Universidad Científica del Perú - UCP
Registrado en el Asiento Nº A00010 de la Partida Nº 11000318, Personas Jurídicas de Iquitos, Superintendencia de los Registros Públicos - SUNARP

FACULTAD DE DERECHO Y CIENCIAS POLÍTICAS

PROGRAMA ACADÉMICO DE DERECHO

TESIS:

"INNOVACIONES EN LA TIPIFICACIÓN DE DELITOS CON LA RATIFICACIÓN DEL CONVENIO CONTRA EL CIBERCRIMEN, EN EL PERÚ EL AÑO 2019".

PARA OPTAR EL TITULO PROFESIONAL DE ABOGADO

AUTOR:

Bachiller Adria Solange GALLARDO GRANDA

ASESOR:

DR. Vladymir VILLAREAL BALBIN

Loreto – San Juan Bautista – Perú

2020

PÁGINA DE APROBACIÓN

Tesis sustentado en acto público el día Viernes 06 de Marzo del 2020, en la Facultad de Derecho y Ciencias Políticas de la Universidad Científica del Perú, identificado por el jurado calificador y dictaminador siguiente:

.....

Dr. José Napoleón Jara Martel
Presidente

.....

Dr. Fernando Martin Robles Sotomayor
Miembro

.....

Mag. Aldo Nervo Atarama Lonzoy
Miembro

.....

Dr. Vladymir Villareal Balbín
Asesor

DEDICATORIA

A mis padres Luis Gallardo y Jesús Granda por haberme apoyado incondicionalmente en todo momento, por sus consejos, sus valores, por la motivación constante que me ha permitido ser una personas de bien.

A mis hermanos Luis, Dayana y Antonella Gallardo por motivarme a seguir esforzándome en mis estudios y darles ese ejemplo a seguir en el desarrollo de sus vidas.

A mi Tío Pedro Gallardo por haber estado ahí apoyándome, aconsejándome como un segundo padre, sintiéndose orgulloso de todos mis logros obtenidos.

A mis Abuelos que se encuentran descansando en la eternidad, que siempre me apoyan desde arriba para lograr mis metas.

A mi novio Francisco Herrera Noel por apoyarme de manera desinteresada en mi vida universitaria hasta la actualidad, siendo el mejor compañero que me ha podido tocar en la vida, quien nunca me dejo rendir, entregando todo su tiempo y dedicación a todas las cosas para que todo vaya bien en mi camino profesional y personal.

Atte.

Adria Solange Gallardo Granda

AGRADECIMIENTO

A Dios, por darme la vida y porque me ha permitido seguir adelante guiándome en los momentos difíciles en el transcurso de mi vida.

Expresar mi gratitud y agradecimiento a mi casa de formación profesional, Universidad Científica del Perú por la oportunidad de haberme permitido ampliar y profundizar mis convicciones y alcanzar este anhelado sueño.

Finalmente un eterno agradecimiento a esta prestigiosa Universidad, a mis docentes Carlos Da Silva Torres y Vladymir Villarreal Balbín, y a todos los que pasaron por mi etapa universitaria, por haberme brindado sus conocimientos, en mi etapa universitaria, lo cual va ayudarme a ser una profesional competitiva.

Atte.

Adria Solange Gallardo Granda

ACTA DE SUSTENTACIÓN

FACULTAD DE DERECHO Y CIENCIAS POLITICAS

UCP UNIVERSIDAD CIENTÍFICA DEL PERÚ

"Año de la Universalización de la Salud"

ACTA DE SUSTENTACIÓN DE TESIS

Con Resolución Decanal N° **037** del 03 de **febrero** de **2020**, la **FACULTAD DE DERECHO Y CIENCIAS POLITICAS DE LA UNIVERSIDAD CIENTÍFICA DEL PERÚ - UCP** designa como Jurado Evaluador y Dictaminador de la Sustentación de Tesis a los Señores:

- Dr. Jose Napoleon Jara Martel — Presidente
- Dr. Fernando Martin Robles Sotomayor — Miembro
- Mag. Aldo Nervo Atarama Lonzoy — Miembro

Como Asesor: **Dr. Vladymir Villareal Balbin**

En la ciudad de Iquitos, siendo las 19:00 horas del día **Viernes 06 de Marzo del 2020** en las instalaciones de la UNIVERSIDAD CIENTÍFICA DEL PERÚ - UCP, se constituyó el Jurado para escuchar la sustentación y defensa de la Tesis: **"Innovaciones en la Tipificación de los Delitos con la Ratificación del Convenio contra el Cibercrimen, en el Perú el año 2019"**
Presentado por la sustentante:

ADRIA SOLANGE GALLARDO GRANDA

Como requisito para optar el título profesional de: **Abogada**
Luego de escuchar la Sustentación y formuladas las preguntas las que fueron respondidas de forma: Satisfactoria
El jurado después de la deliberación en privado llegó a la siguiente conclusión:
La Sustentación es: Aprobada por Unanimidad

En fe de lo cual los miembros del jurado firman el acta.

Dr. José Napoleón Jara Martel
Presidente

Dr. Fernando Martin Robles Sotomayor
Miembro

Mag. Aldo Nervo Atarama Lonzoy
Miembro

CALIFICACIÓN:		
	Aprobado (a) Excelencia	: 19 – 20
	Aprobado (a) Unanimidad	: 16– 18
	Aprobado (a) Mayoría	: 13 – 15
	Desaprobado (a)	: 00 – 12

CONSTANCIA DE ORIGINALIDAD

UNIVERSIDAD CIENTÍFICA DEL PERÚ

"Año de la Universalización de la Salud"

CONSTANCIA DE ORIGINALIDAD DEL TRABAJO DE INVESTIGACIÓN

DE LA UNIVERSIDAD CIENTÍFICA DEL PERÚ - UCP

El presidente del Comité de Ética de la Universidad Científica del Perú - UCP

Hace constar que:

La Tesis titulada:

"INNOVACIÓN EN LA TIPIFICACIÓN DE DELITOS CON LA RATIFICACIÓN DEL CONVENIO CONTRA EL CIBERCRIMEN, EN EL PERÚ EL AÑO 2019".

De la alumna: **ADRIA SOLANGE GALLARDO GRANDA**, de la Facultad de Derecho y Ciencias Políticas, pasó satisfactoriamente la revisión por el Software Antiplagio, con un porcentaje de **18% de plagio**.

Se expide la presente, a solicitud de la parte interesada para los fines que estime conveniente.

San Juan, 11 de febrero del 2020.

Dr. César J. Ramal Asayag
Presidente del Comité de Ética – UCP

CJRA/lasda
021 -2020

Av. Abelardo Quiñones Km. 2.5 (065) 261088 www.ucp.edu.pe

URKUND

Urkund Analysis Result

Analysed Document: UCP_DER_2019_T_Adria Gallardo_V1.pdf (D63751935)
Submitted: 2/11/2020 4:05:00 PM
Submitted By: revision.antiplagio@ucp.edu.pe
Significance: 18 %

Sources included in the report:

1434392697_770__Delitos%252BInformaticos%252BPeru%252BGY-AA-FE-RS.pptx (D14849057)
1434635094_799__reporte_ley_colombia_grupo_1.pdf (D14871030)
1427688394_695__COIP_Patricio_Aguirre.pptx (D13968527)
Cibercriminalidad - Evolución de la delincuencia.pdf (D24862446)
INFORME DE TESIS YNCIO CORRALES YARA STHEFHANY.docx (D54368025)
CAPÍTULO 4.docx (D16252284)
https://es.wikipedia.org/wiki/Convenio_sobre_cibercriminalidad
https://www.eumed.net/rev/caribe/2018/12/delito-informatico-cuba.html
https://www.bcn.cl/obtienearchivo?id=repositorio/10221/26882/1/Convenio_de_Budapest_y_Ciberdelincuencia_en_Chile.pdf
https://alertas.directoriolegislativo.org/wp-content/uploads/2019/01/Exp.-12192-Delitos-Inform%C3%A1ticos.pdf
https://es.slideshare.net/aljathro/anlisis-del-dictamen-modificatorio-de-la-ley-30096-ley-de-delitos-informticos-del-per
https://rm.coe.int/16802fa446
https://es.slideshare.net/Derechotics/34849363-aproximacionlegalaltratamientodelosdelitosinformaticosencolombia
https://repositorio.uesiglo21.edu.ar/bitstream/handle/ues21/14464/SALLENT%20GARCIA%20Florencia.pdf?sequence=1&isAllowed=y
https://www.icmec.org/wp-content/uploads/2016/11/ICMEC_UNICEF_ES.pdf
https://busquedas.elperuano.pe/normaslegales/ley-de-delitos-informaticos-ley-n-30096-1003117-1/

Instances where selected sources appear:

176

INDICE DE CONTENIDO

INDICE DE CUADRO

INDICE DE GRÁFICO

RESUMEN

"INNOVACIONES EN LA TIPIFICACIÓN DE DELITOS CON LA RATIFICACIÓN DEL CONVENIO CONTRA EL CIBERCRIMEN, EN EL PERÚ EL AÑO 2019".

Por:

Bach. Adria Solange GALLARDO GRANDA.

Objetivo: Determinar las modificaciones en la tipificación de delitos que incorpora el Convenio contra el cibercrimen de Budapest en Perú el año 2019. El tipo de estudio fue Básica Descriptiva; el Diseño No experimental, descriptivo, correlacional, transversal. **Método:** La población es finita, al estar compuesta por el estudio de la tipificación de delitos por medios informáticos en tres documentos legales que son el Convenio contra el Cibercrimen de Budapest, la Ley de Delitos Informáticos y el Código Penal. La muestra corresponde al 100% de la población, centrando el estudio en los aspectos pertinentes de los tres dispositivos legales antes enunciados. **Resultados:** Se ha podido determinar que el Convenio contra el cibercrimen de Budapest, ratificado por el Perú el año 2019, existe un 57.14% de coincidencia, haciendo necesario modificar su tipificación del Art 4° de la Ley de Delitos Informáticos, pues la misma no incluye la totalidad de elementos objetivos que propone la Convención y respecto al delito de Falsificación Informática, hallamos un 0% de coincidencia, haciendo necesario implementar su regulación debido a que no se encuentra tipificado ni en el Código Penal ni en la Ley de Delitos Informáticos. **Conclusión:** Finalmente se ha podido verificar que es necesario la modificación del Art 4° "Atentado contra la integridad de sistemas informáticos" y la incorporación del delito informático de Falsificación Informática en el Capítulo referido a delitos contra la fe pública en la Ley N°30096 Ley de Delitos Informáticos.

Palabras claves: Delito Informático, cibercrimen, convenio de Budapest,

ABSTRACT

INNOVATIONS IN THE TIPIFICATION OF DELITIES WITH THE RATIFICATION OF THE CONVENTION AGAINST CIBERCRIMEN, IN THE YEAR 2019.

By:

Bach. Adria Solange GALLARDO GRANDA.

Objective: To determine the changes in the criminalization of the Budapest Cybercrime Convention in Peru in 2019. The type of study was Basic Descriptive; non experimental, descriptive, correlational, crosscutting design. **Method:** The population is finite, being composed of the study of the criminalization of crimes by computer means in three legal documents that are the Budapest Convention against Cybercrime, the Law on Computer Crimes and the Criminal Code. The sample corresponds to 100% of the population, focusing the study on the relevant aspects of the three legal devices listed above. **Results:** It has been determined that the Budapest Convention against Cybercrime, ratified by Peru in 2019, there is a 57.14% coincidence, making it necessary to amend its classification of Article 4 of the Computer Crimes Act, as it does not include the entire objective elements proposed by the Convention and with respect to the crime of Computer Counterfeiting, we find a 0% coincidence, making it necessary to implement its regulation because it is not typified either in the Criminal Code or in the Law on Computer Crimes. **Conclusion:** Finally, it has been possible to verify that it is necessary to amend Article 4 "Attack on the Integrity of Computer Systems" and the incorporation of the computer crime of Computer Counterfeiting into the Chapter related to crimes against public faith under the Computer Crimes Act.

Keywords: Computer Crime, Cybercrime, Budapest Convention,

CAPITULO I
MARCO TEÓRICO

1.1 ANTECEDENTES DEL ESTUDIO

Al efectuar la revisión de los antecedentes de investigaciones, se han encontrado que existen a nivel nacional e internacional, más no a nivel regional, por ser un tema que nunca ha sido investigado en las universidades de la región Loreto, motivo por el que se agrega a continuación los antecedentes internacionales y nacionales, los cuales están ordenados cronológicamente, del más reciente al más antiguo, como detallamos a continuación:

1.1.1. ANTECEDENTES INTERNACIONALES

SANCHEZ (2017). En su trabajo de investigación titulada “Análisis de la Ley 1273 de 2009 y la evolución de la ley con relación a los delitos informáticos en Colombia. Una aproximación al fenómeno de los jóvenes en el sicariato en la ciudad de Pereira” realizada en la Universidad Nacional Abierta y a Distancia - UNAD. Colombia. Para optar el Título de especialista en seguridad Informática, Llegó a las siguientes conclusiones sobre los delitos informáticos en Colombia señalando que: Dentro del desarrollo del presente proyecto se muestran y analizan las diversas técnicas de cibercriminalidad que se cometen con más frecuencia en Colombia, teniendo en cuenta el origen y evolución de las nuevas tecnologías en el área de la informática y las telecomunicaciones.

De esta forma, se observa la evolución en los métodos, técnicas o herramientas que pueden ser aplicaciones o dispositivos hardware que también se han desarrollado para facilitar la tarea de robo, suplantación, estafa y demás delitos que puedan estar clasificados dentro de la lista creciente de las nuevas formas criminales de atentar contra la confidencialidad, integridad y disponibilidad de la información como activo primordial, así mismo que atentan contra los bienes de tipo mueble e intangibles con valor económico de las personas que son víctimas de los ataques o delitos informáticos. Por lo que con el presente proyecto se demuestra que aún falta normatividad en Colombia que logre abarcar todos los ámbitos de seguridad informática y que pueda sancionar correctamente este tipo de incidentes, que dejan daños en todos los entornos de desarrollo y crecimiento del país.

GONZÀLES (2013). En su trabajo de investigación titulada "Delincuencia informática: daños informáticos del artículo 264 del código penal y propuesta de reforma", realizada en la Universidad Complutense de Madrid. Para optar el Título de Doctor en Derecho, arribo a las siguientes conclusiones al tratar la delincuencia informática en Madrid, cuya expansión exponencial de la ciberdelincuencia es innegable y así lo demuestra la dedicación que a estas nuevas prácticas delictivas han dado los diferentes estados en sus normativas. Estamos ante un fenómeno relativamente novedoso, que además tiene una característica inherente al desarrollo tecnológico; la tecnología avanza a un ritmo vertiginoso, y este tipo de delitos, su aparición y su desarrollo tienen, en contradicción con el lento avance del Derecho, esa misma característica. Prueba de ello, son los informes que presentan tablas cronológicas referidas al aumento de este tipo de delitos, e igualmente a las estadísticas que manejan las empresas privadas en cuyos múltiples informes también se recoge el indudable crecimiento exponencial de estas conductas prohibidas, o la recentísima puesta en funcionamiento del Centro Europeo de Ciberdelincuencia de la Unión Europea para coordinar la respuesta ante ciberataques en los Estados de la Unión.

GUERRA (2011) En su trabajo de investigación titulada "Delitos Informáticos Caso de Estudio" realizada en el instituto politécnico nacional de México. Para obtener el Grado de maestro en ingeniería en seguridad y tecnologías de la información, Llegó a las siguientes conclusiones con relación a los delitos informáticos en México: Los delitos informáticos en México, no son exclusivos de la competencia en materia penal, la diversidad de delitos variará con respecto a las ideas que tengan las personas que hagan uso de medios tecnológicos para delinquir. Los delitos informáticos no pueden ser una actividad que se someta al capricho temporal que vive día a día la sociedad y que está en constante crecimiento; por ende, se debe de aspirar a la creación de una ley más eficaz y amplia. México no puede permanecer en el caso de que se tengan que sufrir consecuencias para dar resultados, la jurisprudencia debe de ayudar a mejor legislación en cuanto a vacíos legales, sin embargo resulta complicado que haya resoluciones al respecto, sin antes existir una ley que los regule. No es posible seguirse apegando a figuras típicas que no resuelvan una problemática específica, pues desde su formación se puede apreciar si estas figuras cumplirán con el objeto primordial del derecho: lograr una correcta relación entre los miembros de la sociedad.

SANCHEZ & FERNANDEZ (2009). En su trabajo de investigación titulada "proyecto de Investigación: delitos informáticos" realizada en el instituto tecnológico de Durango, Llegó a las siguientes conclusiones con

respecto de los delitos informáticos: Debido a la naturaleza virtual de los delitos informáticos, puede volverse confusa la tipificación de éstos ya que a nivel general, se poseen pocos conocimientos y experiencias en el manejo de ésta área. Desde el punto de vista de la Legislatura es difícil la clasificación de estos actos, por lo que la creación de instrumentos legales puede no tener los resultados esperados, sumado a que la constante innovación tecnológica obliga a un dinamismo en el manejo de las Leyes relacionadas con la informática; La falta de cultura informática es un factor crítico en el impacto de los delitos informáticos en la sociedad en general, cada vez se requieren mayores conocimientos en tecnologías de la información, las cuales permitan tener un marco de referencia aceptable para el manejo de dichas situaciones.

1.1.2. ANTECEDENTES NACIONALES

RUMICHE (2015). En su trabajo de investigación titulada “Sombras de la normatividad que regula el incremento de la ciberdelincuencia” realizada en la Universidad Nacional José Faustino Sánchez Carrión de Huacho –Perú. Para obtener el Título de Abogado, Arribo a las siguientes conclusiones: Se logró determinar que el ejercicio de la actual normatividad que regula la ciberdelincuencia en Lima 2015, contraviene en constantes disyuntivas ya que es una carta abierta para su correcta aplicación y por lo tanto incide de manera significativa sobre todo en la manera de como se le brinda la adecuada protección al ciudadano, por ende su desfavorable aplicación puede llegar a causar un penoso impacto en nuestra sociedad. De la misma forma se puede establecer que si en la práctica se generaran tantos errores judiciales se devendría en ilegal, y por ende se generaría en inconstitucional. Todo ello generaría un gran impacto constitucional; Señalar que es evidente que la falta de cultura informática es un factor Crítico en el impacto de los delitos informáticos en la sociedad en general, los operadores de justicia cada vez deben tener mayores conocimientos en tecnología de la información y en nuestra actualidad es un poco riesgoso hacer negocios vía Web ya que los instrumentos legales no garantizan con un adecuado marco legal para su efectividad.

HIDALGO (2011). En su trabajo de investigación titulada “Delincuentes Modernos en la Ciudad de la Oroya: En Delitos Informáticos”, realizada en la Universidad de Huánuco, Llegó a las siguientes conclusiones con relación a los delitos informáticos en la Oroya: Debido a la naturaleza virtual de los delitos informáticos, puede volverse confusa la tipificación de éstos ya que a nivel general, se poseen pocos conocimientos y experiencias en el manejo de ésta área. Desde el punto de vista de la Legislatura es difícil la clasificación de estos actos, por lo que la creación de instrumentos legales puede no tener

los resultados esperados, sumado a que la constante innovación tecnológica obliga a un dinamismo en el manejo de las Leyes relacionadas con la informática, siendo la falta de cultura informática un factor crítico en el impacto de los delitos informáticos en la sociedad en general, cada vez se requieren mayores conocimientos en tecnologías de la información, las cuales permitan tener un marco de referencia aceptable para el manejo de dichas situaciones, con nuevas formas de hacer negocios como el comercio electrónico puede que no encuentre el eco esperado en los individuos y en las empresas hacia los que va dirigido ésta tecnología, por lo que se deben crear instrumentos legales efectivos que ataquen ésta problemática, con el único fin de tener un marco legal que se utilice como soporte para el manejo de éste tipo de transacciones.

1.2 BASES TEÓRICAS

Vamos a los conceptos que serán utilizados a lo largo de la presente tesis que ayudarán a un mejor entendimiento de los delitos informáticos presentados en el Convenio de Budapest sobre la Ciberdelincuencia y la legislación peruana.

1.2.1 GENERALIDADES

La realidad del mundo jurídico es fiel testigo de los cambios que se han generado en los aspectos económicos, administrativos, sociales, culturales y sobre todo tecnológicos lo cual ha llevado mejorar la calidad de vida de las personas pues facilitan las herramientas que se son necesarias para agilizar el trabajo diario tanto en casa, el trabajo así como en los estudios, porque en todos nuestros actos cotidianos se ha hecho indispensable el uso de INTERNET. Las redes sociales ya forman parte de nuestra vida no solo en nuestro país sino en el mundo y el cual desempeña un papel fundamental.

Si bien los diversos ámbitos de interacción se ven favorecidos por la fluidez que le brinda esta nueva alternativa tecnológica, no obstante, se incrementan los riesgos relacionados a las tecnologías informáticas y de comunicación. El desarrollo de la tecnología también ha traído consigo nuevas formas delictuales que tienen por medio y/o finalidad los sistemas informáticos e internet.

Las principales características de vulnerabilidad que presenta el mundo informático son las siguientes:

a. La falta de jerarquía en la red, que permite establecer sistemas de control, lo que dificulta la verificación de la información que circula por este medio.

b. El creciente número de usuarios, y la facilidad de acceso al medio tecnológico.

c. El anonimato de los cibernautas que dificulta su persecución tras la comisión de un delito a través de este medio.

d. La facilidad de acceso a la información para alterar datos, destruir sistemas informáticos. Otro factor determinante es la rápida difusión de información a través de este medio tecnológico a muy bajo costo que permite a las organizaciones delictivas perpetrar delitos con mayor facilidad.

1.2.2. En relación a los tratados

Los tratados internacionales

Novak y García-Corrochano (2003) dan a conocer la evolución de los tratados internacionales su importancia en el derecho internacional público a lo largo del tiempo desde hace poco más de 300 años:

Los tratados internacionales se han convertido progresivamente, en la fuente más recurrida del derecho internacional contemporáneo. Su incorporación y posterior desarrollo en esta disciplina fue fruto del intensivo proceso codificador que se inicia a fines del siglo XVIII, el mismo que tuvo como propósito ordenar sistemáticamente las normas consuetudinarias existentes, modificar algunas de ellas y elaborar reglas nuevas, con un criterio jurídico adecuado.

El Perú es un Estado Parte de la Convención de Viena de 1969 sobre el Derecho de los Tratados desde momento de su ratificación el 14 de septiembre del año 2000. Con dicho acto hizo constancia internacional de su consentimiento a obligarse al instrumento y sus pautas para la firma de tratados internacionales.

1.2.2.1. La adhesión a un tratado

ONU (2018) La “adhesión” es el acto por el cual un Estado acepta la oferta o la posibilidad de formar parte de un tratado ya negociado y firmado por otros estados. Tiene los mismos efectos jurídicos que la ratificación. En general, la adhesión se produce una vez que el tratado ha entrado en vigor.

1.2.2.2. Las reservas a un tratado

La Convención de Viena sobre el Derecho de los Tratados de 1969 define el término “reserva” en un tratado internacional:

(…) una declaración unilateral, cualquiera que sea su enunciado o denominación, hecha por un Estado al firmar, ratificar, aceptar o aprobar un tratado o al adherirse a él, con objeto de excluir o modificar los efectos jurídicos de ciertas disposiciones del tratado en su aplicación a ese Estado.

Garnica (2011) cita a Polakiewicz, quien considera que las reservas buscan: Facilitar la participación de más partes en los tratados internacionales. (…) al hacer una reserva se excluyen o modifican términos del tratado o el efecto legal de algunas cláusulas en cuanto a su aplicación en sus respectivos países u organizaciones.

En muchos casos el estado que se reserva busca limitar sus obligaciones conforme al tratado.

1.2.2.3. Las declaraciones a un tratado

Novak, García- Corrochano (2016). A diferencia de las reservas, las declaraciones no están reguladas por el Convención de Viena sobre el Derecho de los Tratados de 1969. Según Novak y García-Corrochano: las declaraciones son manifestaciones de los Estados por las cuales asumen obligaciones sin recibir nada a cambio.

