencia condenatoria por delitos contra el patrimonio. *Anuario Estadístico de la Criminalidad y Seguridad Ciudadana, 2011-2017*, 123.

KATERIN, j. (28 de Mayo de 2019). *es.slideshare.net*. Recuperado el 29 de Mayo de 2020, de es.slideshare.net: https://es.slideshare.net/katerinjohana08/delitos-informticos-148034236

MADE FOR MINDS. (01 de Enero de 2019). *dw.com/es*. Obtenido de dw.com/es: https://www.dw.com/es/seis-ataques-cibern%C3%A9ticos-que-sacudieron-el-mundo/a-46967214

MOISÉS BARRIOS, A. (2017). *Ciberdelitos Amenazas Criminales del Ciberespacio.* Madrid: REUS.

ORANTES, K. (05 de octubre de 2019). *estrategiaynegocios.net*. Recuperado el 14 de Marzo de 2020, de estrategiaynegocios.net: https://www.estrategiaynegocios.net/centroamericaymundo/1324152-330/kevin-mitnick-de-hacker-a-mr-seguridad

ORGANIZACIÓN DE LAS NACIONES UNIDAS. (Abril de 2015). *13° Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal.* Doha. Recuperado el 11 de Mayo de 2020, de https://www.unodc.org/documents/congress/Documentation/A-CONF.222-12_Workshop3/ACONF222_12_s_V1500666.pdf

OXMAN, N. (2013). Estafa Informática a través de Internet: Acerca de la imputación penla del "Phishing" y el "Pharming". *Revista de Derecho de la Pontificia Universidad Católica de Valparaíso*, 211-262.

PEÑA CABRERA FREYRE, A. R. (2011). *Derecho Penal - Parte Especial* (3° ed., Vol. II). Lima: Idemsa.

PEÑA-CABRERA FREYRE, A. R. (2011). *Derecho Penal - Parte Especial.* Lima: Idemsa.

RESOLUCIÓN LEGISLATIVA N° 30913. (12 de Febrero de 2019). Resolución Legislativa que aprueba el Convenio sobre Ciberdelincuencia.

RODRÍGUEZ GARCÍA, M. (02 de Enero de 2019). *AmbitoJurídico.* Obtenido de AmbitoJurídico.com.br: http://www.ambito-juridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=8101

SECRETARÍA DE GOBIERNO DIGITAL. (28 de Mayo de 2020). *gob.pe*. Obtenido de gob.pe: https://www.gob.pe/7025-presidencia-del-consejo-de-ministros-secretaria-de-gobierno-digital/

SEGUIN, P. (30 de Abril de 2020). *avast.com/es*. Obtenido de avast.com/es: https://www.avast.com/es-es/c-spyware

TEMPERINI, M. G. (2013). *conaiisi.unsl.edu.ar* . Recuperado el 14 de marzo de 2020, de conaiisi.unsl.edu.ar: http://conaiisi.unsl.edu.ar/ingles/2013/82-553-1-DR.pdf

VELÁZQUES ELIZARRARÁS, J. C. (2007). *El estudio de caso en las relaciones jurídicas internacionales – Modalidad de aplicación en el derecho internacional.* Mexico: Universidad Nacional Autónoma de Mexico.

VELLOSO, F. (2011). *Informática - Conceitos Básicos.* Sao Paulo: Elsevier.

VILLAVICENCIO TERREROS, F. (2014). Delitos Informáticos. *IUS ET VERITAS*, 291.

VILLAVICENCIO TERREROS, F. (2014). Delitos Informáticos. *IUS ET VERITAS*, 288-289.

WATSON, P. (31 de Agosto de 2019). *infodefensa.com/latam*. Obtenido de infodefensa.com/latam: https://www.infodefensa.com/latam/2019/08/31/noticia-congreso-promulga-ciberdefensa.html

YÚBAL FM. (29 de Abril de 2017). *xataka.com*. Obtenido de xataka.com: https://www.xataka.com/historia-tecnologica/la-historia-de-creeper-el-primer-virus-informatico-jamas-programado

ZARICH, F. (2005). Propiedad Intelectual del Software. En F. ZARICH, *Derecho Informático* (págs. 23-35). Rosario - Argentina: Juris.

ANEXO

Matriz de Consistencia

PROBLEMAS	OBJETIVOS	HIPOTESIS	CATEGORIAS	METODOLOGIA	TECNICA	UNIDAD DE ANALISIS Y MUESTRA
General. ¿De qué manera la suscripción del convenio de Budapest influye en el tratamiento de los delitos informáticos? **Específicos.** ¿Cuál es el desarrollo legislativo de los delitos informáticos en el Perú? -¿Cuál es la problemática actual generada por los delitos informáticos en el Perú? -¿Cómo es la legislación de delitos informáticos en países sudamericanos que suscribieron el convenio de Budapest? -¿Cuáles son los efectos que produce suscripción del convenio de Budapest?	**General.** Explicar la manera en que la suscripción del convenio de Budapest influye en el tratamiento de los delitos informáticos **Específicos.** - Describir es el desarrollo legislativo de los delitos informáticos en el Perú - Analizar la problemática actual generada por los delitos informáticos en el Perú - Analizar la legislación de delitos informáticos en países sudamericanos que suscribieron el convenio de Budapest - Identificar los efectos que produce suscrición del convenio de Budapest	**General** La suscripción del convenio de Budapest influye relativamente en el tratamiento de los delitos informáticos, dado que son la principal característica es la cooperación internacional para combatir los mencionados delitos, la misma que no ha tenido mínima aplicación desde la suscripción. **Específicos.** El desarrollo de la legislación sobre delitos informáticos en el Perú ha sido progresivo y rápido, llegando a equipararse con legislación comparada en la materia. La problemática actual generada por los delitos informáticos en el Perú es cada vez más creciente, dado que los medios cibernéticos utilizados por los ciberdelincuentes son cada vez más diversos, haciendo difícil su identificación, sumado a ello, el escaso presupuesto destinado a destinado para contar con tecnología de alta gama que permita su persecución. La legislación de algunos países -sudamericanos- como Chile y Argentina. que suscribieron el convenio de Budapest resulta ser más rígida. Entre los efecto que produce la suscripción del convenio de Budapest, tenemos: La creación de un marco común de derecho penal sustantivo, la estandarización de procesos penales y la cooperación internacional	**Categoría 1.** **Delitos Informáticos** - Delincuencia Informática - Bien Jurídico Protegido - Sujetos del Delito - Tipos de Delitos Informáticos - Delitos de acceso ilícito **Categoría 2.** **Convenio de Budapest** - Temas regulados - Contenido - Países suscribientes - Convención de Budapest y América Latina - Incidencia en Perú	**Enfoque de investigación:** **Cualitativo:** Puesto que el estudio se basa fundamentalmente en la descripción y la argumentación antes que en mediciones datos estadísticos. **Tipo de investigación:** **Descriptiva Jurídica comparativa:** Porque con este tipo de investigación se realizará una investigación Jurídico-comparativa de la legislación comparada, orientada a la justificación de la suscripción de un convenio. (Según Clasificación del (Aranzamendi, 2015)	**Técnicas** - Análisis documental - Análisis de Legislación - Análisis de Doctrina **Instrumentos** - Ficha de análisis documental - Ficha doctrinario - Ficha de información electrónica (internet). - Ficha de análisis interpretativo normativo.	**Unidad de Análisis Temático** La presente investigación enfoca su análisis en las dos categorías: Delitos Informáticos y la suscripción del Convenio de Budapest. **Muestra no probabilística.** **- Criterios de selección** Casos nacionales