Bajo esta definición, podemos entender que una reserva es una declaración unilateral, pero una declaración no es una reserva, ya que no limita sus obligaciones convencionales.

1.2.3. DERECHO INFORMÁTICO

Flores Salgado (2014) El derecho informático es un conjunto de principios y normas que regulan los efectos jurídicos de la relación entre el Derecho y la Informática.

Para Julio Téllez Valdés, el Derecho Informático es... “Una rama de las ciencias jurídicas que considera a la Informática como instrumento (Informática Jurídica) y objeto de estudio (Derecho de la Informática).

Armando (2008) El Derecho Informático como rama del Derecho tiene una incipiente y corta evolución, la cual data a partir del año de 1949, en el que Norbert Wiener, con su obra, consagra al derecho y las comunicaciones, al expresar la influencia que ejerce la cibernética respecto de la ciencia jurídica, al afirmar... “Así los problemas de la ley deben considerarse como comunicativos y cibernéticos, es decir, son problemas de regulación ordenada y reproducible de ciertas situaciones críticas.”

Para nuestra investigación diremos que el Derecho informático, como rama de Derecho es una interdisciplina que se encarga de estudiar el uso y desarrollo de las tecnologías informáticas, encaminadas a la investigación científica de los problemas jurídicos y como un factor de estrategia para el desarrollo de la sociedad, con el fin de lograr su pleno aprovechamiento, y como instrumento de apoyo para elevar la productividad, competitividad, eficiencia, administración y procuración del derecho en los sectores público, social y privado para propiciar el bienestar común.

1.2.4. LOS DELITOS INFORMATICOS EN LA DOCTRINA

Callegari (1985) Los delitos informáticos han sido mencionados desde la década de los 60 y su concepto ha evolucionado en el tiempo. En esa misma década se consideraba a los delitos informáticos como daños físicos contra infraestructura informática, en la década de los 70 se empezó a utilizar de manera ilícita los sistemas informáticos. Una década después comenzaron los delitos contra infraestructuras críticas, piratería y delitos de patentes. En este periodo de tiempo Callegari definía los delitos informáticos como aquellos que se dan con la ayuda de la informática o de técnicas anexas. Un ejemplo claro de la época era la piratería de software y archivos multimedia, que se incrementarían exponencialmente en las dos siguientes décadas. Con la llegada del Internet a los hogares a inicios de la década de los 90 los delincuentes informáticos tenían un nuevo medio y herramientas para realizar sus actividades.

Una definición que enmarca los temas presentados previamente es el que brinda Villavicencio, quien alega que:

Villavicencio (2014) Los delitos informáticos se vinculan con la idea de la comisión del crimen a través del empleo de la computadora, internet, etcétera; sin embargo, esta forma de criminalidad no solo se comete a través de estos medios, pues éstos solo son instrumentos que facilitan, pero no determinan la comisión de estos delitos. Esta denominación es poco usada en las

legislaciones penales; no obstante, bajo ella se describe una nueva forma de criminalidad desarrollada a partir del elevado uso de la tecnología informática.

En base a las definiciones presentadas previamente, se define a los delitos informáticos no como nuevas conductas ilícitas, sino como nuevas formas como se desarrollan los delitos mediante el uso de medios informáticos conectados a Internet o de manera física teniendo acceso a un dispositivo con algún puerto que permita una conexión al sistema y a los archivos que están contenidos.

El siguiente cuadro presenta los principales delitos informáticos:

Categoría de Delito	Tipo de Delito
Delitos contra la intimidad	Almacenamiento, modificación, revelación o difusión ilegal de datos personales.
Delitos relativos al contenido	Difusión, especialmente por Internet, de pornografía, y en especial de pornografía infantil, declaraciones racistas e información que incita a la violencia.
Delitos económicos, acceso no autorizado y sabotaje	La piratería, el sabotaje informático y la distribución de virus, el espionaje informático, y la falsificación y el fraude informáticos.
Delitos contra la propiedad intelectual	Delitos contra la protección jurídica de programas y la protección jurídica de las bases de datos, los derechos de autor y derechos afines.

1.2.5. CIBERDELINCUENCIA

A la fecha no existe una definición consensuada del término ciberdelincuencia, diferentes autores presentan su definición teniendo como elemento central el uso de dispositivos informáticos y una red para conectarse a otros dispositivos.

La Unión Internacional de Telecomunicaciones (ITU) en su informe de Comprensión de la ciberdelincuencia: Fenómenos, dificultades y respuesta jurídica, del año 2014, brinda dos definiciones de ciberdelincuencia basados en los conceptos trabajados en el taller que tuvo lugar con ocasión del Congreso de las Naciones Unidas sobre Prevención del Delito y Tratamiento del Delincuente:

Ciberdelincuencia en sentido estricto (delito informático) comprende cualquier comportamiento ilícito realizado mediante operaciones electrónicas que atentan contra la seguridad de sistemas informáticos y de los datos que éstos procesan. En sentido general, ciberdelincuencia (delitos relacionados con las computadoras) comprende cualquier comportamiento ilícito cometido por medio de un sistema informático o una red de computadores, o relacionado con éstos, incluidos delitos tales como la posesión ilícita y la puesta a disposición o distribución de información mediante sistemas informáticos o redes de computadores.

Cabe resaltar que algunos años atrás, se trató de dar una definición más precisa incluyendo los objetivos o intenciones, pero ese concepto puede excluir delitos que pueden ser considerados ciberdelincuencia en ciertos acuerdos internacionales, tales como la Legislación Modelo de la Commonwealth sobre la delincuencia informática y relacionada con los computadores o el Convenio del Consejo de Europa sobre la Ciberdelincuencia.

Mehan (2014) brinda un concepto del término ciberdelincuencia, el cual considera: Todas las formas de actividad delictiva perpetradas utilizando tecnología de la información e Internet. (...) El ciberdelito no es más que actividades delictivas tradicionales, como el robo y el fraude, que se lleva a cabo utilizando las tecnologías digitales más avanzadas y que aprovecha la creciente dependencia de la tecnología de la información. Esta dependencia es un factor debilitante que se ha incrementado exponencialmente con la abundancia de sistemas de información interconectados, el desarrollo de la computación en la nube, la virtualización, los dispositivos móviles y los sitios de redes sociales.

Este concepto incluye las principales herramientas y medios para poder realizar las actividades delictivas, y, sobre todo, se hace mención de la convergencia que se está viviendo en la actualidad y que considera los dispositivos más utilizados por la población mundial (computadoras, laptops, celulares, tabletas, entre otros).

El objetivo fundamental de los ciberdelincuentes es maximizar su rentabilidad financiera a la vez que minimizan su riesgo. Un objetivo secundario podría ser el deseo de obtener poder a través del control de información y / o fuentes de información.

1.2.6. EN RELACIÓN A LOS DELITOS INFORMÁTICOS Y CIBERDELINCUENCIA

1.2.6.1. La piratería

La piratería es un problema global que afecta a diferentes industrias en términos económicos y de imagen. La definición de la misma evolucionó en el tiempo al igual que su rango de acción y forma de comisión del delito. García, Jeldres, Mardones dan una definición inicial del término piratería y su evolución en el tiempo:

García, Jeldres, Mardones (2007) El término pirata proviene del latín pirata, que significa “el que emprende o el que intenta fortuna, sin embargo, las acciones de estos hombres estaban al margen de cualquier ley. Según la historia, el más antiguo de los piratas fue un griego de nombre Polícrates, famoso por haber creado una gran fortuna con sus robos. (…) Hoy en día el concepto de pirata se relaciona al establecido en sus orígenes, pero adaptado a las condiciones de la sociedad actual. Piratería es usado generalmente para describir el crimen deliberado de la copia ilegal a gran escala.

Se incorpora al término piratería, elementos como derecho de autor y lo relaciona con actividades y obras más acordes a la época actual:

El término “piratería” abarca la reproducción y distribución de copias de obras protegidas por el derecho de autor, así como su transmisión al público o su puesta a disposición en redes de comunicación en línea, sin la autorización de los propietarios legítimos, cuando dicha autorización resulte necesaria legalmente. La piratería afecta a obras de distintos tipos, como la música, la literatura, el cine, los

programas informáticos, los videojuegos, los programas y las señales audiovisuales

1.2.6.2. El Robo de Datos Confidenciales

La División de Seguridad de la Información de la Oficina del Director de Información de Iowa define a los datos confidenciales como información de identificación personal (IIP) que una persona no desea que sean obtenidos sin su consentimiento. Estos datos pueden ser considerados patrimonio tangible o intangible de una persona o institución. Estos datos pueden incluir el número de identificación, el número de teléfono personal o de terceras personas registradas por uno mismo, las cuentas bancarias, las contraseñas de servicios, entre otros.

En tal sentido, el robo de datos confidenciales se entiende como un delito contra el patrimonio, por el cual se produce el apoderamiento de información de identificación personal ajena, la cual se obtuvo violentando medidas de seguridad.

1.2.6.3. El Fraude Informático

En el Perú, el artículo 8 de la Ley Nº 30096, Ley de Delitos Informáticos; y su modificatoria, Ley 30171, Ley que modifica la Ley 30096, Ley de Delitos Informáticos definen al fraude informático como un delito informático y sus características:

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, clonación de datos informáticos o cualquier interferencia o manipulación en el funcionamiento de un sistema informático (…) (Ley 30171, 2014)

Esta definición del artículo de la ley tras su modificación en el año 2004 cumple con el concepto de marco legal común con los países miembros del Convenio de Budapest sobre la Ciberdelincuencia, por lo que es considerado en más de cincuenta países.

1.2.6.4. La falsificación de información

“Falsificación” (2014) La Enciclopedia Jurídica define la falsificación como la adulteración, corrupción, cambio o imitación para perjudicar a otro u obtener ilícito provecho.

Arias y Aristizábal (2011) citan a varios autores, entre los que se encuentran Bollinger, Smith, Bhatt, Speak, Spijkervet, Herder, Davenport y Earl, para definir a la información como datos procesados, organizados o con significado, necesarios para la creación de conocimiento, la cual es valiosa, evaluada, validada y codificada.

Por ende, la falsificación de información es la adulteración o imitación de datos procesados con el fin de perjudicar a otro u obtener ilícito provecho.

1.2.6.5. La alteración de datos

La alteración es la variar, cambiar o hacer diferente algo ¿Qué es la alteración?"

Un dato es un conjunto discreto, de factores objetivos sobre un hecho real. (…) Los datos describen únicamente una parte de lo que pasa en la realidad y no proporcionan juicios de valor o interpretaciones, y por lo tanto no son orientativos para la acción. La toma de decisiones se basará en datos.

Con las definiciones brindadas líneas arriba, se entiende a la alteración de datos como la variación, cambio o la acción de hacer diferente un conjunto de datos, los cuales contienen información almacenada para la toma futura de decisiones.

1.2.6.6. La destrucción de datos

Se entiende a la destrucción como el acto de arruinar o dañar en forma grave a algo o a alguien para dejarlo arruinado, inservible o dañado. En relación con los datos, se infiere que se trata de la acción de dejar inservibles datos que contienen información almacenada.

1.2.6.7. La privacidad

El concepto de privacidad está relacionado tradicionalmente a las acciones y vida privada de las personas en un ámbito reservado, lo que también es conocido como intimidad. Sarachaga hace uso del concepto tradicional, y lo relaciona al uso las nuevas tecnologías de la información y comunicación, junto a una serie de riesgos propios de ese entorno:

Sarachaga, (2017).La privacidad, en su forma tradicional, puede definirse como aquello que una persona lleva a cabo en un ámbito reservado, algo que se mantiene fuera del alcance de otras personas, y puede ser asociado al concepto de intimidad. Sin embargo, actualmente la tecnología está muy presente en nuestras vidas, por lo que el concepto de privacidad obtiene una dimensión mucho mayor de la que tenía en el pasado. Los datos se convierten en el activo más preciado, además de que es sencillo recogerlos, almacenarlos y tratarlos. (…) Las redes sociales, las compras con tarjetas, las llamadas telefónicas y otras muchas actividades que realizamos día a día son fuente de una cantidad inmensa de datos, entre los cuales se encuentran nuestros datos personales. La tecnología a pesar de ser traducirse en herramientas que nos facilitan el día a día automatizando tareas que nunca antes hubiésemos imaginado, conlleva una serie de riesgos, y la pérdida de privacidad es uno de ellos y un tema muy serio a tratar.

En la presente década la aparición de nuevos servicios en Internet requiere que parte de nuestra información, archivos y actividades dejen de ser privados para ser utilizados para mejoras de servicio o para ser utilizados por terceros para fines comerciales.

1.2.6.8 El Ciberespacio

Clarke y Knake, (2011) El ciberespacio lo conforman todas las redes informáticas del mundo y todo lo que ellas conectan y controlan. No se trata solo de internet. Es importante dejar en claro la diferencia. Internet es una red de redes abierta. Desde cualquier red de internet, podemos comunicarnos con cualquier ordenador conectado con cualquiera otra de las redes de internet. El ciberespacio es Internet más montones de otras redes de ordenadores a las que, se supone, no es posible acceder desde internet. Algunas de esas redes privadas son muy semejantes a internet, pero, al menos teóricamente, se encuentran separadas de ella.

El ciberespacio, por ende, brinda muchas oportunidades para todos sus usuarios y es un medio por el cual los mismos, personas u organizaciones, se pueden conectar para hacer diferentes actividades que serán de beneficio para los mismos. Martínez, Leyva, Félix, Cecenas y Ontiveros citan a Mayans para explicar algunos de los beneficios del ciberespacio, tanto a nivel económico y de accesibilidad:

Martínez, Leyva, Félix, Cecenas, Ontiveros, (2014) El ciberespacio es una dimensión más accesible económicamente que otros canales de difusión e información de utilidad comparable. Esto hace posible que puedan ser millones sus 'habitantes'. (…) El ciberespacio es un entorno conceptualmente accesible y manipulable, donde existen muchas formas de participación y ni siquiera las más complejas y completas son inaccesibles, dado el carácter de lenguaje de su forma de acceder y participar activamente en él.

1.2.7. LA LEY 30096 MODIFICADA POR LA LEY 30191 "LEY DE DELITOS INFORMATICOS" DE PERÚ.

1.2.7.1. Delitos Contra Datos y Sistemas Informáticos

Artículo 2. Acceso ilícito

El que deliberada e ilegítimamente accede a todo o en 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 deliberada e ilegítimamente 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 inutiliza, 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.

1.2.7.2. Delitos Informáticos Contra la Indemnidad y Libertad Sexuales

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 llevar a cabo actividades sexuales con él, 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 y 4 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 y 4 del artículo 36 del Código Penal.

1.2.7.3. Delitos Informáticos Contra la Intimidad y el Secreto de las Comunicaciones.

Artículo 6. Tráfico ilegal de datos

DEROGADO

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 del 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.

La pena privativa de libertad será no menor de cinco ni mayor de ocho años cuando el delito recaiga sobre información clasificada como secreta, reservada o confidencial de conformidad con la Ley 27806, Ley de Transparencia y Acceso a la Información Pública.

La pena privativa de libertad será no menor de ocho ni mayor de diez cuando el delito comprometa la defensa, seguridad o soberanía nacionales.

Si el agente comete el delito como integrante de una organización criminal, la pena se incrementa hasta en un tercio por encima del máximo legal previsto en los supuestos anteriores.

1.2.7.4. Delitos Informáticos Contra el Patrimonio

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, 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.

1.2.7.5. Delitos Informáticos Contra la Fe Pública

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.

1.2.7.6. Disposiciones Comunes

Artículo 10. Abuso de mecanismos y dispositivos informáticos

El que deliberada e ilegítimamente fabrica, diseña, desarrolla, vende, facilita, distribuye, importa u obtiene para su utilización, uno o más mecanismos, programas informáticos, dispositivos, contraseñas, códigos de acceso o cualquier otro dato informático, específicamente diseñados para la comisión de los delitos previstos en la presente Ley, o el que ofrece o presta servicio que contribuya a ese propósito, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días-multa.

1.2.8. EL CONVENIO DE BUDAPEST SOBRE LA CIBERDELINCUENCIA

El Convenio de Budapest sobre la Ciberdelincuencia es un tratado multilateral de naturaleza jurídica derivada del Derecho Internacional, el cual

permite a los estados partes a obligarse al mismo vía el consentimiento para el logro de un objetivo específico.

Es considerado el primer tratado internacional sobre delitos cometidos a través de internet y otros sistemas informáticos, el cual busca brindar herramientas de derecho penal sustantivo y procesal, así como mejorar capacidades de cada estado parte mediante cooperación internacional en tiempo real para la lucha contra la ciberdelincuencia.

La adhesión al Convenio no generará mayor costo a los Estados Parte fuera de la adecuación de la legislación interna de ser necesario y los trámites a seguir según procedimientos del Convenio, pero a cambio, como se mencionó en el párrafo anterior, contarán con una herramienta para combatir delitos cometidos con el uso de dispositivos informáticos. La entrada en vigor para los Estados Parte se realizará según lo establecido por el instrumento.

En relación a la cooperación internacional, los Estados decidirán los recursos a destinar para la lucha contra la ciberdelincuencia en base a sus posibilidades y de igual manera podrán aprovechar las modalidades de cooperación disponibles dentro del Convenio.

1.2.8.1. El contexto para su creación

La difusión masiva del Internet, y la aparición de dispositivos electrónicos y sistemas operativos pensados para todo público a inicios de la década de los noventa permitieron a las poblaciones de todo el mundo el conocer y explotar un nuevo mundo de posibilidades. Esto vino acompañado de un rápido desarrollo en el campo de las tecnologías de la información y comunicación que cada día estaban introduciéndose en todos los sectores de la sociedad moderna generando cambios importantes en la economía y la sociedad, y creando mayor dependencia a sus usuarios por la velocidad, facilidades y otros beneficios que las mismas brindaban.

Las nuevas tecnologías traspasaron las fronteras y el tiempo, haciendo innecesario estar en una ubicación geográfica específica, el esperar horas o días para hacer operaciones comerciales o enterarse de eventos en el mundo. La comunicación también se había vuelto instantánea, y la noción de horarios y tiempo desaparecía en el nuevo entorno del ciberespacio.

En este nuevo contexto, cualquier persona con un dispositivo adecuado y conexión a Internet era capaz de tener acceso a servicios en el ciberespacio o a redes privadas o públicas alrededor del mundo sin importar desde qué punto del planeta se encuentre. Por un lado, esta situación rompía los conceptos de fronteras para dar libertad a la población mundial, pero, por otro lado, generaba una incertidumbre por el mal uso de las nuevas herramientas disponibles en el ciberespacio, la cual no podía ser controlada con facilidad debido a la nueva naturaleza transfronteriza que adquirían las redes de la información.

La aparición de virus alrededor del mundo y la evolución de la comisión de delitos tradicionales que incrementaban su alcance de daño mediante el uso de nuevas tecnologías, fueron nuevos retos que los Estados empezaron a tomar con mayor preocupación. Los delincuentes ya no debían estar en el Estado donde se realizaban los delitos, es por eso que era necesario crear instrumentos jurídicos internacionales que ayuden a afrontar este nuevo desafío, sobre todo para el bienestar y protección de las poblaciones y sus derechos humanos en la nueva era de la Sociedad de la Información, la cual hace uso intensivo de la tecnología y comunicación para el desarrollo de las personas.

1.2.8.2. Antecedentes del Convenio

En noviembre de 1996 el Comité de Europeo para los Problemas Criminales (CDPC) vía decisión número CDPC/103/211196 establece un "Comité de Expertos Encargados de Delitos Informáticos" para examinar revisar las recomendaciones 89 y 95 sobre procedimiento penal vinculado a la tecnología de la información y elaborar un borrador de instrumento jurídicamente vinculante.

El 4 de febrero de 1997 mediante decisión número CM/Del/Dec (97) 583 se establece en el Consejo de Europa el "Comité de Expertos en la Delincuencia en el Ciberespacio (PC-CY)" para elaborar un instrumento jurídicamente vinculante que trate el problema de los delitos cometidos por medios electrónicos.

El nuevo comité se encargó de elaborar un borrador del instrumento entre abril de 1997 y diciembre del año 2000 con recomendaciones de expertos y la participación de Estados miembros y no miembros del Consejo de Europa. En abril del 2000 se desclasificó y

publicó el proyecto de Convenio que seguiría siendo modificado en los siguientes meses.

En noviembre de 2001 el Consejo de Europa aprobó el tratado No. 185 del Consejo de Europa o Convenio de Budapest sobre la Ciberdelincuencia. A partir de ese momento el instrumento quedaba abierto para la firma de los Estados que participaron en su elaboración.

Casi tres años después, con la expresión de consentimiento y entrega de los instrumentos de ratificación, aceptación o aprobación depositados en poder del Secretario General (artículo 36.2) de por lo menos cinco Estados, los cuales deben incluir a tres estados miembros del Consejo de Europa (Albania, Croacia, Estonia, Hungría y Lituania) para su entrada en vigencia; y habiendo expirado el plazo estipulado de tres meses de la expresión del consentimiento de los Estados para quedar vinculados por el Convenio (artículo 36.3); entra en vigor a nivel internacional el 1 de julio de 2004 el Convenio de Budapest sobre la Ciberdelincuencia.

En la sesión plenaria 50 del CDPC de junio de 2001 se aprobó el proyecto de Convenio y en la sesión Con este acto, el Convenio mencionado previamente pasa a ser el primer tratado internacional sobre delitos cometidos a través de internet y otras redes informáticas relacionados a derechos de autor, fraude informático, pornografía infantil y violaciones de seguridad en la red. Mientras brinda herramientas de derecho y cooperación judicial a las partes para la protección de sus poblaciones en relación a los ciberdelitos.

1.2.8.3. Los objetivos del Convenio

El principal objetivo del Convenio de Budapest sobre la Ciberdelincuencia es: aplicar una política penal común con objeto de proteger a la sociedad frente a la ciberdelincuencia, en particular mediante la adopción de una legislación adecuada y la mejora de la cooperación internacional (COE, 2001a, p.1).

Con el logro del objetivo, se busca incrementar las capacidades y eficiencia en la investigación, persecución y proceso penal; así como permitir la obtención de pruebas electrónicas de los delitos cometidos para los Estados Parte mediante la cooperación internacional en tiempo real.

1.2.8.4. La estructura del Convenio

El Convenio contiene un Preámbulo y un total de cuarenta y ocho artículos distribuidos en cuatro capítulos:

• Capítulo I: Terminología,
• Capítulo II: Medidas que deben adoptarse a nivel nacional,
• Capítulo III: Cooperación Internacional y
•Capítulo IV: Cláusulas finales, con sus correspondientes secciones y títulos.

Posteriormente, el 28 de enero de 2003, se adicionó un Prólogo que entraba en vigor el 1 de marzo de 2006, donde se penalizaba los actos racistas y xenófobos cometidos mediante medios informáticos. Dicho Prólogo no se considera para que los Estados puedan realizar los procedimientos de adhesión o ratificación del Convenio.

1.2.8.5. Artículos del Convenio

Medidas que deberán adoptarse a nivel nacional

Derecho penal sustantivo – Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos

Artículo 2 – Acceso ilícito

Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno el acceso deliberado e ilegítimo a todo o parte de un sistema informático. Las Partes podrán exigir que el delito se cometa infringiendo medidas de seguridad, con la intención de obtener datos informáticos u otra intención delictiva, o en relación con un sistema informático conectado a otro sistema informático.

Artículo 3 – Interceptación ilícita

Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la interceptación deliberada e ilegítima por medios técnicos de datos informáticos en transmisiones no públicas dirigidas a un sistema informático, originadas en un sistema informático o efectuadas dentro del mismo, incluidas las emisiones electromagnéticas provenientes de un sistema informático que transporte dichos datos informáticos. Las Partes

podrán exigir que el delito se cometa con intención delictiva o en relación con un sistema informático conectado a otro sistema informático.

Artículo 4 – Ataques a la integridad de los datos

Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno todo acto deliberado e ilegítimo que dañe, borre, deteriore, altere o suprima datos informáticos.

Las Partes podrán reservarse el derecho a exigir que los actos definidos en el párrafo 1 comporten daños graves.

Artículo 5 – Ataques a la integridad del sistema

Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la obstaculización grave, deliberada e ilegítima del funcionamiento de un sistema informático mediante la introducción, transmisión, daño, borrado, deterioro, alteración o supresión de datos informáticos.

Artículo 6 – Abuso de los dispositivos

Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la comisión deliberada e ilegítima de los siguientes actos:

a) La producción, venta, obtención para su utilización, importación, difusión u otra forma de puesta a disposición de:

i) Cualquier dispositivo, incluido un programa informático, concebido o adaptado principalmente para la comisión de cualquiera de los delitos previstos en los artículos 2 a 5 del presente Convenio;

ii) Una contraseña, código de acceso o datos informáticos similares que permitan acceder a todo o parte de un sistema informático, con intención de que sean utilizados para cometer cualquiera de los delitos contemplados en los artículos 2 a 5; y

b) La posesión de alguno de los elementos contemplados en los incisos i) o ii) del apartado a) del presente artículo con intención de que sean utilizados para cometer cualquiera de los delitos previstos en los artículos 2 a 5. Las Partes podrán exigir en su derecho interno la

posesión de un número determinado de dichos elementos para que se considere que existe responsabilidad penal.

No se interpretará que el presente artículo impone responsabilidad penal cuando la producción, venta, obtención para la utilización, importación, difusión o cualquier otra forma de puesta a disposición mencionada en el párrafo 1 del presente artículo no tenga por objeto la comisión de uno de los delitos previstos de conformidad con los artículos 2 a 5 del presente Convenio, como en el caso de las pruebas autorizadas o de la protección de un sistema informático.

Las Partes podrán reservarse el derecho a no aplicar el párrafo 1 del presente artículo, siempre que dicha reserva no afecte a la venta, distribución o cualesquiera otras formas de puesta a disposición de los elementos mencionados en el inciso 1 a) ii) del presente artículo.

1.2.8.6. Delitos Informático

Artículo 7 – Falsificación informática

Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la introducción, alteración, borrado o supresión deliberados e ilegítimos de datos informáticos que genere datos no auténticos con la intención de que sean tomados o utilizados a efectos legales como auténticos, con independencia de que los datos sean legibles e inteligibles directamente. Las Partes podrán exigir que exista una intención dolosa o delictiva similar para que se considere que existe responsabilidad penal.

Artículo 8 – Fraude informático

Las Partes adoptarán las medidas legislativas o de otro tipo que resulten necesarias para tipificar como delito en su derecho interno los actos deliberados e ilegítimos que causen perjuicio patrimonial a otra persona mediante:

La introducción, alteración, borrado o supresión de datos informáticos; cualquier interferencia en el funcionamiento de un sistema informático, con la intención, dolosa o delictiva, de obtener de forma ilegítima un beneficio económico para uno mismo o para otra persona.

1.2.8.7. Delitos relacionados con el contenido

Artículo 9 – Delitos relacionados con la pornografía infantil

Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la comisión deliberada e ilegítima de los siguientes actos:

- La producción de pornografía infantil con la intención de difundirla a través de un sistema informático;
- La oferta o la puesta a disposición de pornografía infantil a través de un sistema informático;
- La difusión o la transmisión de pornografía infantil a través de un sistema informático;
- La adquisición, para uno mismo o para otros, de pornografía infantil a través de un sistema informático;
- La posesión de pornografía infantil en un sistema informático o en un dispositivo de almacenamiento de datos informáticos.

A los efectos del párrafo 1 anterior, se entenderá por «pornografía infantil» todo material pornográfico que contenga la representación visual de: un menor adoptando un comportamiento sexualmente explícito; una persona que parezca un menor adoptando un comportamiento sexualmente explícito; imágenes realistas que representen a un menor adoptando un comportamiento sexualmente explícito.

A los efectos del párrafo 2 anterior, se entenderá por «menor» toda persona menor de 18 años. Las Partes podrán, no obstante, exigir un límite de edad inferior, que deberá ser como mínimo de 16 años.

Las Partes podrán reservarse el derecho a no aplicar, en todo o en parte, los apartados d) y e) del párrafo 1 y los apartados b) y c) del párrafo 2.

1.2.8.8 Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines

Artículo 10 – Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines

Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno las infracciones de la propiedad intelectual que defina su legislación, de

conformidad con las obligaciones que haya contraído en aplicación del Acta de París de 24 de julio de 1971, por la cual se revisó el Convenio de Berna para la protección de las obras literarias y artísticas, del Acuerdo sobre los aspectos de los derechos de propiedad intelectual relacionados con el comercio y del Tratado de la OMPI sobre Derecho de Autor, a excepción de cualquier derecho moral otorgado por dichos Convenios, cuando tales actos se cometan deliberadamente, a escala comercial y por medio de un sistema informático.

Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno las infracciones de los derechos afines definidas en su legislación, de conformidad con las obligaciones que haya asumido en aplicación de la Convención Internacional sobre la Protección de los Artistas Intérpretes o Ejecutantes, los Productores de Fonogramas y los Organismos de Radiodifusión (Convención de Roma), del Acuerdo sobre los aspectos de los derechos de propiedad intelectual relacionados con el comercio y del Tratado de la OMPI sobre Interpretación o Ejecución y Fonogramas, a excepción de cualquier derecho moral conferido por dichos Convenios, cuando tales actos se cometan deliberadamente, a escala comercial y por medio de un sistema informático.

En circunstancias bien delimitadas, toda Parte podrá reservarse el derecho de no imponer responsabilidad penal en virtud de los párrafos 1 y 2 del presente artículo, siempre que se disponga de otros recursos efectivos y que dicha reserva no vulnere las obligaciones internacionales que incumban a dicha Parte en aplicación de los instrumentos internacionales mencionados en los párrafos 1 y 2 del presente artículo.

1.2.9. CODIGO PENAL

1.2.9.1 Violación del Secreto de las Comunicaciones

Artículo 162º - Interferencia telefónica

El que, indebidamente, interfiere o escucha una conversación telefónica o similar será reprimido con pena privativa de libertad no menor de uno ni mayor de tres años. Si el agente es funcionario público, la pena privativa de libertad será no menor de tres ni mayor de cinco años e inhabilitación conforme al artículo 36º incisos l, 2 y 4.

1.2.9.2. Pornografía Infantil en el Código Penal Peruano

Artículo 181°-A.- Explotación sexual comercial infantil y adolescente en ámbito del turismo.

El que promueve, publicita, favorece o facilita la explotación sexual comercial en el ámbito del turismo, a través de cualquier medio escrito, folleto, impreso, visual, audible, electrónico, magnético o a través de Internet, con el objeto de ofrecer relaciones sexuales de carácter comercial de personas de catorce (14) y menos de dieciocho (18) años de edad será reprimido con pena privativa de libertad no menor de cuatro (4) ni mayor de ocho (8) años. Si la víctima es menor de catorce años, el agente, será reprimido con pena privativa de la libertad no menor de seis (6) ni mayor de ocho (8) años. El agente también será sancionado con inhabilitación conforme al artículo 36° incisos 1, 2, 4 y 5. Será no menor de ocho (8) ni mayor de diez (10) años de pena privativa de la libertad cuando ha sido cometido por autoridad pública, sus ascendientes, maestro o persona que ha tenido a su cuidado por cualquier título a la víctima.

Artículo 181°-B.- Formas agravadas.

En los casos de los delitos previstos en los artículos 179°, 181° y 181°-A, cuando el agente sea el padre o la madre, el tutor o curador, en la sentencia se impondrá, además de la pena privativa de libertad que corresponda, la pena accesoria de inhabilitación a que se refiere el numeral 5) del artículo 36.

Artículo 182°-A.- Publicación en los medios de comunicación sobre delitos de libertad sexual a menores.

Los gerentes o responsables de las publicaciones o ediciones a transmitirse a través de los medios de comunicación masivos que publiciten la prostitución infantil, el turismo sexual infantil o la trata de menores de dieciocho años de edad serán reprimidos con pena privativa de la libertad no menor de dos ni mayor de seis años. El agente también será sancionado con inhabilitación conforme al inciso 4 del artículo 36° y con trescientos sesenta días multa.

Artículo 183°.- Exhibiciones y publicaciones obscenas

Será reprimido con pena privativa de libertad no menor de dos ni mayor de cuatro años el que, en lugar público, realiza exhibiciones, gestos, tocamientos u otra conducta de índole obscena. Será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años:

1. El que muestra, vende o entrega a un menor de dieciocho años, por cualquier medio, objetos, libros, escritos, imágenes, visuales o auditivas, que por su carácter obsceno, pueden afectar gravemente el pudor, excitar prematuramente o pervertir su instinto sexual. 2. El que incita a un menor de dieciocho años a la práctica de un acto obsceno o le facilita la entrada a los prostíbulos u otros lugares de corrupción. 3. El administrador, vigilante o persona autorizada para controlar un cine u otro espectáculo donde se exhiban representaciones obscenas, que permita ingresar a un menor de dieciocho años.

Artículo 183°-A.- Pornografía infantil

El que posee, promueve, fabrica, distribuye, exhibe, ofrece, comercializa o publica, importa o exporta por cualquier medio objetos, libros, escritos, imágenes, videos o audios, o realiza espectáculos en vivo de carácter pornográfico, en los cuales se utilice a personas de catorce y menos de dieciocho años de edad, será sancionado con pena privativa de libertad no menor de seis ni mayor de diez años y con ciento veinte a trescientos sesenta y cinco días multa. La pena privativa de libertad será no menor de diez ni mayor de doce años y de cincuenta a trescientos sesenta y cinco días multa cuando: 1. El menor tenga menos de catorce años de edad. 2. El material pornográfico se difunda a través de las tecnologías de la información o de la comunicación. Si la víctima se encuentra en alguna de las condiciones previstas en el último párrafo del artículo 173° o si el agente actúa en calidad de integrante de una organización dedicada a la pornografía infantil, la pena privativa de libertad será no menor de doce ni mayor de quince años. De ser el caso, el agente será inhabilitado conforme a los numerales 1, 2 y 4 del artículo 36°.

Artículo 183°-B.- Proposiciones sexuales a niños, niñas y adolescentes

El que contacta con un menor de catorce años para solicitar u obtener de él material pornográfico, o para llevar a cabo actividades sexuales con él, 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 y 4 del artículo 36°. 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 y 4 del artículo 36°.

1.2.9.3. Delitos Contra los Derechos Intelectuales

Artículo 216: Copia o reproducción no autorizada.

Será reprimido con pena privativa de la libertad no menor de dos ni mayor de cuatro años y de diez a sesenta días-multa, a quien estando autorizado para publicar una obra, lo hiciere en una de las formas siguientes:

a. Sin mencionar en los ejemplares el nombre del autor, traductor, adaptador, compilador o arreglador.

b. Estampe el nombre con adiciones o supresiones que afecte la reputación del autor como tal, o en su caso, del traductor, adaptador, compilador o arreglador.

c. Publique la obra con abreviaturas, adiciones, supresiones, o cualquier otra modificación, sin el consentimiento del titular del derecho.

d. Publique separadamente varias obras, cuando la autorización se haya conferido para publicarlas en conjunto; o las publique en conjunto, cuando solamente se le haya autorizado la publicación de ellas en forma separada.

Artículo 217: Reproducción, difusión, distribución y circulación de la obra sin la autorización del autor.

Será reprimido con pena privativa de libertad no menor de dos ni mayor de seis años y con treinta a noventa días-multa, el que con respecto a una obra, una interpretación o ejecución artística, un fonograma o una emisión o transmisión de radiodifusión, o una grabación audiovisual o una imagen fotográfica expresada en cualquier forma, realiza alguno de los siguientes actos sin la autorización previa y escrita del autor o titular de los derechos:

a. La modifique total o parcialmente.

b. La distribuya mediante venta, alquiler o préstamo público.

c. La comunique o difunda públicamente, transmita o retransmita por cualquiera de los medios o procedimientos reservados al titular del respectivo derecho."

d. La reproduzca, distribuya o comunique en mayor número que el autorizado por escrito.

La pena será no menor de cuatro años ni mayor de ocho y con sesenta a ciento veinte días multa, cuando el agente la reproduzca total o parcialmente, por cualquier medio o procedimiento y si la distribución se realiza mediante venta, alquiler o préstamo al público u otra forma de transferencia de la posesión del soporte que contiene la obra o

producción que supere las dos (2) Unidades Impositivas Tributarias, en forma fraccionada, en un solo acto o en diferentes actos de inferior importe cada uno.

Artículo 218: Formas agravadas;

La pena será privativa de libertad no menor de cuatro ni mayor de ocho años y con noventa a ciento ochenta días multa cuando:

a. Se dé a conocer al público una obra inédita o no divulgada, que haya recibido en confianza del titular del derecho de autor o de alguien en su nombre, sin el consentimiento del titular.

b. La reproducción, distribución o comunicación pública se realiza con fines comerciales u otro tipo de ventaja económica, o alterando o suprimiendo el nombre o seudónimo del autor, productor o titular de los derechos."

c. Conociendo el origen ilícito de la copia o reproducción, la distribuya al público, por cualquier medio, la almacene, oculte, introduzca en el país o la saque de éste.

d. Se fabrique, ensamble, importe, exporte, modifique, venda, alquile, ofrezca para la venta o alquiler, o ponga de cualquier otra manera en circulación dispositivos, sistemas tangibles o intangibles, esquemas o equipos capaces de soslayar otro dispositivo destinado a impedir o restringir la realización de copias de obras, o a menoscabar la calidad de las copias realizadas, o capaces de permitir o fomentar la recepción de un programa codificado, radiodifundido o comunicado en otra forma al público, por aquellos que no están autorizados para ello."

e. Se inscriba en el Registro del Derecho de Autor la obra, interpretación, producción o emisión ajenas, o cualquier otro tipo de bienes intelectuales, como si fueran propios, o como de persona distinta del verdadero titular de los derechos.

Artículo 219: Plagio.

Será reprimido con pena privativa de libertad no menor de cuatro ni mayor de ocho años y noventa a ciento ochenta días multa, el que con respecto a una obra, la difunda como propia, en todo o en parte, copiándola o reproduciéndola textualmente, o tratando de disimular la copia mediante ciertas alteraciones, atribuyéndose o atribuyendo a otro, la autoría o titularidad ajena.

Artículo 220: Formas agravadas.

Será reprimido con pena privativa de libertad no menor de cuatro ni mayor de ocho años y noventa a trescientos sesenta y cinco días-multa:

a. Quien se atribuya falsamente la calidad de titular originario o derivado, de cualquiera de los derechos protegidos en la legislación del derecho de autor y derechos conexos y, con esa indebida atribución, obtenga que la autoridad competente suspenda el acto de comunicación, reproducción o distribución de la obra, interpretación, producción, emisión o de cualquier otro de los bienes intelectuales protegidos.

b. Quien realice actividades propias de una entidad de gestión colectiva de derecho de autor o derechos conexos, sin contar con la autorización debida de la autoridad administrativa competente.

c. El que presente declaraciones falsas en cuanto certificaciones de ingresos; asistencia de público; repertorio utilizado; identificación de los autores; autorización supuestamente obtenida; número de ejemplares producidos, vendidos o distribuidos gratuitamente o toda otra adulteración de datos susceptible de causar perjuicio a cualquiera de los titulares del derecho de autor o conexos.

d. Si el agente que comete el delito integra una organización destinada a perpetrar los ilícitos previstos en el presente capítulo.

e. Si el agente que comete cualquiera de los delitos previstos en el presente capítulo, posee la calidad de funcionario o servidor público.

Artículo 220-A: Elusión de medida tecnológica efectiva;

El que, con fines de comercialización u otro tipo de ventaja económica, eluda sin autorización cualquier medida tecnológica efectiva que utilicen los productores de fonogramas, artistas, intérpretes o ejecutantes, así como los autores de cualquier obra protegida por derechos de propiedad intelectual, será reprimido con pena privativa de libertad no mayor de dos años y de diez a sesenta días multa.

Artículo 220-B: Productos destinados a la elusión de medidas tecnológicas;

El que, con fines de comercialización u otro tipo de ventaja económica, fabrique, importe, distribuya, ofrezca al público, proporcione

o de cualquier manera comercialice dispositivos, productos o componentes destinados principalmente a eludir una medida tecnológica que utilicen los productores de fonogramas, artistas intérpretes o ejecutantes, así como los autores de cualquier obra protegida por derechos de propiedad intelectual, será reprimido con pena privativa de libertad no mayor de dos años y de diez a sesenta días-multa.

Artículo 220-C: Servicios destinados a la elusión de medidas tecnológicas;

El que, con fines de comercialización u otro tipo de ventaja económica, brinde u ofrezca servicios al público destinados principalmente a eludir una medida tecnológica efectiva que utilicen los productores de fonogramas, artistas intérpretes o ejecutantes, así como los autores de cualquier obra protegida por derechos de propiedad intelectual, será reprimido con pena privativa de libertad no mayor de dos años y de diez a sesenta días-multa.

Artículo 220-D: Delitos contra la información sobre gestión de derechos;

El que, sin autorización y con fines de comercialización u otro tipo de ventaja económica, suprima o altere, por sí o por medio de otro, cualquier información sobre gestión de derechos, será reprimido con pena privativa de libertad no mayor de dos años y de diez a sesenta días-multa.

La misma pena será impuesta al que distribuya o importe para su distribución información sobre gestión de derechos, a sabiendas que esta ha sido suprimida o alterada sin autorización; o distribuya, importe para su distribución, transmita, comunique o ponga a disposición del público copias de las obras, interpretaciones o ejecuciones o fonogramas, a sabiendas que la información sobre gestión de derechos ha sido suprimida o alterada sin autorización.

Artículo 220-E: Etiquetas, carátulas o empaques;

El que fabrique, comercialice, distribuya, almacene, transporte, transfiera o de otra manera disponga con fines comerciales u otro tipo de ventaja económica etiquetas o carátulas no auténticas adheridas o diseñadas para ser adheridas a un fonograma, copia de un programa de ordenador, documentación o empaque de un programa de ordenador o a la copia de una obra cinematográfica o cualquier otra obra audiovisual,

será reprimido con pena privativa de libertad no menor de tres años ni mayor de seis años y de y de sesenta a ciento veinte días multa.

Artículo 220-F: Manuales, licencias u otra documentación, o empaques no auténticos relacionados a programas de ordenador

El que elabore, comercialice, distribuya, almacene, transporte, transfiera o de otra manera disponga con fines comerciales u otro tipo de ventaja económica manuales, licencias u otro tipo de documentación, o empaques no auténticos para un programa de ordenador, será reprimido con pena privativa de libertad no menor de cuatro años ni mayor de seis años y de sesenta a ciento veinte días multa.

1.2.9.4. Delitos Contra la Fe Pública Falsificación de Documentos en General

Artículo 427.- Falsificación de documentos

El que hace, en todo o en parte, un documento falso o adultera uno verdadero que pueda dar origen a derecho u obligación o servir para probar un hecho, con el propósito de utilizar el documento, será reprimido, si de su uso puede resultar algún perjuicio, con pena privativa de libertad no menor de dos ni mayor de diez años y con treinta a noventa días-multa si se trata de un documento público, registro público, título auténtico o cualquier otro trasmisible por endoso o al portador y con pena privativa de libertad no menor de dos ni mayor de cuatro años, y con ciento ochenta a trescientos sesenta y cinco días-multa, si se trata de un documento privado.

Artículo 428° Falsedad ideológica

El que inserta o hace insertar, en instrumento público, declaraciones falsas concernientes a hechos que deban probarse con el documento, con el objeto de emplearlo como si la declaración fuera conforme a la verdad, será reprimido, si de su uso puede resultar algún perjuicio, con pena privativa de libertad no menor de tres ni mayor de seis años y con ciento ochenta a trescientos sesenta y cinco días-multa. El que hace uso del documento como si el contenido fuera exacto, siempre que de su uso pueda resultar algún perjuicio, será reprimido, en su caso, con las mismas penas.

1.2.10. CUADROS COMPARATIVOS

- Cuadro Comparativo Conceptualizado

Tipo	Código Penal Peruano	Convenio de Budapest
Delitos contra La confidencialidad, La integridad y la disponibilidad de los datos y sistemas informáticos	Acceso ilícito: El que deliberada e ilegítimamente accede a todo o en 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. (Fuente: Ley N° 30096 modificada por Ley N° 30171)	Acceso ilícito (Art. 2): Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno el acceso deliberado e ilegítimo a todo o partes de un sistema informático. Las Partes podrán exigir que el delito se cometa infringiendo medidas de seguridad, con la intención de obtener datos informáticos u otra intención delictiva, o en relación con un sistema informático conectado a otro sistema informático.
	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 del mismo, incluidas las emisiones electromagnéticas provenientes de un sistema informático que transporte dichos datos	Interceptación ilícita (Art. 3): Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la interceptación deliberada e ilegítima por medios técnicos de datos informáticos en transmisiones no públicas dirigidas a un sistema informático, originadas en un sistema informático o efectuadas dentro del mismo, incluidas las

	informáticos, será reprimido con una pena privativa de libertad no menor de tres ni mayor de seis años. La pena privativa de libertad será no menor de cinco ni mayor de ocho años cuando el delito recaiga sobre información clasificada como secreta, reservada o confidencial de conformidad con la Ley 27806, Ley de Transparencia y Acceso a la Información Pública. La pena privativa de libertad será no menor de ocho ni mayor de diez cuando el delito comprometa la defensa, seguridad o soberanía nacionales. (Fuente: Ley N° 30096 modificada por Ley N° 30171)	emisiones electromagnéticas provenientes de un sistema informático que transporte dichos datos informáticos. Las Partes podrán exigir que el delito se cometa con intención delictiva o en relación con un sistema informático conectado a otro sistema informático.
	Atentado a la integridad de datos informáticos: El que deliberada e ilegítimamente 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.	Ataques a la integridad de los datos (Art. 4): 1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno todo acto deliberado e ilegítimo que dañe, borre, deteriore, altere o suprima datos informáticos. 2. Las Partes podrán reservarse el derecho a exigir que los actos definidos en el párrafo 1 comporten daños graves.

	Atentado a la integridad de sistemas informáticos: El que deliberada e ilegítimamente inutiliza, 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. (Fuente: Ley N° 30096 modificada por Ley N° 30171)	Ataques a la integridad del sistema (Art. 5): Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la obstaculización grave, deliberada e ilegítima del funcionamiento de un sistema informático mediante la introducción, transmisión, daño, borrado, deterioro, alteración o supresión de datos informáticos.
	Abuso de mecanismos y dispositivos informáticos: El que deliberada e ilegítimamente fabrica, diseña, desarrolla, vende, facilita, distribuye, importa u obtiene para su utilización, uno o más mecanismos, programas informáticos, dispositivos, contraseñas, códigos de acceso o cualquier otro dato informático, específicamente diseñados para la comisión de los delitos previstos en la presente Ley, o el que ofrece o presta servicio que contribuya a ese propósito, será reprimido con pena privativa de	Abuso de los dispositivos (Art. 6): Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la comisión deliberada e ilegítima de los siguientes actos: a) la producción, venta, obtención para su utilización, importación, difusión u otra forma de puesta a disposición de: (i)un dispositivo, incluido un programa informático, diseñado o adaptado principalmente para la comisión de cualquiera de los delitos previstos de conformidad con los anteriores artículos 2 a 5; (ii)una contraseña, un

	libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días-multa.” (Fuente: Ley N° 30096 modificada por Ley N° 30171)	código de acceso o datos informáticos similares que permitan tener acceso a la totalidad o a una parte de un sistema informático, con el fin de que sean utilizados para la comisión de cualquiera de los delitos contemplados en los artículos 2 a 5; y b)la posesión de alguno de los elementos contemplados en los anteriores apartados (i) o (ii) con el fin de que sean utilizados para cometer cualquiera de los delitos previstos en los artículos 2 a 5. Cualquier Parte podrá exigir en su derecho interno que se posea un número determinado de dichos elementos para que se considere que existe responsabilidad penal.
Delitos informáticos	Falsedad ideológica: El que inserta o hace insertar, en instrumento público, declaraciones falsas concernientes a hechos que deban probarse con el documento, con el objeto de emplearlo como si la declaración fuera conforme a la verdad, será reprimido, si de su uso puede resultar algún perjuicio, con pena privativa de libertad no menor de tres ni mayor	Falsificación informática (Art. 7): Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno, cuando se cometa de forma deliberada e ilegítima, la introducción, alteración, borrado o supresión de datos informáticos que dé lugar a datos no auténticos, con la intención de que sean tenidos en cuenta o

	de seis años y con ciento ochenta a trescientos sesenta y cinco días-multa. El que hace uso del documento como si el contenido fuera exacto, siempre que de su uso pueda resultar algún perjuicio, será reprimido, en su caso, con las mismas penas. (Fuente: Art. 428 CP)	utilizados a efectos legales como si se tratara de datos auténticos, con independencia de que los datos sean o no directamente legibles e inteligibles. Cualquier Parte podrá exigir que exista una intención fraudulenta o una intención delictiva similar para que se considere que existe responsabilidad penal.
	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, 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	Fraude Informático (Art. 8): Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno los actos deliberados e ilegítimos que causen un perjuicio patrimonial a otra persona mediante: a) cualquier introducción, alteración, borrado o supresión de datos informáticos; b) cualquier interferencia en el funcionamiento de un sistema informático, con la intención fraudulenta o delictiva de obtener ilegítimamente un beneficio económico para uno mismo o para otra persona.

	destinado afines asistenciales o a programas de apoyo social. (Fuente: Ley N° 30096 modificada por Ley N° 30171)	
Delitos relacionados con el contenido	Pornografía infantil: El que posee, promueve, fabrica, distribuye, exhibe, ofrece, comercializa o publica, importa o exporta por cualquier medio objetos, libros, escritos, imágenes, videos o audios, o realiza espectáculos en vivo de carácter pornográfico, en los cuales se utilice a personas de catorce y menos de dieciocho años de edad, será sancionado con pena privativa de libertad no menor de seis ni mayor de diez años y con ciento veinte a trescientos sesenta y cinco días multa. La pena privativa de libertad será no menor de diez ni mayor de doce años y de cincuenta a trescientos sesenta y cinco días multa cuando:1. El menor tenga menos de catorce años de edad.2. El material pornográfico se difunda a través de las tecnologías de la información o de la comunicación. Si la	Delitos relacionados con la pornografía infantil (Art: 9): Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la comisión deliberada e ilegítima de los siguientes actos: a) la producción de pornografía infantil con vistas a su difusión por medio de un sistema informático; b) la oferta o la puesta a disposición de pornografía infantil por medio de un sistema informático; c) la difusión o transmisión de pornografía infantil por medio de un sistema informático, d) la adquisición de pornografía infantil por medio de un sistema informático para uno mismo o para otra persona; e) la posesión de pornografía infantil en un sistema informático o en un medio de almacenamiento de datos informáticos.2. A los efectos del anterior apartado 1, por pornografía infantil se entenderá todo material

	víctima se encuentra en alguna de las condiciones previstas en el último párrafo del artículo 173 o si el agente actúa en calidad de integrante de una organización dedicada a la pornografía infantil, la pena privativa de libertad será no menor de doce ni mayor de quince años. De ser el caso, el agente será inhabilitado conforme a los numerales 1, 2 y 4 del artículo 36. (Fuente: Art.183-A CP modificado por la Ley N° 30096)	pornográfico que contenga la representación visual de: a) un menor comportándose de una forma sexualmente explícita; b) una persona que parezca un menor comportándose de una forma sexualmente explícita; c) imágenes realistas que representen a un menor comportándose de una forma sexualmente explícita. 3. A los efectos del anterior apartado 2, por menor se entenderá toda persona menor de 18 años. No obstante, cualquier Parte podrá establecer un límite de edad inferior, que será como mínimo de 16 años. 4. Cualquier Parte podrá reservarse el derecho a no aplicar, en todo o en parte, las letras d) y e) del apartado 1, y las letras b) y c) del apartado 2.
Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines	Delitos contra los derechos intelectuales: Artículo 216: Copia o reproducción no autorizada; Artículo 217: Reproducción, difusión, distribución y circulación de la obra sin la autorización del autor; Artículo 218: Formas agravadas; Artículo 219: Plagio; Artículo 220:	Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines (Art. 10): 1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno las infracciones de la propiedad intelectual,

	Formas agravadas; Artículo 220-A: Elusión de medida tecnológica efectiva; Artículo 220-B: Productos destinados a la elusión de medidas tecnológicas; Artículo 220-C: Servicios destinados a la elusión de medidas tecnológicas; Artículo 220-D: Delitos contra la información sobre gestión de derechos; Artículo 220-E: Etiquetas, carátulas o empaques; Artículo 220-F: Manuales, licencias u otra documentación, o empaques no auténticos relacionados a programas de ordenador (Fuente: Art. 216 al 220 del CP)	según se definan en la legislación de dicha Parte, de conformidad con las obligaciones asumidas en aplicación del Acta de París de 24 de julio de 1971 por la que se revisó el Convenio de Berna para la protección de las obras literarias y artísticas, del Acuerdo sobre los aspectos de los derechos de propiedad intelectual relacionados con el comercio y del Tratado de la OMPI sobre la propiedad intelectual, a excepción de cualquier derecho moral otorgado por dichos Convenios, cuando esos actos se cometan deliberadamente, a escala comercial y por medio de un sistema informático. 2. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno las infracciones de los derechos afines definidas en la legislación de dicha Parte, de conformidad con las obligaciones que ésta haya asumido en aplicación de la Convención Internacional sobre la protección de los artistas intérpretes o ejecutantes, los

		productores de fonogramas y los organismos de radiodifusión (Convención de Roma), del Acuerdo sobre los aspectos de los derechos de propiedad intelectual relacionados con el comercio y del Tratado de la OMPI sobre las obras de los intérpretes y ejecutantes y los fonogramas, a excepción de cualquier derecho moral otorgado por dichos Convenios, cuando esos actos se cometan deliberadamente, a escala comercial y por medio de un sistema informático. 3. En circunstancias bien delimitadas, cualquier Parte podrá reservarse el derecho a no exigir responsabilidad penal en virtud de los apartados 1 y 2 del presente artículo, siempre que se disponga de otros recursos efectivos y que dicha reserva no vulnere las obligaciones internacionales que incumban a dicha Parte en aplicación de los instrumentos internacionales mencionados en los apartados 1 y 2 del presente artículo.

- Cuadro Comparativo con Articulado

Convenio de Budapest	El Perú	Comentario
Capítulo I – Terminología		
Artículo 1 - Definiciones -Sistema informático, - Datos informáticos, - Proveedor de servicios, -Datos relativos al tráfico	El Código Penal no señala definiciones	Solo describe las conductas punibles y sus correspondientes sanciones.
Capítulo II - Medidas que deberán adoptarse a nivel nacional		
Sección 1 - Derecho penal sustantivo		
Título 1 - Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos		
Artículo 2 - Acceso ilícito	Artículo 2 de la Ley 30096, Ley de delitos informáticos - Acceso ilícito; y su modificatoria en la Ley 30171, Ley que modifica la Ley 30096.	El artículo 2 establece los plazos de pena privativa de libertad y los días multa.
Artículo 3 – Interceptación ilícita	Artículo 7 de la Ley 30096, Ley de delitos informáticos - Interceptación de datos informáticos; y su modificatoria en la Ley 30171, Ley que modifica la Ley 30096.	El artículo 7 establece los plazos de pena privativa de libertad.
Artículo 4 - Ataques a la integridad de los datos	Artículo 3 de la Ley 30096, Ley de delitos informáticos - Atentado a la	El artículo 3 establece plazos de pena privativa de libertad y días-multa.

	integridad de datos informáticos; y su modificatoria en la Ley 30171, Ley que modifica la Ley 30096.	
Artículo 5 - Ataques a la integridad del sistema	Artículo 4 de la Ley 30096, Ley de delitos informáticos - Atentado a la integridad de sistemas informáticos; y su modificatoria en la Ley 30171, Ley que modifica la Ley 30096.	El artículo 4 establece plazos de pena privativa de libertad y días-multa.
Artículo 6 - Abuso de los dispositivos	*Artículo 10 de la Ley 30096, Ley de delitos informáticos - Abuso de mecanismos y dispositivos informáticos; y su modificatoria en la Ley 30171, Ley que modifica la Ley 30096.	*La legislación peruana no sanciona actos preparatorios, pero sí la tenencia ilegal de armas (delito de peligro). La legislación peruana podría incorporar los conceptos del Convenio.
Título 2 – Delitos informáticos		
Artículo 7 - Falsificación Informática	La legislación peruana no prevé la figura de falsedad informática, pero se podría incorporar dentro del título de delitos contra la Fe Pública como	En la declaración del artículo se hace mención de que se podrá exigir que exista una intención fraudulenta o delictiva similar para generar responsabilidad penal.

	conducta que utiliza sistemas informáticos.	
Artículo 8 – Fraude informático	Artículo 8 de la Ley 30096, Ley de delitos informáticos – Fraude Informático; y su modificatoria en la Ley 30171, Ley que modifica la Ley 30096.	El artículo 8 establece plazos de pena privativa de libertad y días-multa.
Título 3 - Delitos relacionados con el contenido		
Artículo 9 – Delitos relacionados con la pornografía infantil	Artículo 181-A. del Código Penal - Turismo sexual infantil y Artículo 183- A. del Código Penal – Pornografía Infantil.	Los artículos establecen el tiempo de pena privativa según los casos presentados y tendrán relación con el artículo 36. El artículo 183- A podría tener relación con el artículo 173 del Código Penal según las condiciones del caso.
Título 4 – Delitos relacionados con infracciones de la propiedad intelectual y de los derechos Afines		
Artículo 10 – Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines	Temas en materia de Propiedad intelectual, industrial y de derechos conexos son regulados por la Convención de Roma.	El Código Penal prevé un título de delitos contra la propiedad intelectual y propiedad industrial.
Título 5 - Otras formas de responsabilidad y de sanción		
Artículo 11 - Tentativa y Complicidad	El Código Penal trata la tentativa en el Capítulo II de la Parte General (artículos 16 al 19). En relación a la	

	complicidad, está regulado en el Capítulo IV de la Parte General (artículos 23 al 27).	
Artículo 12 - Responsabilidad de las personas jurídicas	Artículo 27 del Código Penal - Actuación en nombre de otro y Artículo 105 del Código Penal - Medidas aplicables a las personas jurídicas.	El artículo 27 describe los actos que generan responsabilidad penal y el artículo 105 las medidas aplicables como clausura, disolución, liquidación, suspensión, prohibición de actividades, con sus correspondientes plazos.
Artículo 13 - Sanciones y medidas	Artículo 28 del Código Penal - Clases de Pena y Artículo 105 - Medidas aplicables a las personas jurídicas.	El artículo 28 establece cuatro penas aplicables: privativa de libertad, restrictiva de libertad, limitativas de derechos y multa.

1.3. DEFINICIÓN DE TÉRMINOS BÁSICOS

A continuación procedemos a desarrollar los conceptos operacionales de los principales términos jurídicos, relevantes en el presente tema de investigación, los cuales han sido ordenados alfabéticamente, como detallamos a continuación:

a. **Adolescente.**

Se considera adolescente a todo ser humano desde los doce hasta cumplir los dieciocho años de edad. (CNA, 2000, Art. I del Título Preliminar)

b. **Concurso Ideal de Delitos.**

Cuando varias disposiciones son aplicables al mismo hecho se reprimirá hasta con el máximo de la pena más grave, pudiendo incrementarse ésta hasta en una cuarta parte, sin que en ningún caso pueda exceder de treinta y cinco años. (CP, 1991 y 2006, Art. 48)

c. **Concurso Real de Delitos.**

Cuando concurran varios hechos punibles que deban considerarse como otros tantos delitos independientes, se sumarán las penas privativas de libertad que fije el juez para cada uno de ellos hasta un máximo del doble de la pena del delito más grave, no pudiendo exceder de 35 años. Si alguno de estos delitos se encuentra reprimido con cadena perpetua se aplicará únicamente ésta. (CP, 1991 y 2006, Art. 50)

d. **Datos informáticos.**

Toda representación de hechos, información o concepto expresados de cualquier forma que se preste a tratamiento informático, incluidos los programas diseñados para que un sistema informático ejecute una función.

e. **Delito.**

Acción o conducta típica, antijurídica, culpable y además punible; aquí se incluyen especiales elementos de punibilidad previstos en algunos tipos o para algunas personas. (Diccionario Español Jurídico de la RAE, 2016)

f.**Difundir.**

Propagar o divulgar conocimientos, noticias, actitudes, costumbres, modas, etc. (Diccionario de la RAE, 2017)

g. **Distribuir.**

Entregar una mercancía a los vendedores y consumidores. (Diccionario de la RAE, 2017)

h. **Falsedad.**

Es la ausencia de posibles verificaciones para lo que se está enjuiciando.

i. **Falsificación**

Es un acto consistente en la creación o modificación de ciertos documentos, efectos, productos (bienes o servicios), con el fin de hacerlos parecer como verdaderos o para alterar o simular la verdad.

j. **Indemne.**

Libre o exento de daño. (Diccionario de la RAE, 2017)

k. **Indemnidad Sexual.**

Derecho a que la persona no sufra interferencia en la formación de su propia sexualidad. Principalmente se aplica a los menores y personas incapaces. La violación de este derecho hace que afecte de forma psíquica al desarrollo y tomen como correctos actos que no lo son. Los sujetos afectados tienen como derecho, una vez sean adultos, de decidir sobre su propio comportamiento sexual. (Dudas legislativas.com, 2018).

l. **Informática.**

Conjunto de conocimientos científicos y técnicas que hacen posible el tratamiento automático de la información por medio de computadoras. (Dicc. RAE, 2017)

m. **Internet.**

Red mundial descentralizada, formada por la conexión directa entre ordenadores y demás dispositivos mediante un protocolo especial de comunicación, el TCP/IP, con el propósito de que los usuarios puedan comunicarse en el "ciberespacio" y acceder a grandes cantidades de información de todo el mundo. (Diccionario Español Jurídico de la RAE, 2016)

n. **Libertad Informática.**

Esfera de libertad personal que debe reconocerse a toda persona frente a los abusos de la informática. (Diccionario Español Jurídico de la RAE, 2016)

ñ. Libertad Sexual.

Facultad de la persona de autodeterminarse en el ámbito de su sexualidad. (Diccionario Español Jurídico de la RAE, 2016)

o. **Niño (a).**

Se considera niño a todo ser humano desde su concepción hasta cumplir los doce años de edad (CNA, 2000, Art. I del Título Preliminar)

p. **Pornografía**

La pornografía es la filmación, fotografiado y exposición de manera explícita de relaciones sexuales.

q. **Propiedad Intelectual.**

Es una regulación que engloba los derechos de los creadores y autores. A través de dicha regulación es posible su protección, organización y defensa frente a terceros.

r. **Proposición.**

Acción y efecto de proponer, es decir, hacer una propuesta. (Diccionario de la RAE, 2017).

s. **Sistema Informático**

Todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, cuya función, o la de alguno de sus elementos, será el tratamiento automatizado de datos en ejecución de un programa.

t.**Tecnología de la Información.**

Es un término que comprende todo lo que está vinculado con el almacenamiento, protección, procesamiento y transmisión de la información. Este concepto engloba todo lo relacionado con la informática, la electrónica y las telecomunicaciones. Los avances tecnológicos como el Internet, las comunicaciones móviles, los satélites, etc. Han hecho significativos cambios en el sistema económico y social, influyendo en las relaciones sociales.

CAPITULO II
PLANTEAMIENTO DE PROBLEMA

2.1. DESCRIPCIÓN DEL PROBLEMA

El incremento de la accesibilidad a la tecnología ha creado un nuevo panorama de las acciones de los “delitos informáticos”, que en la actualidad ya cuentan con tipificaciones en los diferentes marcos reglamentarios de la legislación peruana, a tal punto que llega a formar parte del Convenio de BUDAPEST. Hoy en día, los diferentes actos ilícitos con ayuda de los sistemas informáticos se han ido perfeccionando, desarrollándose diferentes delitos nuevos, que no se logran con armas convencionales, sino con las nuevas armas que nos ha dado la Internet, recibiendo estas, las sanciones respectivas a la gravedad o modalidad que se haya cometido dichos actos ilícitos.

Uno de los mayores problemas es que se han hecho varios intentos para adoptar una definición global del cibercrimen pero el alcance de este término es aún incierto, por razones a que todavía no se le da la debida importancia y no se hace de conocimiento a la población, de estos delitos que tienden a desarrollarse mediante el uso del internet, lo que no ha permitido un combate eficaz dado los alcances globales del problema, siendo el principal medio que utiliza el sujeto activo es la Internet.

Finalmente nos enfrentamos ante una problemática en la cual el sujeto activo conoce perfectamente de lenguajes de programación y han comprendido el funcionamiento de los sistemas que maneja una computadora conectada a la red para cometer sus finalidades ilícitas. No obstante, nuestro ordenamiento jurídico a través de convenio de Budapest ha ido innovando modalidades con la finalidad de que se puedan reprimir de manera eficiente estos delitos informáticos que atentan contra los derechos fundamentales de las personas.

Ante ese diagnóstico de la situación que existe en el Perú respecto a los delitos por medios informáticos, nuestro país en Febrero del 2019 ha ratificado el Convenio contra el cibercrimen de Budapest, esperándose que con la incorporación de esa norma internacional a nuestra legislación, se mejore la lucha contra los delincuentes informáticos.

En efecto, el pronóstico de la aplicación de ese Convenio en nuestro país, es que el estado que tiene el deber de cautelar los derechos de los individuos públicos, lo realizará con mayor efectividad, en tal sentido, al lograr regularse de manera eficaz las leyes que sancionan a los delincuentes informáticos, se va

lograr disminuir o contrarrestar los índices de criminalidad cibernética en nuestro país.

Por lo señalado, el problema que planteamos, está dirigido a identificar las modificaciones que incorpora el convenio contra el cibercrimen de Budapest, en la tipificación de los delitos por medios informáticos vigentes en nuestra legislación, analizándolo doctrinariamente, a partir del estudio de la legislación nacional y los instrumentos internacionales sobre la materia, siendo nuestra propuesta, que el referido Convenio, sí trae modificaciones tanto en nuestro Código Penal, como en la Ley de Delitos Informáticos, disposiciones que debidamente identificadas, podrán implementarse como parte de la lucha contra este tipo de criminalidad.

2.2 FORMULACIÓN DEL PROBLEMA

2.2.1 PROBLEMA GENERAL

¿Cuáles son las modificaciones en la tipificación de delitos que incorpora el Convenio contra el cibercrimen de Budapest en Perú el año 2019?

2.2.2 PROBLEMAS ESPECÍFICOS

Problema Específico 1

¿Cuáles son las modificaciones en la Ley de Delitos Informáticos que incorpora el Convenio contra el cibercrimen de Budapest en Perú el año 2019?

Problema Específico 2

¿Cuáles son las modificaciones en el Código Penal que incorpora el Convenio contra el cibercrimen de Budapest en Perú el año 2019?

2.3 OBJETIVOS

2.3.1 OBJETIVO GENERAL

Determinar las modificaciones en la tipificación de delitos que incorpora el Convenio contra el cibercrimen de Budapest en Perú el año 2019.

2.3.2 OBJETIVOS ESPECÍFICOS

Objetivo Específico 1

Establecer las modificaciones en la Ley de Delitos Informáticos que incorpora el Convenio contra el cibercrimen de Budapest en Perú el año 2019.

Objetivo Específico 2

Identificar las modificaciones en el Código Penal que incorpora el Convenio contra el cibercrimen de Budapest en Perú el año 2019.

2.4 JUSTIFICACIÓN DE LA INVESTIGACIÓN

El presente trabajo es de importancia y valor teórico, toda vez que va a servir para conocer el contenido del Convenio contra el Cibercrimen de Budapest y como influencia en la legislación peruana.

En ese sentido, su Implicancia Práctica radica en que el referido Convenio ha sido ratificado por el Perú en el mes de Febrero del 2019, a través de la Resolución Legislativa N° 30913, motivo por el cual los aportes teóricos sobre los delitos que regula ese Convenio, serán analizados a partir de la comparación con los delitos tipificados en la Ley de Delitos Informáticos y el Código Penal peruano.

Su Relevancia Social, la podemos encontrar en que el presente estudio va a ser de utilidad para los operadores del sistema de justicia en materia penal, y en general para todos los abogados que se haya imbuidos en el diario quehacer profesional del derecho penal y en especial de los delitos por medios informáticos.

Finalmente, podemos precisar que la Utilidad Metodológica de este estudio, contribuye al conocimiento sobre el Convenio contra el Cibercrimen de Budapest y servirá como punto de partida para otros estudios más detallados sobre los diferentes delitos por medios informáticos.

2.5 HIPOTESIS

Las modificaciones en la tipificación de delitos que incorpora el Convenio contra el cibercrimen de Budapest el año 2019, se producen en la Ley de Delitos Informáticos y en el Código Penal.

2.6 VARIABLES

2.6.1 IDENTIFICACIÓN DE LA VARIABLE

- Variable.
  Convenio contra el cibercrimen de Budapest.

2.6.2 DEFINICIÓN CONCEPTUAL Y OPERACIONAL DE LA VARIABLE.

Definición Conceptual de la Variable.

El Convenio sobre el Cibercrimen, también conocido como el Convenio de Budapest, es un tratado internacional vinculante en materia penal, que establece herramientas legales para perseguir penalmente aquellos delitos cometidos ya sea en contra de sistemas o medios informáticos, o mediante el uso de los mismos.

Definición Operacional de la variable.

La variable se define operacionalmente como un tratado internacional vinculante en materia penal, que establece herramientas legales para perseguir penalmente a los cibercriminales o ciberdelincuentes, por delitos cometidos en contra de sistemas o medios informáticos, o mediante el uso de los mismos; el cual será investigado a través de una Ficha de Registro de Datos con el índice si/no incluye.

2.6.3 OPERACIONALIZACIÓN DE LAS VARIABLES.

VARIABLE	INDICADORES	INDICES
CONVENIO CONTRA EL CIBERCRIMEN DE BUDAPEST	Ley de Delitos Informáticos: • Modificaciones en el Delito de Acceso Ilícito. • Modificaciones en el Delito de Atentado contra la Integridad de datos informáticos. • Modificaciones en el Delito de Atentado contra la Integridad de sistemas informáticos. • Modificaciones en el Delito de Grooming • Modificaciones en el Delito de Interceptación de Datos Informáticos. • Modificaciones en el Delito de Fraude Informático. • Modificaciones en el Delito de Suplantación de Identidad	Si /No incluye

	Código Penal: • Modificaciones en el Delito de Pornografía Infantil. • Modificaciones en los Delitos contra la propiedad intelectual. • Modificaciones en los Delitos contra la fe pública.	Si/No incluye

CAPITULO III
METODOLOGÍA

3.1 TIPO Y DISEÑO DE INVESTIGACIÓN

Las investigaciones pueden ser básicas o aplicadas, una investigación es de tipo básica, porque está orientada a lograr un nuevo conocimiento de manera sistemática metódica, con el objetivo de ampliar el conocimiento de una nueva realidad, mientras que la investigación es aplicada cuando está orientada a lograr un nuevo conocimiento, destinado a procurar soluciones de problemas prácticos (Alzamora De Los Godos, 2009, p. 13); en tal sentido, por la finalidad de la presente investigación, consideramos que es básica, también denominada, teórica o dogmática, porque busca ampliar el conocimiento sobre la Convención contra el Cibercrimen de Budapest y su innovación en la tipificación de delitos en Perú en el año 2019.

El diseño de investigación es el plan o estrategia concebida para obtener la información que se desea con el fin de responder al planteamiento del problema. El diseño de investigación es de dos tipos, experimental y no experimental, el cual puede ser a su vez longitudinal o transversal, siendo los tipos del transversal, los exploratorios, descriptivos, correlaciónales y explicativos causales (Hernández, 2014, p. 127-128). De conformidad con lo señalado por el prestigioso investigador mexicano, el diseño de la presente investigación es no experimental – transversal – descriptivo.

Esta investigación es descriptiva, debido a que se va a describir la Convención contra el Cibercrimen de Budapest y su innovación en la tipificación de delitos en Perú en el año 2019; es transversal debido a que se estudia la variable en un tiempo determinado y único (Gavagnin, 2009, p. 117), habiéndose escogido en este caso el período de tiempo del año 2019. Es no experimental debido a que no se genera ninguna situación, sino que se observan situaciones ya existentes, no provocadas intencionalmente en la investigación por quién la realiza (Hernández, 2014, p. 152).

3.2 POBLACIÓN Y MUESTRA

La población es finita, al estar compuesta por el estudio de la tipificación de delitos por medios informáticos en tres documentos legales que son la Convención contra el Cibercrimen de Budapest, la Ley de Delitos Informáticos y el Código Penal.

La muestra corresponde al 100% de la población, centrando el estudio en los aspectos pertinentes de los tres dispositivos legales antes enunciados.

3.3 TÉCNICAS, INSTRUMENTOS Y PROCEDIMIENTOS DE RECOLECCIÓN DE DATOS

3.3.1 TÉCNICAS DE RECOLECCIÓN DE DATOS

La Técnica a utilizar será el análisis documental.

3.3.2 INSTRUMENTOS DE RECOLECCIÓN DE DATOS

El Instrumento a aplicar será la Ficha de registro de datos.

3.3.3 PROCEDIMIENTOS DE RECOLECCIÓN DE DATOS

Se recolectarán los datos a partir del análisis minucioso de los documentos que conforman la muestra, en lo referente a delitos por medios informáticos considerados en la Convención contra el Cibercrimen de Budapest.

3.3.4 PROCESAMIENTO Y ANÁLISIS DE DATOS.

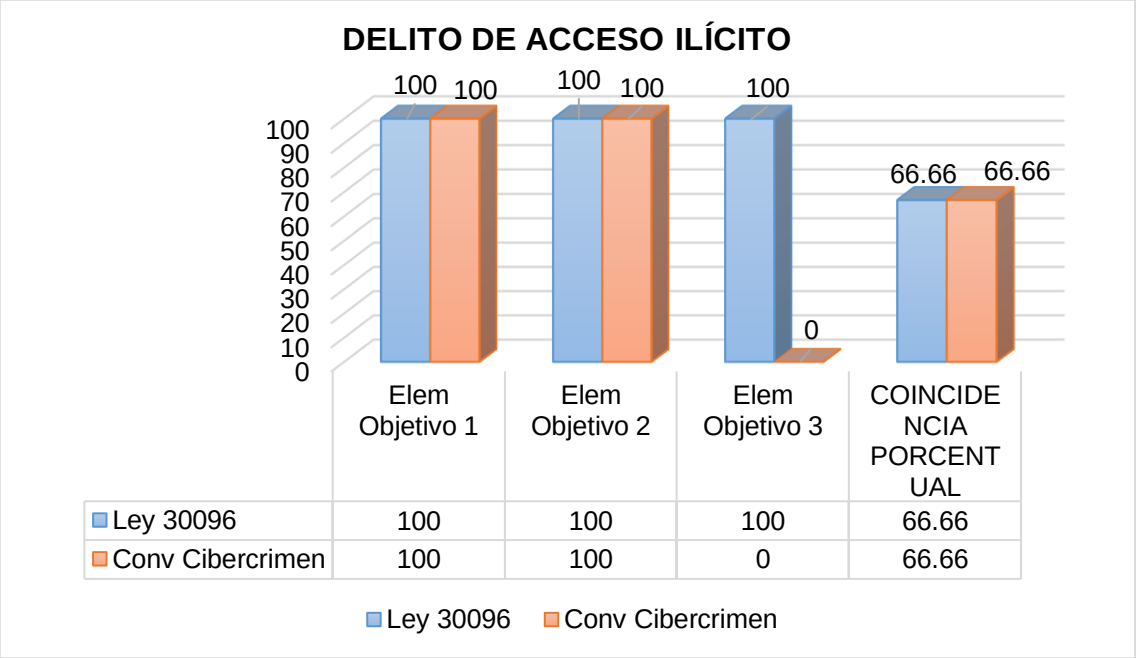
El análisis e interpretación de los datos se realizarán empleando la estadística descriptiva, frecuencia, modo, y porcentaje para el estudio de la variable. Para el análisis e interpretación de la información recolectada se utilizará el software SPSS versión 22, donde se realizará el vaciado de todos los datos obtenidos, para posteriormente ser analizados estadísticamente y luego ser presentados en forma tabular y gráfica.

CAPITULO I V
RESULTADOS
Cuadro 1
COMPARACIÓN ENTRE LA LEY N°30096 LEY DE DELITOS INFORMATICOS Y EL CONVENIO CONTRA EL CIBERCRIMEN RESPECTO AL "DELITO DE ACCESO ILICITO"

	ELEMENTOS OBJETIVOS	LEY 30096 – DE DELITOS "INFORMATICOS ACCESO ILICITO"	CONVENIO CIBERCRIMEN "ACCESO ILÍCITO"	TOTAL
DELITOS CONTRA LA CONFIDENCIALIDAD, LA INTEGRIDAD Y LA DISPONIBILIDAD DE LOS DATOS Y SISTEMAS INFORMÁTICOS.	1er elemento objetivo	Acceso a un Sistema Informático	Acceso deliberado e ilegítimo a un sistema informático.	Si 100%
	2do elemento objetivo	Vulneración de Medidas de Seguridad	Acceso deliberado e ilegítimo a un sistema informático. Infringiendo medidas de seguridad,	Si 100%
	3er elemento objetivo	Exceder los Límites de Autorización de Acceso.		No 0%
TOTAL DE COINCIDENCIA PORCENTUAL				**66,66%**

Fuente: Base de Datos del Autor

Gráfico 1



Fuente: Cuadro N° 1

En la Tabla N° 1 y el Gráfico N° 1 se presenta al delito de Acceso Ilícito, el que se encuentra conformado por tres elementos objetivos, de los cuales dos se repiten en la Convención contra el Cibercrimen, teniendo 100% de coincidencia en cada uno, y el tercer elemento objetivo no se repite, con 0% de coincidencia, lo que nos da un porcentaje total de coincidencia de 66.66%.

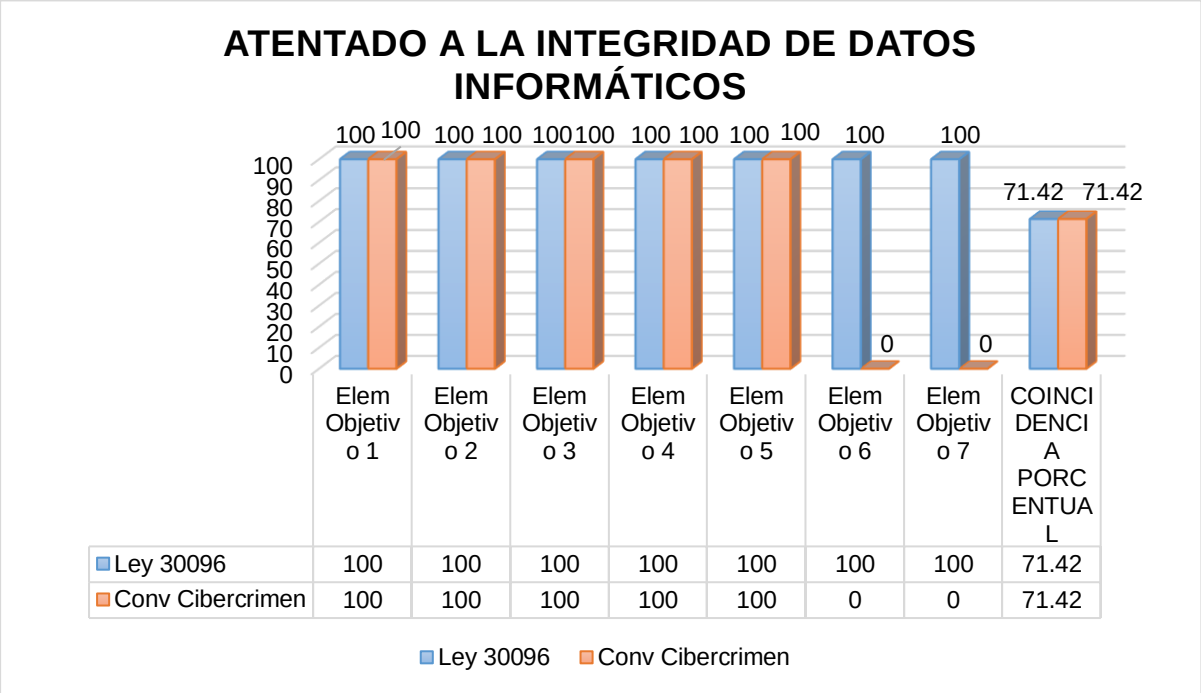
Cuadro 2

COMPARACIÓN ENTRE LA LEY N°30096 LEY DE DELITOS INFORMATICOS Y EL CONVENIO CONTRA EL CIBERCRIMEN RESPECTO AL "DELITO DE ATENTADO A LA INTEGRIDAD DE DATOS INFORMÁTICOS"

DELITOS CONTRA LA CONFIDENCIALIDAD, LA INTEGRIDAD Y LA DISPONIBILIDAD DE LOS DATOS Y SISTEMAS INFORMÁTICOS.	ELEMENTOS OBJETIVOS	LEY 30096 – DE DELITOS INFORMATICOS "ATENTADO A LA INTEGRIDAD DE DATOS INFORMÁTICOS"	CONVENIO CIBERCRIMEN "ATAQUES A LA INTEGRIDAD DE LOS DATOS"	TOTAL
	1er elemento objetivo	Dañar Datos Informáticos.	Dañe datos informáticos.	SI 100%
	2do elemento objetivo	Borrar Datos Informáticos.	Borre datos informáticos.	SI 100%
	3er elemento objetivo	Deteriorar Datos Informáticos.	Deteriore datos informáticos.	SI 100%
	4to elemento objetivo	Alterar Datos Informáticos.	Altere datos informáticos.	SI 100%
	5to elemento objetivo	Suprimir Datos Informáticos.	Suprima datos informáticos.	SI 100%
	6to elemento objetivo	Hacer Inaccesibles Datos Informáticos.		NO 0%
	7mo elemento objetivo	Introducir Datos Informáticos.		NO 0%
TOTAL DE COINCIDENCIA PORCENTUAL				**71,42%**

Fuente: Base de Datos del Autor

Gráfico 2



Fuente: Cuadro N° 2

En la Tabla N° 2 y el Gráfico N° 2 se presenta al delito de Atentado a la Integridad de Datos Informáticos, el que se encuentra conformado por siete elementos objetivos, de los cuales cinco se repiten en la Convención contra el Cibercrimen, teniendo 100% de coincidencia en cada uno, y el sexto, séptimo elemento objetivo no se repiten, con 0% de coincidencia, lo que nos da un porcentaje total de coincidencia de 71.42%.

Cuadro 3

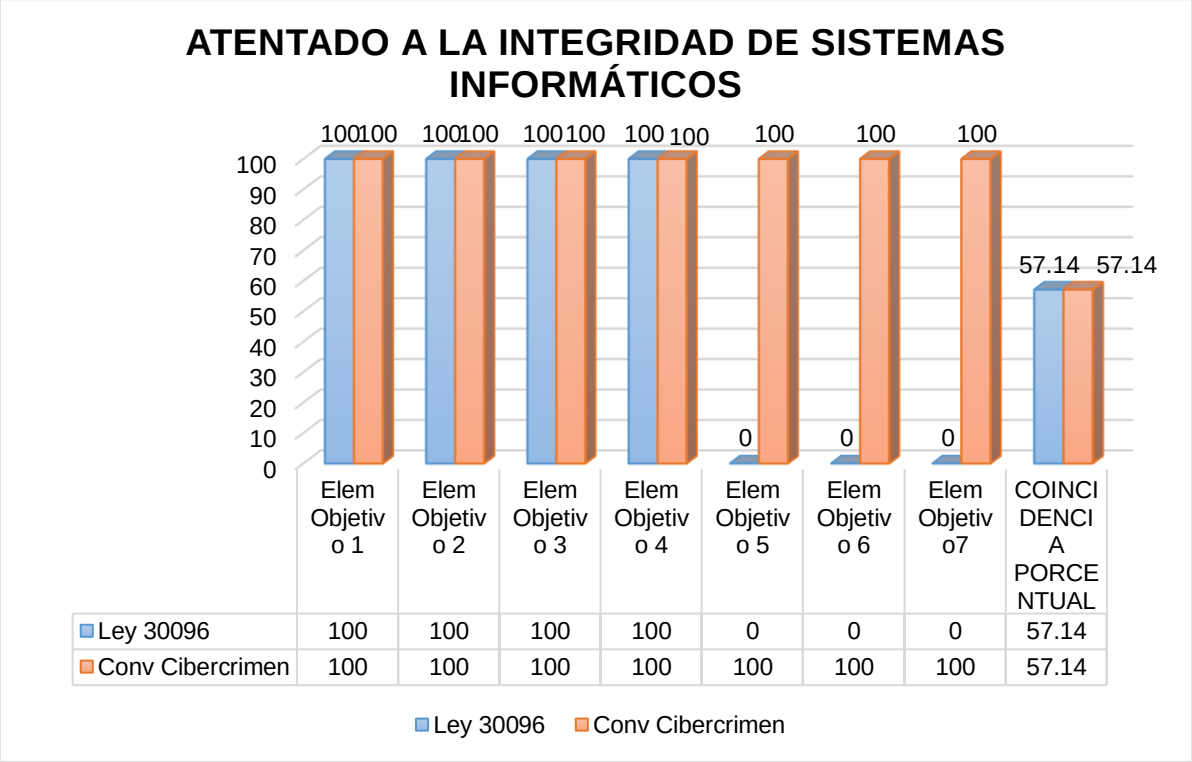
COMPARACIÓN ENTRE LA LEY N°30096 LEY DE DELITOS INFORMATICOS Y EL CONVENIO CONTRA EL CIBERCRIMEN RESPECTO AL "DELITO DE ATENTADO A LA INTEGRIDAD DE SISTEMAS INFORMÁTICOS"

	ELEMENTOS OBJETIVOS	LEY 30096 – DE DELITOS INFORMATICOS "ATENTADO A LA INTEGRIDAD DE SISTEMAS INFORMÁTICOS"	CONVENIO CIBERCRIMEN "ATAQUES A LA INTEGRIDAD DEL SISTEMA"	TOTAL
DELITOS CONTRA LA CONFIDENCIALIDAD, LA INTEGRIDAD Y LA DISPONIBILIDAD DE LOS DATOS Y SISTEMAS INFORMÁTICOS.	1er elemento objetivo	Inutiliza, total o parcialmente, un sistema informático.	Alteración datos informáticos que obstaculice el funcionamiento de un sistema informático.	SI 100%
	2do elemento objetivo	Impide el acceso a un sistema informático.	Supresión de datos informáticos que obstaculice el funcionamiento de un sistema informático.	SI 100%
	3er elemento objetivo	Entorpece su funcionamiento o la prestación de sus servicios.	Daño datos informáticos que obstaculice el funcionamiento de un sistema informático.	SI 100%
	4to elemento objetivo	Imposibilita su funcionamiento o la prestación de sus servicios.	Deterioro datos informáticos que obstaculice el funcionamiento	SI 100%

			de un sistema informático.	
	5to Elemento Objetivo		Introducción datos informáticos que obstaculice el funcionamiento de un sistema informático.	NO 0%
	6to Elemento Objetivo		Transmisión datos informáticos que obstaculice el funcionamiento de un sistema informático.	NO 0%
	7mo Elemento Objetivo		Borrado datos informáticos que obstaculice el funcionamiento de un sistema informático.	NO 0%
TOTAL DE COINCIDENCIA PORCENTUAL				**57,14%**

Fuente: Base de Datos del Autor

Gráfico 3



Fuente: Cuadro N° 3

En la Tabla N° 3 y el Gráfico N° 3 se presenta al delito de Atentado a la Integridad de Sistemas Informáticos, el que se encuentra conformado por siete elementos objetivos, de los cuales cuatro se repiten en la Convención contra el Cibercrimen, teniendo 100% de coincidencia en cada uno, y el quinto, sexto y séptimo elemento objetivo no se repiten, con 0% de coincidencia, lo que nos da un porcentaje total de coincidencia de 57.14%.

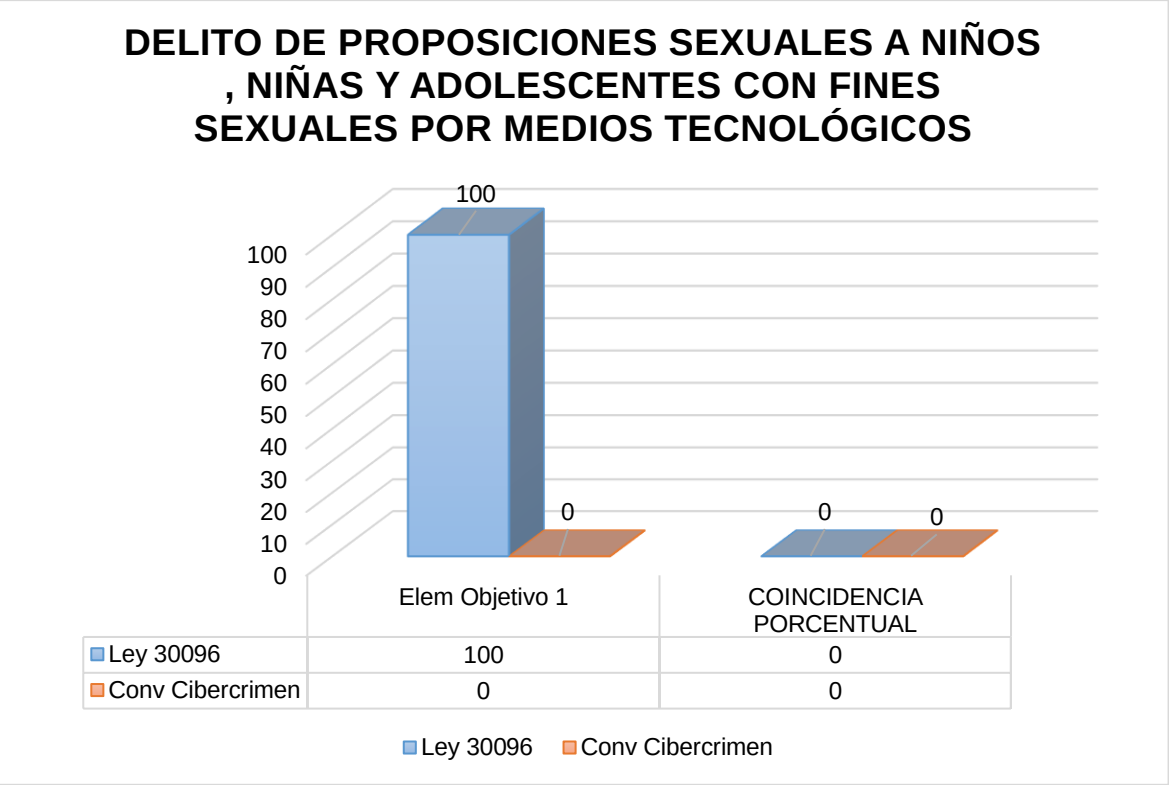
Cuadro 4

COMPARACIÓN ENTRE LA LEY N°30096 LEY DE DELITOS INFORMATICOS Y EL CONVENIO CONTRA EL CIBERCRIMEN RESPECTO AL "DELITO DE PROPOSICIONES A NIÑOS, NIÑAS Y ADOLESCENTES CON FINES SEXUALES POR MEDIOS TECNOLOGICOS"

DELITOS INFORMÁTICOS CONTRA LA INDEMNIDAD Y LIBERTAD SEXUALES	ELEMENTOS OBJETIVOS	LEY 30096 – DE DELITOS "PROPOSICIONES A NIÑOS, NIÑAS Y ADOLESCENTES CON FINES SEXUALES POR MEDIOS TECNOLOGICOS"	CONVENIO CIBERCRIMEN "PROPOSICIONES A NIÑOS, NIÑAS Y ADOLESCENTES CON FINES SEXUALES POR MEDIOS TECNOLOGICOS"	TOTAL
	1er elemento objetivo	Contactar con un menor de edad por la internet u otro medio análogo para solicitar material pornográfico o llevar a cabo actividades sexuales.	.	NO 0%
TOTAL DE COINCIDENCIA PORCENTUAL				**00%**

Fuente: Base de Datos del Autor

Gráfico 4



Fuente: Cuadro N° 4

En la Tabla N° 4 y el Gráfico N° 4 se presenta al delito de Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos, el que se encuentra conformado por un elemento objetivo, de los cuales no se repiten en la Convención contra el Cibercrimen ni en la Ley 30096 de Delitos informáticos, teniendo 00% de coincidencia en cada uno, lo que nos da un porcentaje total de coincidencia de 00.00%.

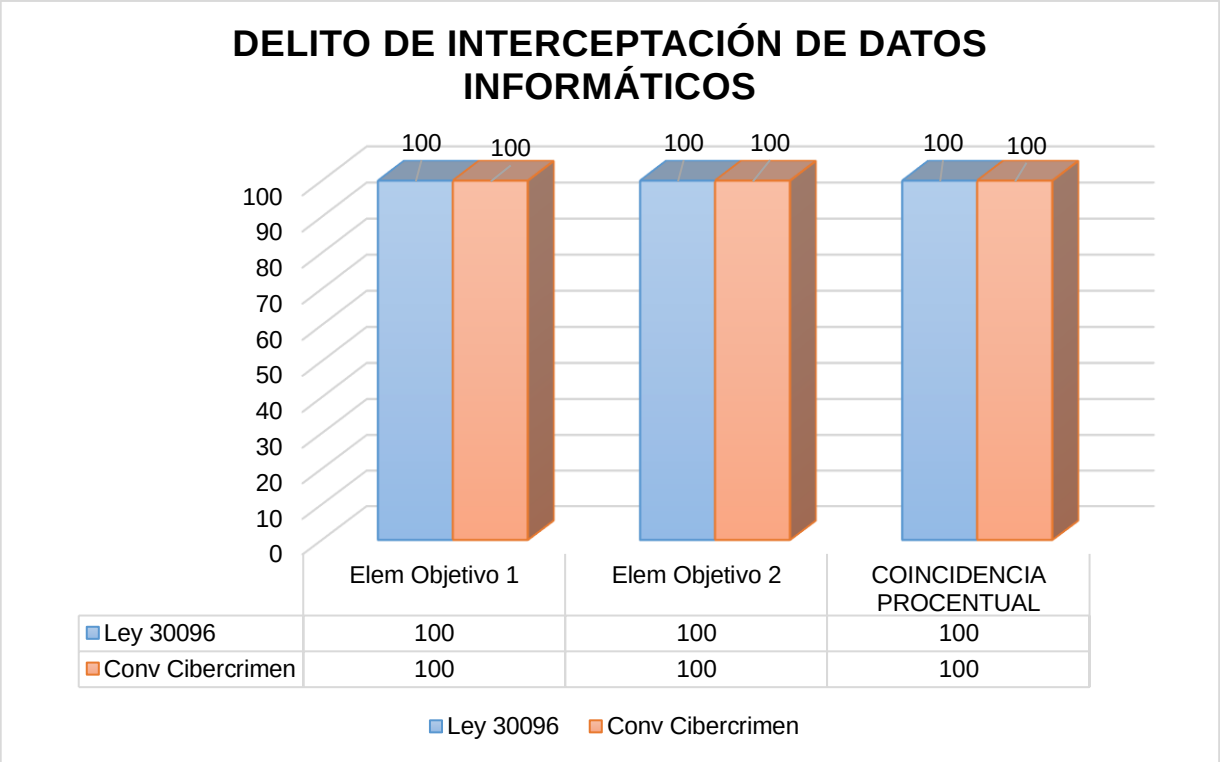
Cuadro 5

COMPARACIÓN ENTRE LA LEY N°30096 LEY DE DELITOS INFORMATICOS Y EL CONVENIO CONTRA EL CIBERCRIMEN RESPECTO AL "DELITO DE INTERCEPTACIÓN DE DATOS INFORMÁTICOS"

DELITOS CONTRA LA CONFIDENCIALIDAD, LA INTEGRIDAD Y LA DISPONIBILIDAD DE LOS DATOS Y SISTEMAS INFORMÁTICOS.	ELEMENTOS OBJETIVOS	LEY 30096 – DE DELITOS INFORMATICOS "INTERCEPTACION DE DATOS INFORMATICOS "	CONVENIO CIBERCRIMEN "INTERCEPTACION ILICITA"	TOTAL
	1er elemento objetivo	Interceptar Datos Informáticos	Interceptación deliberada e ilegítima por medios técnicos de datos informáticos en transmisiones no públicas dirigidas a un sistema informático.	SI 100%
	2do elemento objetivo	Interceptar las emisiones electromagnéticas que transportan estos datos en las transmisiones privadas.	Interceptación deliberada e ilegítima por medios técnicos de datos informáticos emisiones electromagnéticas provenientes de un sistema informático que transporte dichos datos informáticos.	SI 100%
TOTAL DE COINCIDENCIA PORCENTUAL				**100%**

Fuente: Base de Datos del Autor

Gráfico 5



Fuente: Cuadro N° 5

En la Tabla N° 5 y el Gráfico N° 5 se presenta al delito de Interceptación de Datos Informáticos, el que se encuentra conformado por dos elementos objetivos, de los cuales los dos se repiten en la Convención contra el Cibercrimen, teniendo 100% de coincidencia en cada uno, lo que nos da un porcentaje total de coincidencia de 66.66%.

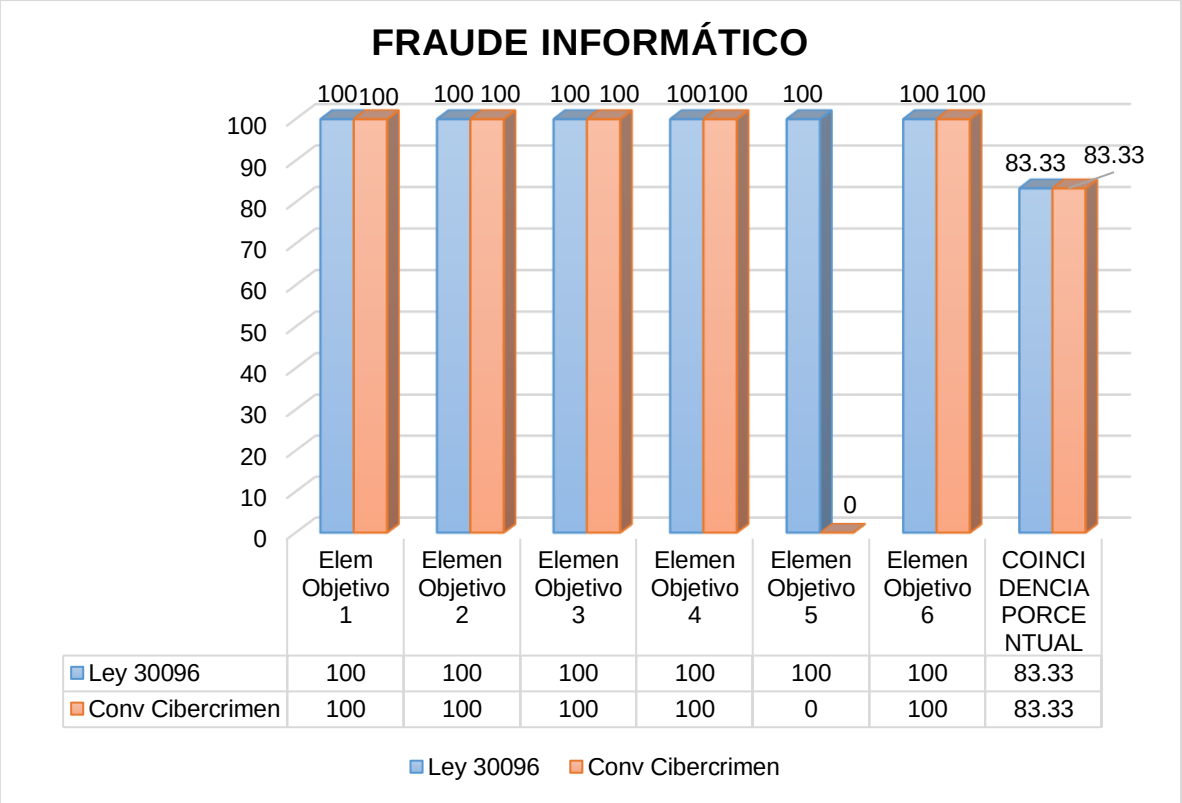
Cuadro 6

COMPARACIÓN ENTRE LA LEY N°30096 LEY DE DELITOS INFORMATICOS Y EL CONVENIO CONTRA EL CIBERCRIMEN RESPECTO AL "DELITO DE FRAUDE INFORMÁTICO"

DELITOS INFORMÁTICOS	ELEMENTOS OBJETIVOS	LEY 30096 – DE DELITOS INFORMATICOS "FRAUDE INFORMÁTICO"	CONVENIO CIBERCRIMEN "FRAUDE INFORMÁTICO"	TOTAL
	1er elemento objetivo	Introduce datos informáticos.	Introducción de datos informáticos	SI 100%
	2do elemento objetivo	Altera datos informáticos.	Alteración de datos informáticos	SI 100%
	3er elemento objetivo	Borra datos informáticos.	Borrado de datos informáticos	SI 100%
	4to elemento objetivo	Suprime datos informáticos.	Supresión de datos informáticos	SI 100%
	5to elemento objetivo	Clona datos informáticos		NO 0%
	6to elemento objetivo	Cualquier interferencia o manipulación en el funcionamiento de un sistema informático.	Interferencia en el funcionamiento de un sistema informático, con la intención fraudulenta o delictiva de obtener ilegítimamente un beneficio económico para uno mismo o para otra persona.	SI 100%
TOTAL DE COINCIDENCIA PORCENTUAL				**83,33%**

Fuente: Base de Datos del Autor

Gráfico 6



Fuente: Cuadro N° 6

En la Tabla N° 6 y el Gráfico N° 6 se presenta al delito de Fraude Informático, el que se encuentra conformado por seis elementos objetivos, de los cuales cinco se repiten en la Convención contra el Cibercrimen, teniendo 100% de coincidencia en cada uno, y en el quinto elemento objetivo no se repite, con 0% de coincidencia, lo que nos da un porcentaje total de coincidencia de 83.33%.

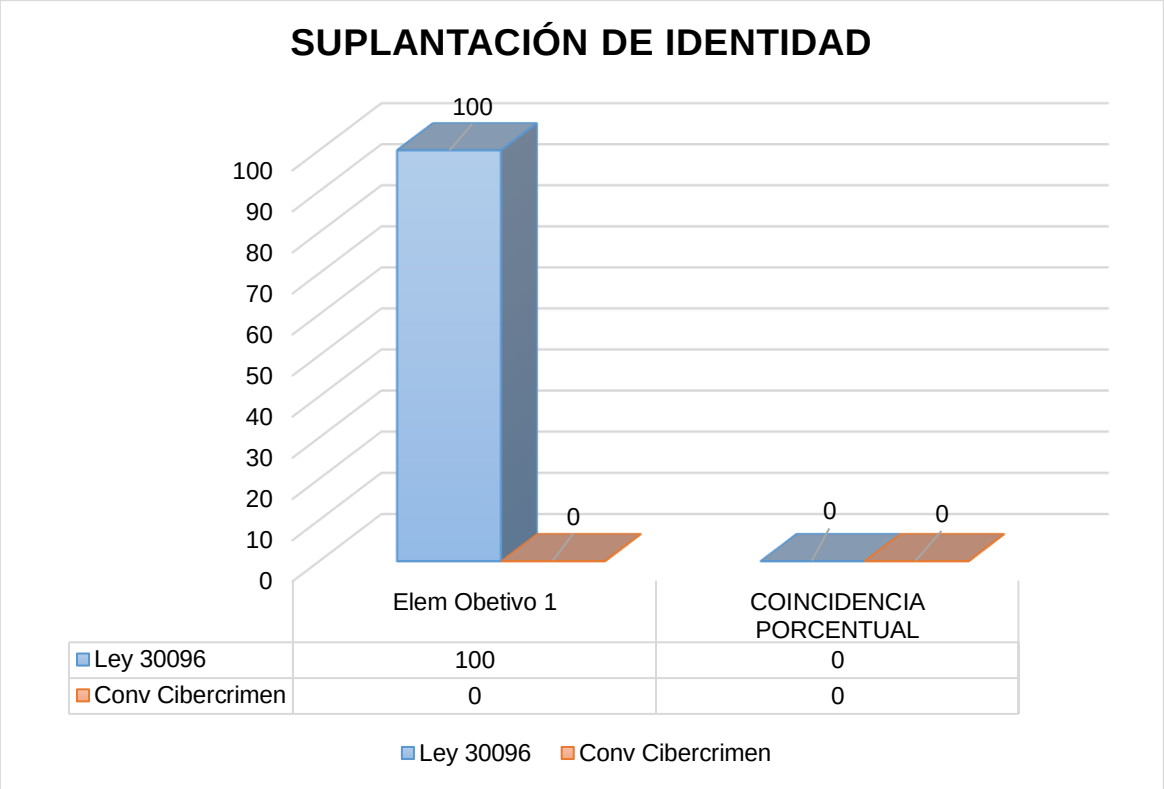
Cuadro 7

COMPARACIÓN ENTRE LA LEY N°30096 LEY DE DELITOS INFORMATICOS Y EL CONVENIO CONTRA EL CIBERCRIMEN RESPECTO AL "DELITO DE SUPLANTACIÓN DE IDENTIDAD"

DELITOS INFORMÁTICOS CONTRA LA FE PÚBLICA	ELEMENTOS OBJETIVOS	LEY 30096 – DE DELITOS "SUPLANTACIÓN DE IDENTIDAD"	CONVENIO CIBERCRIMEN "SUPLANTACIÓN DE IDENTIDAD"	TOTAL
	1er elemento objetivo	Suplantar la identidad de una persona natural o jurídica, siempre que de dicha conducta resulte algún perjuicio.		NO 0%
TOTAL DE COINCIDENCIA PORCENTUAL				**00%**

Fuente: Base de Datos del Autor

Gráfico 7



Fuente: Cuadro N° 7

En la Tabla N° 7 y el Gráfico N° 7 se presenta al delito de Suplantación de Identidad, el que se encuentra conformado por seis elementos objetivos, de los cuales no se repiten en la Convención contra el Cibercrimen, teniendo 00% de coincidencia en cada uno, lo que nos da un porcentaje total de coincidencia de 00.00%.

Cuadro 8

COMPARACIÓN ENTRE LA LEY N°30096 LEY DE DELITOS INFORMATICOS Y EL CONVENIO CONTRA EL CIBERCRIMEN RESPECTO AL "DELITO DE ABUSO DE MECANISMOS Y DISPOSITIVOS INFORMÁTICOS"

DELITOS CONTRA LA CONFIDENCIALIDAD, LA INTEGRIDAD Y LA DISPONIBILIDAD DE LOS DATOS Y SISTEMAS INFORMÁTICOS.	ELEMENTOS OBJETIVOS	LEY 30096 – DE DELITOS "ABUSO DE MECANISMOS Y DISPOSITIVOS INFORMÁTICOS"	CONVENIO CIBERCRIMEN "ABUSO DE LOS DISPOSITIVOS"	TOTAL
	1er elemento objetivo	Fabrica uno o más mecanismos, programas informáticos, dispositivos, contraseñas, códigos de acceso o cualquier otro dato informático, específicamente diseñados para la comisión de los delitos previstos en la presente Ley,	Producción, para su utilización, importación, difusión u otra forma de puesta a disposición de un dispositivo, incluido un programa informático, diseñado o adaptado principalmente una contraseña, un código de acceso o datos informáticos similares que permitan tener acceso a la totalidad o a una parte de un sistema informático, con el fin de que sean utilizados para la comisión de cualquiera de	SI 100%

			los delitos contemplados en los artículos 2 a 5.	
	2do elemento objetivo	Diseña uno o más mecanismos, programas informáticos, dispositivos, contraseñas, códigos de acceso o cualquier otro dato informático, específicamente diseñados para la comisión de los delitos previstos en la presente Ley,		NO 0%
	3er elemento objetivo	Desarrolla uno o más mecanismos, programas informáticos, dispositivos, contraseñas, códigos de acceso o cualquier otro dato informático, específicamente diseñados para la comisión de los delitos previstos en la presente Ley,		NO 0%
	4to elemento objetivo	Vende uno o más mecanismos, programas informáticos,	Venta, para su utilización, importación, difusión u otra forma de	SI 100%

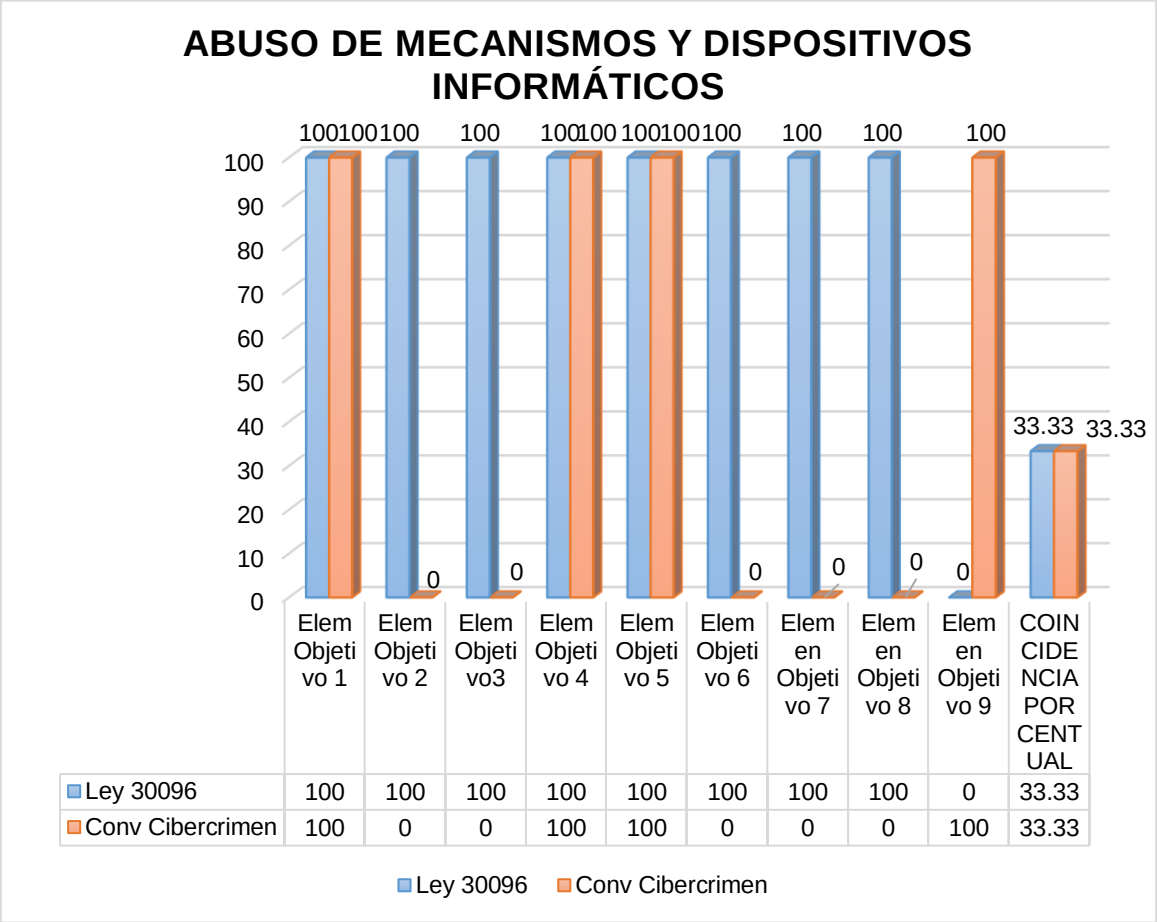
		dispositivos, contraseñas, códigos de acceso o cualquier otro dato informático, específicamente diseñados para la comisión de los delitos previstos en la presente Ley,	puesta a disposición de un dispositivo, incluido un programa informático, diseñado o adaptado principalmente una contraseña, un código de acceso o datos informáticos similares que permitan tener acceso a la totalidad o a una parte de un sistema informático, con el fin de que sean utilizados para la comisión de cualquiera de los delitos contemplados en los artículos 2 a 5.	
	5to Elemento Objetivo	Facilita uno o más mecanismos, programas informáticos, dispositivos, contraseñas, códigos de acceso o cualquier otro dato informático, específicamente diseñados para la comisión de los delitos	Obtención para su utilización, importación, difusión u otra forma de puesta a disposición de un dispositivo, incluido un programa informático, diseñado o adaptado principalmente	SI 100%

		previstos en la presente Ley,	una contraseña, un código de acceso o datos informáticos similares que permitan tener acceso a la totalidad o a una parte de un sistema informático, con el fin de que sean utilizados para la comisión de cualquiera de los delitos contemplados en los artículos 2 a 5.	
	6to Elemento Objetivo	Distribuye uno o más mecanismos, programas informáticos, dispositivos, contraseñas, códigos de acceso o cualquier otro dato informático, específicamente diseñados para la comisión de los delitos previstos en la presente Ley,		NO 0%
	7mo Elemento Objetivo	Importa u obtiene para su utilización, uno o más mecanismos,		NO 0%

		programas informáticos, dispositivos, contraseñas, códigos de acceso o cualquier otro dato informático, específicamente diseñados para la comisión de los delitos previstos en la presente Ley.		
	8vo Elemento Objetivo	Ofrece o presta servicio que contribuya a ese propósito.		NO 0%
	9no Elemento Objetivo		Posesión de alguno de los elementos contemplados en los anteriores apartados anteriores con el fin de que sean utilizados para cometer cualquiera de los delitos previstos en los artículos 2 a 5.	NO 0%
TOTAL DE COINCIDENCIA PORCENTUAL				**33,33%**

Fuente: Base de Datos del Autor

Gráfico 8



Fuente: Cuadro N° 8

En la Tabla N° 8 y el Gráfico N° 8 se presenta al delito de Abuso de Mecanismos y Dispositivos Informáticos, el que se encuentra conformado por nueve elementos objetivos, de los cuales tres se repiten en la Convención contra el Cibercrimen, teniendo 100% de coincidencia en cada uno, y el segundo, tercero, sexto, séptimo, octavo y noveno elemento objetivo no se repite, con 00% de coincidencia, lo que nos da un porcentaje total de coincidencia de 33.33%.

Cuadro 9

COMPARACIÓN ENTRE LA LEY N°30096 LEY DE DELITOS INFORMATICOS Y EL CONVENIO CONTRA EL CIBERCRIMEN RESPECTO AL "DELITO DE PORNOGRAFÍA INFANTIL"

	ELEMENTOS OBJETIVOS	CODIGO PENAL "PORNOGRAFIA INFANTIL"	CONVENIO CIBERCRIMEN "DELITOS RELACIONADOS CON LA PORNOGRAFÍA INFANTIL"	TOTAL
DELITOS RELACIONADOS CON EL CONTENIDO	1er elemento objetivo	Posee por cualquier medio objetos, libros, escritos, imágenes, videos o audios, o realiza espectáculos en vivo de carácter sexual, en los cuales participen menores de dieciocho años de edad	Posesión de pornografía infantil en un sistema informático o en un medio de almacenamiento de datos informáticos	SI 100%
	2do elemento objetivo	Promueve por cualquier medio objetos, libros, escritos, imágenes, videos o audios, o realiza espectáculos en vivo de carácter sexual, en los cuales participen menores de dieciocho años de edad		NO 0%
	3er elemento objetivo	Fabrica por cualquier medio objetos, libros, escritos, imágenes, videos o audios, o realiza espectáculos en	Producción de pornografía infantil con vistas a su difusión por medio de un sistema informático.	SI 100%

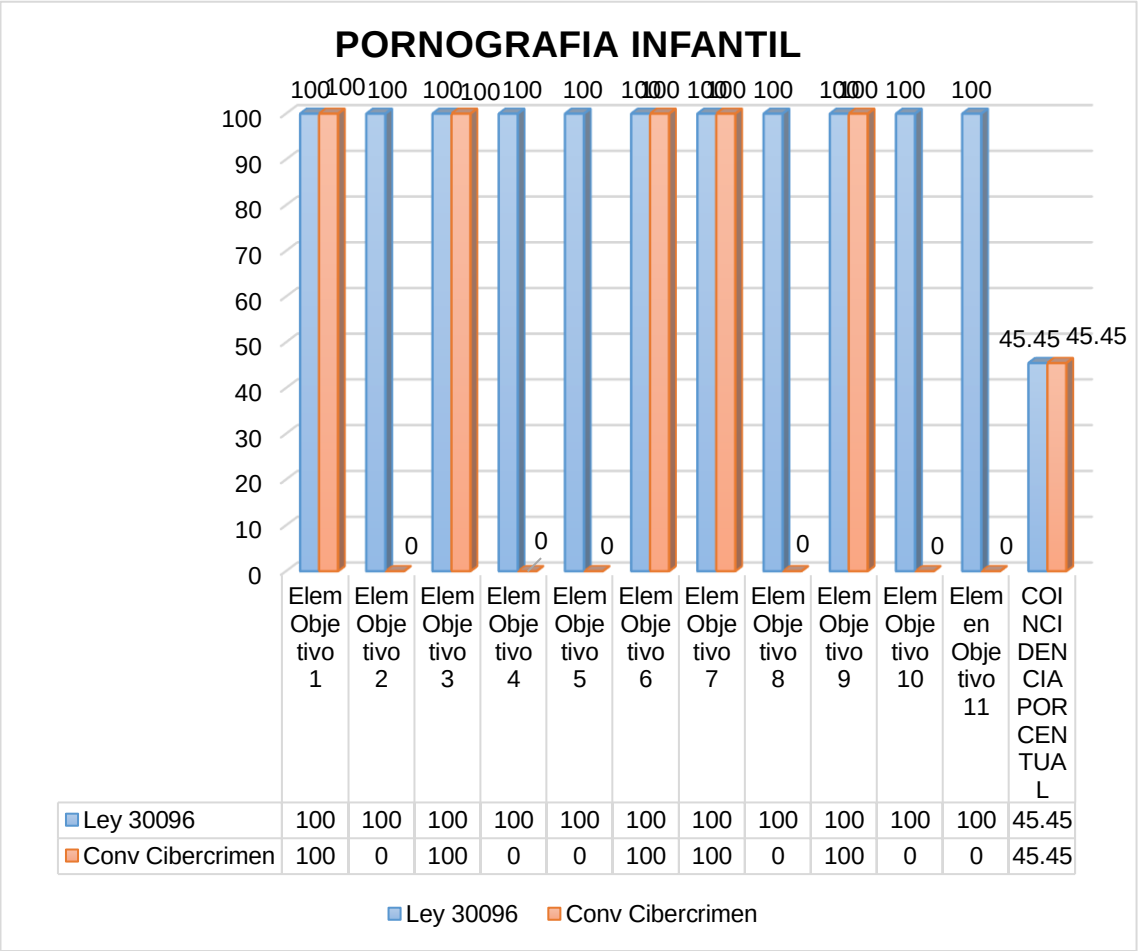
		vivo de carácter sexual, en los cuales participen menores de dieciocho años de edad		
	4to elemento objetivo	Distribuye por cualquier medio objetos, libros, escritos, imágenes, videos o audios, o realiza espectáculos en vivo de carácter sexual, en los cuales participen menores de dieciocho años de edad		NO 0%
	5to elemento objetivo	Exhibe por cualquier medio objetos, libros, escritos, imágenes, videos o audios, o realiza espectáculos en vivo de carácter sexual, en los cuales participen menores de dieciocho años de edad		NO 0%
	6to elemento objetivo	Ofrece por cualquier medio objetos, libros, escritos, imágenes, videos o audios, o realiza espectáculos en vivo de carácter sexual, en los cuales participen menores de dieciocho años de edad	Oferta o la puesta a disposición de pornografía infantil por medio de un sistema informático;	SI 100%

	7mo elemento objetivo	Comercializa por cualquier medio objetos, libros, escritos, imágenes, videos o audios, o realiza espectáculos en vivo de carácter sexual, en los cuales participen menores de dieciocho años de edad	Adquisición de pornografía infantil por medio de un sistema informático para uno mismo o para otra persona.	SI 100%
	8vo elemento objetivo	Publicita por cualquier medio objetos, libros, escritos, imágenes, videos o audios, o realiza espectáculos en vivo de carácter sexual, en los cuales participen menores de dieciocho años de edad		NO 0%
	9no elemento objetivo	Publica por cualquier medio objetos, libros, escritos, imágenes, videos o audios, o realiza espectáculos en vivo de carácter sexual, en los cuales participen menores de dieciocho años de edad	Difusión o transmisión de pornografía infantil por medio de un sistema informático.	SI 100%
	10mo elemento objetivo	Importa por cualquier medio objetos, libros, escritos, imágenes, videos o audios, o realiza espectáculos en		NO 0%

		vivo de carácter sexual, en los cuales participen menores de dieciocho años de edad		
	11vo elemento objetivo	Exporta por cualquier medio objetos, libros, escritos, imágenes, videos o audios, o realiza espectáculos en vivo de carácter sexual, en los cuales participen menores de dieciocho años de edad.		NO 0%
TOTAL DE COINCIDENCIA PORCENTUAL				**45,45%**

Fuente: Base de Datos del Autor

Gráfico 9



Fuente: Cuadro N° 9

En la Tabla N° 9 y el Gráfico N° 9 se presenta al delito de Pornografía Infantil, el que se encuentra conformado por once elementos objetivos, de los cuales cinco se repiten en la Convención contra el Cibercrimen, teniendo 100% de coincidencia en cada uno, y el segundo, cuarto, quinto, octavo, decimo y onceavo elemento objetivo no se repiten, con 0% de coincidencia, lo que nos da un porcentaje total de coincidencia de 45.45%.

Cuadro 10

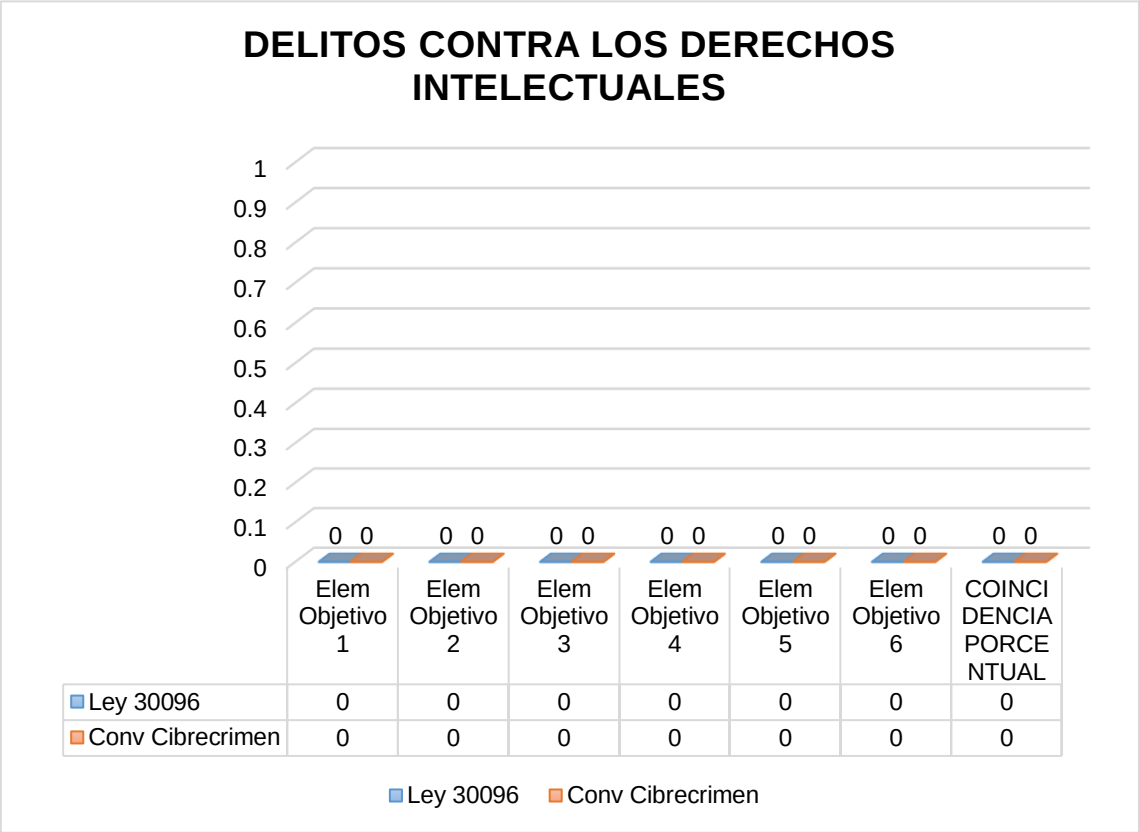
COMPARACIÓN ENTRE LA LEY N°30096 LEY DE DELITOS INFORMATICOS Y EL CONVENIO CONTRA EL CIBERCRIMEN RESPECTO AL "DELITO CONTRA LOS DERECHOS INTELECTUALES"

DELITOS RELACIONADOS CON INFRACCIONES DE LA PROPIEDAD INTELECTUAL Y DE LOS DERECHOS AFINES	ELEMENTOS OBJETIVOS	CODIGO PENAL "DELITOS CONTRA LOS DERECHOS INTELECTUALES"	CONVENIO CIBERCRIMEN "DELITOS RELACIONADOS CON INFRACCIONES DE LA PROPIEDAD INTELECTUAL Y DE LOS DERECHOS AFINES"	TOTAL
	1er elemento objetivo	No mencione en los ejemplares el nombre del autor o traductor;		NO 0%
	2do elemento objetivo	Estampe el nombre con adiciones o supresiones que afecten la reputación del autor como tal ;		NO 0%
	3er elemento objetivo	Publique la obra con abreviaturas ,adiciones o supresiones sin el consentimiento del titular ;		NO 0%
	4to elemento objetivo	Publique separadamente varias obras, cuando la autorización se haya conferido para publicarlas en conjunto, cuando solamente se le haya		NO 0%

		autorizado la publicación de ellas por separado.		
	5to elemento objetivo		Protección de las obras literarias y artísticas, del Acuerdo sobre los aspectos de los derechos de propiedad intelectual relacionados con el comercio sobre la propiedad intelectual, cuando esos actos se cometan deliberadamente, a escala comercial y por medio de un sistema informático.	NO 0%
	6to elemento objetivo		Protección de los artistas intérpretes o ejecutantes, los productores de fonogramas y los organismos de radiodifusión sobre las obras de los intérpretes y ejecutantes y los fonogramas, cuando esos actos se cometan deliberadamente, a escala comercial y por medio de un sistema informático.	NO 0%
TOTAL DE COINCIDENCIA PORCENTUAL				**00%**

Fuente: Base de Datos del Autor

Gráfico 10



Fuente: Cuadro N° 10

En la Tabla N° 10 y el Gráfico N° 10 se presenta al delito Contra los Derechos Intelectuales, el que se encuentra conformado por seis elementos objetivos, de los cuales no se repiten en la Convención contra el Cibercrimen ni en la Ley 30096 de Delitos informáticos, teniendo 00% de coincidencia en cada uno, lo que nos da un porcentaje total de coincidencia de 00.00%.

Cuadro 11

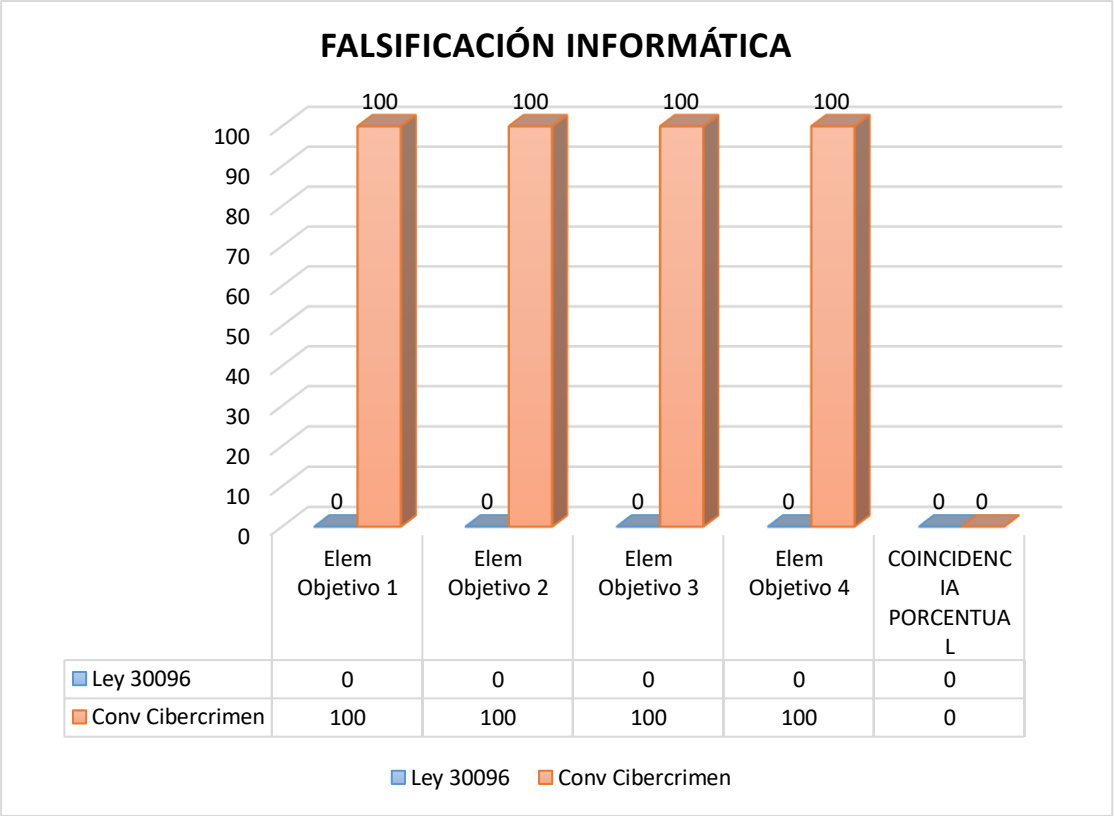
COMPARACIÓN ENTRE LA LEY N°30096 LEY DE DELITOS INFORMATICOS Y EL CONVENIO CONTRA EL CIBERCRIMEN RESPECTO AL "DELITO DE FALSIFICACIÓN INFORMÁTICA"

DELITOS INFORMÁTICOS	ELEMENTOS OBJETIVOS	LEY 30096 – DE DELITOS "FALSIFICACIÓN INFORMATICA"	CONVENIO CIBERCRIMEN "FALSIFICACIÓN INFORMATICA"	TOTAL
	1er elemento objetivo		. Introducción 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,	NO 0%
	2do elemento objetivo		Alteración 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,	NO 0%
	3er elemento objetivo		Borrado 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,	NO 0%
	4to elemento objetivo		Supresión de datos informáticos que dé lugar a datos no	NO 0%

			auténticos, con la intención de que sean tenidos en cuenta o utilizados a efectos legales como si se tratara de datos auténticos.	
TOTAL DE COINCIDENCIA PORCENTUAL				**00%**

Fuente: Base de Datos del Autor

Gráfico 11



Fuente: Cuadro N° 11

En la Tabla N° 11 y el Gráfico N° 11 se presenta el delito de Falsificación Informática, el que se encuentra conformado por cuatro elementos objetivos, de los cuales no se repiten en la Convención contra el Cibercrimen, teniendo 00% de coincidencia en cada uno, lo que nos da un porcentaje total de coincidencia de 00.00%.

CAPITULO V
DISCUSIÓN DE RESUTADOS

En cuanto al delito de Acceso Ilícito, conforme a los resultados de la Tabla y Gráfico 1, hallamos un 66.6% de coincidencia, sin embargo los aspectos en que no existe coincidencia es debido que la Ley de Delitos Informáticos incluye elementos objetivos adicionales que los propuestos en la convención, el 100% de los elementos objetivos considerados en la convención están incluidos en la tipificación de la Ley de Delitos Informáticos. Nuestro resultado coincide con lo señalado por Villavicencio que dice: “Por la característica que presenta este tipo penal -acceso ilícito- se le puede calificar como un delito de mera actividad, porque esta figura exige el acto de acceder (entrar en un lugar o pasar a él) sin autorización a un sistema informático, vulnerar (transgredir, quebrantar, violar una ley o precepto) las medidas de seguridad, de esta manera se configura el ilícito; por tanto el delito queda consumado en el momento que se vulnera las medidas de seguridad establecida para impedir el acceso ilícito, y para ellos es necesario que se realice esta conducta con dolo”. (Villavicencio, 2015, p. 292).

Respecto al delito de Atentado contra la integridad de datos informáticos conforme a los resultados de la Tabla y Grafico 2, hallamos un 71.42% de coincidencia, sin embargo los aspectos en que no existe coincidencia es debido que la Ley de Delitos Informáticos incluye elementos objetivos adicionales que los propuestos en la convención, el 100% de los elementos objetivos considerados en la convención están incluidos en la tipificación de la Ley de Delitos Informáticos. Nuestro resultado coincide con lo señalado por Villavicencio que sostiene: “Por la característica que presenta este tipo penal - atentado a la integridad de los datos informáticos - es clasificado como un delito de mera actividad, porque esta figura exige el solo cumplimiento del tipo penal, la sola realización de la conducta de introducir, borrar, deteriorar, alterar, suprimir y hacer inaccesible los datos informáticos para que se pueda configurar el ilícito, sin importar el resultado posterior. Por tanto el delito queda consumado al realizarse cualquiera de estos actos”. (Villavicencio, 2015, p. 292).

En lo referente al delito de Atentado contra la integridad de sistemas informáticos conforme a los resultados de la Tabla y Grafico 3, hallamos un 57.14% de coincidencia, haciendo necesario modificar su tipificación del Art 4° de la Ley de Delitos Informáticos, pues la misma no incluye la totalidad de elementos objetivos que propone la Convención. Nuestro resultado coincide con lo señalado por Villavicencio que sostiene: “Por la característica que presenta este tipo penal (atentado contra la integridad de sistemas informáticos) se clasifica como un delito de resultado, porque para la configuración de este ilícito

no basta con cumplir el tipo que es (inutilizar o perturbar), sino además es necesario que la acción vaya seguido de un resultado (impedir el acceso, imposibilitar su funcionamiento, o la prestación de sus servicios). Por tanto, el delito se consuma cuando se impide el acceso, se imposibilita el funcionamiento, etcétera; del sistema informático, caso contrario el hecho solo dará lugar a la tentativa". (Villavicencio, 2015, p. 293).

En cuanto al delito de Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos (Grooming) conforme a los resultados de la Tabla y Grafico 4, hallamos un 00% de coincidencia, no haciendo necesario modificar su tipificación del Art 5° de la Ley de Delitos Informáticos, pues el mismo no ha sido considerado en la convención en razón que en el año 2001, que se formula aun no existía esta figura delictiva. Nuestro resultado coincide con lo señalado por Villavicencio que sostiene: "Por estas características se clasifica a esta figura como un delito de resultado cortado, porque en este ilícito el agente persigue un resultado que está más allá del tipo y que ha de producirse por sí solo, sin su intervención y con posterioridad. En esta figura penal el legislador adelanta las barreras de punibilidad al sancionar el solo hecho de contactar con el menor de edad, sin importar si logra su objetivo el que es obtener material pornográfico o llegar a obtener acceso sexual; sin embargo, este articulo tiene muchas falencias que podría violar el principio de legalidad, al no tener una redacción clara, y a consecuencia de ello se podría sancionar a personas que sólo contactan con un menor de edad sin tener la finalidad de obtener material pornográfico y otro similar porque el término contactar no está delimitado, por consiguiente se estaría sancionando el solo hecho de establecer un contacto o comunicación con un menor de edad". (Villavicencio, 2015, p. 295).

Respecto al delito de Interceptación de Datos Informáticos conforme a los resultados de la Tabla y Grafico 5, hallamos un 100% de coincidencia, no haciendo necesario modificar su tipificación del Art 7° de la Ley de Delitos Informáticos, pues la misma incluye la totalidad de elementos objetivos que propone la Convención, el 100% de los elementos objetivos considerados en la convención están incluidos en la tipificación de la Ley de Delitos Informáticos. Nuestro resultado coincide con lo señalado por Villavicencio que sostiene: "Este tipo penal -interceptar datos informáticos - es un delito de peligro abstracto y por ende, sólo basta con demostrar la interceptación de datos informáticos para que el delito quede consumado. Por ende, se trata de un delito de mera actividad porque basta con el solo hecho de interceptar datos informáticos para que se consuma el delito. (Villavicencio, 2015, p. 296)

En cuanto al delito de Fraude Informático conforme a los resultados de la Tabla y Grafico 6, hallamos un 83.33% de coincidencia, no haciendo necesario modificar su tipificación del Art 8° de la Ley de Delitos Informáticos, pues la misma incluye la totalidad de elementos objetivos que propone la Convención. Nuestro resultado coincide con lo señalado por Villavicencio que manifiesta: "Este tipo penal - fraude informático - se clasifica como un delito de resultado porque no basta cumplir con el tipo penal para que se consuma el delito de fraude informático, sino que además, es necesario que esa acción vaya seguida de un resultado separado de la misma conducta el que consiste en causar un perjuicio a tercero, de otro modo el delito quedaría en tentativa". (Villavicencio, 2015, p. 297)

Respecto al delito de Suplantación de Identidad conforme a los resultados de la Tabla y Grafico 7, hallamos un 00% de coincidencia, sin embargo los aspectos en que no existe coincidencia es debido que la Ley de Delitos Informáticos incluye elementos objetivos adicionales que los propuestos en la convención. Nuestro resultado coincide con lo señalado por Villavicencio que sostiene: "Esta figura penal -suplantación de identidad- se clasifica como un delito de resultado porque no basta con realizar la conducta típica el cual es suplantar la identidad, sino que además es necesario que esa acción vaya seguida de un resultado separado de la misma conducta el cual es causar un perjuicio. (Villavicencio, 2015, p. 298).

Respecto al Delito de Abuso de Mecanismos y Dispositivos Informáticos conforme a los resultados de la Tabla y Grafico 8, hallamos un 33.33% de coincidencia, sin embargo los aspectos en que no existe coincidencia es debido que la Ley de Delitos Informáticos incluye elementos objetivos adicionales que los propuestos en la convención. Nuestro resultado coincide con lo señalado por Villavicencio que sostiene: "Este tipo penal - abuso de mecanismos y dispositivos informáticos - se clasifica como un delito de mera actividad, porque la figura exige cumplir con la conducta descrita en el tipo penal para la consumación del delito sin importar el resultado posterior. Aquí, el legislador adelanta las barreras de punibilidad al sancionar el solo hecho de fabricar, diseñar, vender, etcétera; mecanismos y programas orientados a cometer diversos delitos previstos en la ley. Esta figura penal es una construcción cercana a la idea del llamado derecho penal del enemigo porque se sanciona actos preparatorios alegando la puesta en peligro de la seguridad informática. (Villavicencio, 2015, p. 298)

En lo referente al delito de Pornografía Infantil conforme a los resultados de la Tabla y Grafico 9, hallamos un 45.45% de coincidencia, sin embargo los aspectos en que no existe coincidencia es debido que la Ley de Delitos

Informáticos incluye elementos objetivos adicionales que los propuestos en la convención. Nuestro resultado coincide con lo señalado por Villavicencio que sostiene: “Este delito se consuma con la sola proposición, a un menor de edad con fines sexuales, ya sea para obtener material pornográfico o para acceder sexualmente, esta conducta es sancionable porque afecta la indemnidad del menor y la libertad sexual y el medio utilizado para facilitar el contacto es la informática. En esta conducta tipificada se nota la intención del legislador de proteger penalmente varios bienes jurídicos, cuya titularidad corresponde a menores de edad, cuales son los adecuados procesos de formación y socialización de unos y otros, y su intimidad”. (Villavicencio, 2015, p. 295).

Respecto a los delitos contra la propiedad intelectual conforme a los resultados de la Tabla y Grafico 10, hallamos un 00% de coincidencia, si bien hallamos un 00% de coincidencia no consideramos necesario modificar la tipificación de los artículos 216 al 225° del Código Penal Peruano pues los mismos incluyen elementos objetivos adicionales que los propuestos en la convención. Nuestro resultado refleja que la Convención de Cibercrimen establece los elementos objetivos de manera general basándose en las obligaciones asumidas en aplicación del Acta de París de 24 de julio de 1971 por la que se revisó el Convenio de Berna para la protección de las obras literarias y artísticas y en aplicación de la Convención Internacional sobre la protección de los artistas intérpretes o ejecutantes, los productores de fonogramas y los organismos de radiodifusión (Convención de Roma), del Acuerdo sobre los aspectos de los derechos de propiedad intelectual relacionados con el comercio y del Tratado de la OMPI sobre las obras de los intérpretes y ejecutantes y los fonogramas, a excepción de cualquier derecho moral otorgado por dichos Convenios.

Finalmente, respecto al delito de Falsificación Informática conforme a los resultados de la Tabla y Grafico 11, hallamos un 0% de coincidencia, haciendo necesario implementar su regulación debido a que no se encuentra tipificado ni en el Código Penal ni en la Ley de Delitos Informáticos. Nuestro resultado coincide con lo señalado por Villanueva que sostiene: “La Falsificación Informática debe ser considerada como un tipo penal especial y dejar a la Falsificación documentaria como un tipo penal base, al momento de ser regulada, ello en atención a la naturaleza del objeto material del delito. Sin embargo, a efecto de evitar cualquier tipo de impunidad, bien podría aplicarse la falsificación que señala el artículo 427 del Código Penal cuando, de la comisión de un hecho ilícito se advierta el empleo de un medio electrónico, en atención a lo que señala el Código Procesal Penal y la Ley de Firmas y Certificados

Digitales". (Villanueva, F (2012). Boletín Legal de derecho penal informático. Cybercrimen. P 05-06)

CONCLUSIONES

Primero.- En la Presente Investigación se ha podido determinar que el Convenio contra el Cibercrimen de Budapest, ratificado por el Perú el año 2019 con Resolución Legislativa N° 30913, modifica la tipificación del delito de "Atentado contra la integridad de sistemas informáticos", previsto en el artículo 4° de la Ley N° 30096 de Delitos Informáticos e incorpora el delito de Falsificación Informática, que no ha sido previsto ni en la Ley de Delitos Informáticos, ni en el Código Penal.

Segundo.- De nuestros resultados y discusión, encontramos que respecto al delito de "Atentado contra la integridad de sistemas informáticos", previsto en el Art. 4° de la Ley N° 30096 y en el Art. 5° del Convenio, existe únicamente un 57% de similitud, debiendo agregarse en nuestra legislación, los elementos objetivos señalados en el Convenio, modificándose su tipificación en ese sentido. Asimismo, en el Capítulo referido a delitos contra la fe pública de la Ley de Delitos Informáticos, debe incluirse el delito de Falsificación Informática, en cumplimiento al compromiso realizado por nuestro país al ratificar el Convenio contra el Cibercrimen de Budapest.

Tercero.- De nuestros resultados y discusión, encontramos que en el Código Penal Peruano se ha podido evidenciar que los delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines, así como el delito de Pornografía Infantil se encuentran debidamente tipificados en nuestro ordenamiento Jurídico, por haber asumido la totalidad (100%) de los elementos objetivos que contempla el Convenio, y agregado otros más, motivo por el cual no es necesario modificar la tipificación contenida en el Código Penal.

RECOMENDACIONES

PRIMERA.- Que la Universidad Científica del Perú difunda el conocimiento del Convenio contra el Cibercrimen de Budapest entre los estudiantes de derecho y otras facultades, a través de conferencias, seminarios u otras actividades que van a permitir a todas las personas mantenerse al tanto de las nuevas tendencias en su campo profesional, profundizar más los conocimientos en nuestros ordenamientos jurídicos y mecanismos de cooperación que de ellos deriven, ya que es más que imprescindible en esta era globalizada, donde todo está en constante cambio y renovación.

SEGUNDA.- Que la Universidad Científica del Perú gestione la modificación de la Ley N° 30096 Ley de Delitos Informáticos, a fin de que se modifique el delito de "Atentado contra la integridad de sistemas informáticos", y se incorpore el delito de Falsificación Informática en la Ley 30096 de Delitos Informáticos, con la finalidad de rediseñar la política criminal en materia informática, y esto traiga como consecuencia la aplicación de sanción punitiva a quienes cometan delitos informáticos.

TERCERA.- Se gestione como propuesta de modificación de la Ley de Delitos Informáticos, a los proyectos siguientes:

PROYECTO DE LEY N°1
EXPOSICIÓN DE MOTIVOS

a) La evolución de las tecnologías de la información

De acuerdo a la presente investigación que hemos realizado se ha podido evidenciar que el delito de Falsificación Informática ha sido tipificado en el Convenio sobre la Ciberdelincuencia de Budapest, pero en nuestro ordenamiento jurídico no se encuentra tipificado dicho delito, haciéndolo impune frente a actos delictivos que pudieran cometer los ciberdelincuentes.

Actualmente, miles de personas utilizan el Internet para su comunicación, operaciones económicas, consultas de información hasta compra en plataformas virtuales, es decir, está presente en todos los ámbitos de nuestra vida cotidiana y ha transformad en una herramienta con la que desarrollamos nuestras actividades sociales, políticas y económicas.

Este desarrollo de las tecnologías de información y comunicación (TIC) junto al uso de Internet en diversos sectores de la sociedad se configuran como el escenario perfecto para aquellos que buscan un beneficio perjudicando a otras personas, a través del anonimato. Por ello, la creciente demanda de Internet,

resulta un campo fértil para la delincuencia, que ha encontrado nuevas formas para consumar delitos a través de medios electrónicos y tecnológicos, los cuales son aprovechados para afectar a la ciudadanía, las empresas y el gobierno, lo que hace de imperiosa necesidad la modificación de nuestro actual ordenamiento jurídico.

Esta evolución de la era tecnológica ha promovido que el desarrollo de diversas sociedades la incluyan en sus actividades cotidianas, empresas, así como gobiernos tienen acceso a información a través de la disponibilidad del Internet, lo que la configura en una herramienta fundamental hoy en día. Dicha libertad que brindan los espacios cibernéticos, los cuales se desarrollan con rapidez, hacen que los usuarios sean desprotegidos ante el surgimiento de nuevos delitos que necesitan ser tipificados, como es el caso de la Falsificación Informática.

b) Sustento Normativo de la Iniciativa

Actualmente, en nuestro país existe un vacío legal en cuanto a una regulación jurídica del delito de Falsificación Informática, lo que genera que los casos queden impunes, al no ser denunciados por las víctimas porque no existe un marco legal en el cual se puedan amparar.

A pesar de estar vigente la Ley Nº 30096, Ley de Delitos Informáticos, de fecha 22 de octubre del 2013, existe una falta de regulación en el Capítulo 6 en cuanto a Delitos informáticos contra la fe pública.

Vivimos en una era tecnológica que día a día tiene impacto en nuestra sociedad, en la cual el uso de la comunicación electrónica está siendo utilizado para realizar actos ilícitos, convirtiéndose en un problema social.

c) Concepto de Falsificación Informática.

Para definir la falsificación informática tenemos que delimitar el concepto de falsificación, el cual se configura a través de una serie de comportamientos ofensivos que puede originarse desde la introducción de datos no auténticos hasta la supresión de datos no auténticos con el objeto de que los datos sean tomados en cuenta como si fueran auténticos.

De acuerdo a la definición citada en el párrafo anterior se puede determinar que el delito de Falsificación Informática esto es, la introducción, alteración, borrado o supresión 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, con independencia de que los datos sean o no directamente legibles o inteligibles.

d) Presupuesto para la Configuración del Delito de Falsificación Informática

Para que se configure el acoso virtual deben de concurrir los siguientes elementos:

1) Introducción 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,

2) Alteración 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.

3) Borrado 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.

4) Supresión 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.

ANÁLISIS COSTO BENEFICIO

La presente iniciativa legislativa no genera gastos económicos para el tesoro público nacional.

IMPACTO EN LA LEGISLACIÓN

La presente iniciativa legislativa no contraviene ninguna norma de carácter constitucional, ni genera afectación expresa sobre la legislación nacional vigente, más bien responde a la necesidad de establecer un mecanismo de solución eficaz que tenga por objeto la disminución de los delitos informáticos.

De ser aprobada la presente iniciativa empezará a regir desde el día siguiente de su publicación en el diario oficial.

FORMULA LEGISLATIVA.

LEY QUE INCORPORA EL DELITO DE FALSIFICACIÓN INFORMÁTICA EN LA LEY Nº 30096, LEY DE DELITOS INFORMÁTICOS.

ARTICULO 1°: Objeto de la Ley

El objeto de la presente Ley es incorporar el delito de Falsificación Informática en el art 9-A de la Ley Nº 30096, Ley de Delitos Informáticos y de esta manera prevenir aquellas conductas que están dirigidas a dañar a otra persona a través de medios tecnológicos.

ARTICULO 2°: Incorporación del Art. a la Ley de Delitos Informáticos

Incorpórese el art.9-A a la Ley de Delitos Informáticos, el cual quedará redactado de la siguiente manera:

Art.9°-A: ***"El que, a través de la utilización de cualquier sistema informático*** **o** ***cualquier medio de comunicación*** **o** ***tecnología de transmisión de datos, de manera pública o privada, sistemática en el tiempo, introduce, altera, borra o suprime 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, será reprimido con pena privativa de la libertad no menor de uno ni mayor de cinco años.***

PROYECTO DE LEY N°2
EXPOSICIÓN DE MOTIVOS

El presente proyecto de ley propone modificar el Art 4° de la Ley 30096 Ley de Delitos Informáticos con la finalidad de incluir nuevos verbos rectores con la finalidad de perfeccionar nuestro ordenamiento jurídico y como resultado de ello va a cooperar a que nuestros operadores de justicia puedan aplicar de manera eficaz nuestra norma condenando dichos actos delictivos y no crear impunidad dentro de nuestra nación.

Actualmente, los delitos informáticos que pueden ser considerados como crímenes electrónicos, tan graves que pueden llegar a ser un genérico problema para el avance de la informática. La criminalidad informática tiene un alcance mayor y puede incluir delitos tradicionales como el fraude, el robo, chantaje, falsificación y la malversación de caudales públicos en los cuales ordenadores y redes han sido utilizados como medio. Con el desarrollo de la programación y de Internet, los delitos informáticos se han vuelto más frecuentes y sofisticados.

Los delitos informáticos se han venido desarrollando con el avance de la tecnología y esto hace mucho más complejo poder llegar con los responsable, tanto en estados unidos como en otros de países estos han tenido mucho más auge, teniendo un impacto en los ciudadanos, afectándolos ya sea económicamente trayendo consigo responsabilidades enormes en cuanto se refiere a deudas con las instituciones, pero no solo así muchos de ellas también han tenido que liderar con la crítica social porque algunas intimidades han sido reveladas. Existen actividades delictivas que se realizan por medio de estructuras electrónicas que van ligadas a un sin número de herramientas delictivas que buscan infringir y dañar todo lo que encuentren en el ámbito informático.

Este desarrollo de las tecnologías de información y comunicación (TIC) junto al uso de Internet en diversos sectores de la sociedad se configuran como el escenario perfecto para aquellos que buscan un beneficio perjudicando a otras personas, a través del anonimato. Esta evolución de la era tecnológica ha promovido que el desarrollo de diversas sociedades la incluyan en sus actividades cotidianas, empresas, así como gobiernos tienen acceso a información a través de la disponibilidad del Internet, lo que la configura en una herramienta fundamental hoy en día. Dicha libertad que brindan los espacios cibernéticos, los cuales se desarrollan con rapidez, hacen que los usuarios sean desprotegidos ante el surgimiento de nuevas conductas delictuales que necesitan ser tipificados, como es el presente caso.

ANÁLISIS COSTO BENEFICIO

La presente iniciativa legislativa no genera gastos económicos para el tesoro público nacional.

IMPACTO EN LA LEGISLACIÓN

La presente iniciativa legislativa no contraviene ninguna norma de carácter constitucional, ni genera afectación expresa sobre la legislación nacional vigente, más bien guarda absoluta coherencia con lo previsto en los numerales 6. 8. 10 del Art 2° de la Constitución Política del Perú así como también con el Convenio sobre la Ciberdelincuencia de Budapest.

De ser aprobada la presente iniciativa empezara a regir desde el día siguiente de su publicación en el diario oficial.

FORMULA LEGISLATIVA.

LEY QUE MODIFICA EL DELITO DE ATENTADO CONTRA LA INTEGRIDAD DE SISTEMAS INFORMATICOS EN LA LEY Nº 30096, LEY DE DELITOS INFORMÁTICOS.

ARTICULO 1°: Objeto de la Ley

El objeto de la presente Ley es modificar el delito de Atentado Contra la Integridad de Sistemas Informáticos tipificado en el art 4° de la Ley Nº 30096, Ley de Delitos Informáticos con la finalidad de garantizar la lucha eficaz contra la ciberdelincuencia.

ARTICULO 2°: Modificación del Art. a la Ley de Delitos Informáticos

Modifíquese el art. 4° de la Ley N° 30096 “Ley de Delitos Informáticos”, el cual quedará redactado de la siguiente manera:

Art. 4°: ***" El que deliberada e ilegítimamente inutiliza, introduce, borra o, altera, 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."***

CAPITULO VI

BIBLOGRAFIA

REFERENCIAS BIBLIOGRÁFICAS

ALZAMORA DE LOS GODOS, L., CALDERÓN, J. y DEL AGUILA, E. (2009) Guía de Elaboración de Proyectos de Tesis Doctoral. Lima: Universidad Alas Peruanas – Vicerrectorado de Investigación y Postgrado.

ARIAS, J., ARISTIZÁBAL, C. (2011). El dato, la información, el conocimiento y su productividad en empresas del sector público de Medellín. Semestre Económico. Colombia.

ARMANDO, Á. M. (2008). La Problemática Jurídica en la Regulación de los Delitos Informáticos. México.

CALLEGARI, N. (1985). Delitos Informáticos y Legislación. Revista de la Facultad de Derecho y Ciencias Políticas. España

CLARKE, R. & KNAKE (2011). Guerra en la red, los nuevos campos de batalla. Barcelona. Editorial Planeta.

FLORES SALGADO, L. (2014). Derecho Informático. México: Gripo Editorial Patria.

GARCÍA, F., JELDRES, A., MARDONES, M. (2007). Conducta del consumidor y Piratería en la Industria Musical Tesis. Universidad de Chile. Santiago de Chile.

GAVAGNIN TAFFAREL, Osvaldo. (2009). La Creación del Conocimiento. Plan y Elaboración de una Tesis de Post Grado. Lima: Editorial Unión.

GONZÁLES HURTADO, Jorge Alexandre. (2013) Delitos Informáticos: Daños informáticos del artículo 264 del código penal y propuesta de reforma. Tesis. Madrid.

GUERRA VALDIVIA, Alicia Rubí. (2011) Delitos Informáticos-Caso de estudio. Tesis. México.

HERNÁNDEZ, R. (2014) Metodología de la Investigación. México: Editorial McGraw-Hill/Interamericana Editores. Sexta Edición.

HIDALGO ÁVILA, Cesar Raúl. (2011) Delincuentes Modernos en la Ciudad de la Oroya: En Delitos Informáticos. Tesis. Oroya - Perú.

MEHAN, J. (2014). CyberWar, CyberTerror, CyberCrime and CyberActivism, 2nd Edition. Londres. IT Governance Publishing.

NOVAK, F., GARCÍA-CORROCHANO, L. (2003). Derecho Internacional Público. Tomo I: Introducción y fuentes. Lima. Thomson Reuters.

REYES SÁNCHEZ, Yuridia & FERNANDEZ ARAMBURO, Ever. (2009) Proyecto de Investigación: Delitos Informáticos. Durango.

RUMICHE PAZO, José Alfonso. (2015) Sombras de la Normatividad que regula el incremento de la ciberdelincuencia en Lima. Tesis. Huacho-Perú. 2015.

SÁNCHEZ CASTILLO, ZULAY NAYIV (2017). Análisis de la Ley 1273 de 2009 y la evolución de la Ley con relación a los delitos Informáticos en Colombia. Tesis. Colombia.

VILLAVICENCIO TERREROS, Felipe. (2014) Delitos Informáticos en La Ley 30096 y La Modificación de la Ley 30071. Lima – Perú.

WEBGRAFÍA

Falsificación. (2014). Recuperado el 24 de octubre de 2018 de http://www.enciclopediajuridica.biz14.com/d/falsificaci%C3%B3n/falsificaci%C3%B3n.htm

GARNICA, C. (2011). Reservas y declaraciones interpretativas de los tratados internacionales. Recuperado de http://cijfldm.blogspot.com/2011/11/reservasy- declaraciones.html

ITU. (2014). Comprensión del Ciberdelito: Fenómenos, Dificultades y Respuesta Jurídica. Recuperado de https://www.itu.int/en/ITUD/Cybersecurity/Documents/Cybercrime2014_S.pdf

MARTÍNEZ, L., LEYVA, M., FÉLIX, L., CECENAS, P., ONTIVEROS, V. (2014). Recuperado de http://www.upd.edu.mx/PDF/Libros/Ciberespacio.pdf

PEÑA, D. (2014). Aproximación criminógena: delitos informáticos contra la indemnidad y libertades sexuales Ley Nº 30096. Disponible en: https://www.uigv.edu.pe/fileadmin/facultades/derecho/Archivos/ARTICULOS_DOCENTES/ARTICULO_DELITOS_INFORMATICOS_INDEMNIDAD_SEXUAL_2014.pdf

PUELLES, R. (S/F) Documento de trabajo: Luces y sombras en la lucha contra la delincuencia informática en el Perú. Disponible en: http://bit.ly/1m1tnRGRed Peruana Contra la Pornografía Infantil. Disponible en: http://www.seguroseninternet.org/es/grooming.html

REAL ACADEMIA ESPAÑOLA (2016) Diccionario del Español Jurídico de la Real Academia Española. Disponible en: http://dej.rae.es/#/entry-id/E152500

REAL ACADEMIA ESPAÑOLA (2017) Diccionario de la Lengua Española. Disponible en: http://dle.rae.es/

SARACHAGA, A. (2017). Privacidad desde una perspectiva internacional: Introducción. Recuperado de https://blogs.deusto.es/masterinformatica/privacidad-introduccion/

ONU. (s.f.). Declaraciones y Reservas de la Convención de Viena sobre el Derecho de los Tratados. Recuperado de https://treaties.un.org/pages/ViewDetailsIII.aspx?src=TREATY&mtdsg_no=X XIII-1&chapter=23&Temp=mtdsg3&clang=_en#EndDec

SISTEMA PERUANO DE INFORMACION JURIDICA http://spijlibre.minjus.gob.pe/normativa_libre/main.asp

VILLANUEVA, F (2012). Cybercrimen. En el Boletín Legal de derecho penal informático. Recuperado http://www.iriartelaw.com/sites/default/files/boletin-cybercrimen-noviembre-2012.pd

CAPITULO VII

ANEXOS

MATRIZ DE CONSISTENCIA

ANEXO N° 1

TITULO: "Innovaciones en la Tipificación de Delitos con la Ratificación del Convenio contra el Cibercrimen, en el Perú el año 2019".

PROBLEMA	OBJETIVOS	HIPÓTESIS	VARIABLES	INDICADORES	METODOLOGÍA
Problema General ¿Cuáles son las modificaciones en la tipificación de delitos que incorpora el Convenio contra el cibercrimen de Budapest en Perú el año 2019? **Problemas Específicos** • ¿Cuáles son las modificaciones en la Ley de Delitos Informáticos que incorpora el Convenio contra el cibercrimen de Budapest en Perú el año 2019? • ¿Cuáles son las modificaciones en el Código Penal que incorpora el	**Objetivo General** Determinar las modificaciones en la tipificación de delitos que incorpora el Convenio contra el cibercrimen de Budapest en Perú el año 2019. **Objetivos Específicos** • Establecer las modificaciones en la Ley de Delitos Informáticos que incorpora el Convenio contra el cibercrimen de Budapest en Perú el año 2019.	Las modificaciones en la tipificación de delitos que incorpora el Convenio contra el cibercrimen de Budapest el año 2019, se producen en la Ley de Delitos	**Variable** Convenio contra el cibercrimen de Budapest. **Dimensiones** • Ley de Delitos Informáticos • Código Penal	• Modificaciones en el Delito de Acceso Ilícito. • Modificaciones en el Delito de Atentado contra la Integridad de datos informáticos. • Modificaciones en el Delito de Atentado contra la Integridad de sistemas informáticos.	**Tipo y Nivel de Investigación:** Básica Descriptiva **Método:** Teórico Inductivo **Diseño de la Investigación:** No experimental – Transversal **Población y Muestra:** La población es finita, al estar compuesta por el estudio de la tipificación de delitos por medios informáticos en tres documentos legales que

Convenio contra el cibercrimen de Budapest en Perú el año 2019?	• Identificar las modificaciones en el Código Penal que incorpora el Convenio contra el cibercrimen de Budapest en Perú el año 2019.	Informáticos y en el Código Penal.		• Modificaciones en el Delito de Grooming • Modificaciones en el Delito de Interceptación de Datos Informáticos. • Modificaciones en el Delito de Fraude Informático. • Modificaciones en el Delito de Pornografía Infantil. • Modificaciones en los Delitos contra la propiedad intelectual. • Modificaciones en los Delitos contra la fe pública.	son la Convención contra el Cibercrimen de Budapest, la Ley de Delitos Informáticos y el Código Penal. **Recolección de Datos** Como Instrumento de investigación se ha utilizado la Ficha de Registro de Datos

Anexo N° 2

CUADRO SEGÚN LEY DE DELITOS INFORMÁTICOS

LEY DE DELITOS INFORMATICOS	BIEN JURÍDICO PROTEGIDO	ELEMENTOS OBJETIVOS	ELEMENTOS SUBJETIVOS	AGRAVANTES
ACCESO ILÍCITO	La confidencialidad, la integridad, y la disponibilidad de los datos y sistemas informáticos.	- Acceso a todo o en parte de un sistema informático. -Vulneración de medidas de seguridad establecidas para impedir el acceso. -Exceso que sobrepasa los límites de la autorización de acceso.	Dolo	1. El agente comete el delito en calidad de integrante de una organización criminal. 2. El agente comete el delito mediante el abuso de una posición especial de acceso a la data o información reservada o al conocimiento de esta información en razón del ejercicio de un cargo o función. 3. El agente comete el delito con el fin de obtener un beneficio económico, salvo en los delitos que prevén dicha circunstancia.

				4. El delito compromete fines asistenciales, la defensa, la seguridad y la soberanía nacionales.
ATENTADO A LA INTEGRIDAD DE DATOS INFORMÁTICOS.	La confidencialidad, la integridad, y la disponibilidad de los datos informáticos.	- Dañar datos informáticos. - Borrar datos informáticos. - Deteriorar datos informáticos. - Alterar datos informáticos. - Suprimir datos informáticos. -Hacer inaccesibles datos informáticos. - Introducir datos informáticos.	Dolo	1. El agente comete el delito en calidad de integrante de una organización criminal. 2. El agente comete el delito mediante el abuso de una posición especial de acceso a la data o información reservada o al conocimiento de esta información en razón del ejercicio de un cargo o función. 3. El agente comete el delito con el fin de obtener un beneficio económico, salvo en los delitos que prevén dicha circunstancia. 4. El delito compromete fines asistenciales, la defensa, la

				seguridad y la soberanía nacionales.
ATENTADO A LA INTEGRIDAD DE SISTEMAS.	La confidencialidad, la integridad, y la disponibilidad de los sistemas informáticos.	- inutiliza, total o parcialmente, un sistema informático, - Impide el acceso a este. - Entorpece su funcionamiento o la prestación de sus servicios. - Imposibilita su funcionamiento o la prestación de sus servicios.	Dolo	1. El agente comete el delito en calidad de integrante de una organización criminal. 2. El agente comete el delito mediante el abuso de una posición especial de acceso a la data o información reservada o al conocimiento de esta información en razón del ejercicio de un cargo o función. 3. El agente comete el delito con el fin de obtener un beneficio económico, salvo en los delitos que prevén dicha circunstancia. 4. El delito compromete fines asistenciales, la defensa, la seguridad y la soberanía nacionales.

GROOMING	La indemnidad sexual de los niños menores de 14 años. La libertad sexual de los menores de entre 14 a 18 años	- Contactar con un menor de edad por la internet u otro medio análogo para solicitar material pornográfico o llevar a cabo actividades sexuales.	Dolo	No tiene agravantes, ya que la Ley de Delitos Informáticos no los establece.
INTERCEPTACIÓN DE DATOS INFORMÁTICOS.	La reserva, la intimidad, y confidencialidad de los datos informáticos.	- Interceptar datos informáticos y las emisiones electromagnéticas que transportan estos datos en las transmisiones privadas.	Dolo	1. cuando la interceptación recaiga sobre información clasificada como secreta, reservada o confidencial, de conformidad con la Ley 27806, Ley de Transparencia y Acceso a la información Pública, cuya penalidad oscila entre cinco a ocho años 2. cuando la interceptación recaiga sobre información que compromete a la defensa, seguridad o soberanía nacional, cuya penalidad se encuentra entre ocho a diez años. 3. consiste en la calidad del agente (integrante de una

				organización criminal) que comete delitos cuya penalidad se incrementa hasta en un tercio por encima del máximo legal previsto en los supuestos anteriores.
FRAUDE INFORMÁTICO.	El patrimonio	- Introduce datos informáticos o cualquier interferencia o manipulación en el funcionamiento de un sistema informático. -Altera datos informáticos o cualquier interferencia o manipulación en el funcionamiento de un sistema informático. -Borra datos informáticos o cualquier interferencia o manipulación en el funcionamiento de un sistema informático.	Dolo	Cuando se afecte el patrimonio del estado a fines asistenciales y programas de apoyo social. 1. El agente comete el delito en calidad de integrante de una organización criminal. 2. El agente comete el delito mediante el abuso de una posición especial de acceso a la data o información reservada o al conocimiento de esta información en razón del ejercicio de un cargo o función.

		- Suprime datos informáticos o cualquier interferencia o manipulación en el funcionamiento de un sistema informático. - Clona datos informáticos o cualquier interferencia o manipulación en el funcionamiento de un sistema informático.		3. El agente comete el delito con el fin de obtener un beneficio económico, salvo en los delitos que prevén dicha circunstancia. 4. El delito compromete fines asistenciales, la defensa, la seguridad y la soberanía nacionales.
SUPLANTACIÓN DE IDENTIDAD	Fe pública, la seguridad y fiabilidad del tráfico jurídico y probatorio.	- Suplantar la identidad de una persona natural o jurídica, siempre que de dicha conducta resulte algún perjuicio.	Dolo	1. El agente comete el delito en calidad de integrante de una organización criminal. 2. El agente comete el delito mediante el abuso de una posición especial de acceso a la data o información reservada o al conocimiento de esta información en razón del ejercicio de un cargo o función. 3. El agente comete el delito con el fin de obtener un

				beneficio económico, salvo en los delitos que prevén dicha circunstancia. 4. El delito compromete fines asistenciales, la defensa, la seguridad y la soberanía nacionales.
ABUSO DE MECANISMOS Y DISPOSITIVOS INFORMÁTICOS	La integridad de datos y programas. La privacidad La indemnidad sexual e integridad moral de las personas.	- Fabrica uno o más mecanismos, programas informáticos, dispositivos, contraseñas, códigos de acceso o cualquier otro dato informático, específicamente diseñados para la comisión de los delitos previstos en la presente Ley, - Diseña uno o más mecanismos, programas informáticos, dispositivos, contraseñas, códigos de acceso o cualquier otro dato informático, específicamente diseñados para	Dolo	1. El agente comete el delito en calidad de integrante de una organización criminal. 2. El agente comete el delito mediante el abuso de una posición especial de acceso a la data o información reservada o al conocimiento de esta información en razón del ejercicio de un cargo o función. 3. El agente comete el delito con el fin de obtener un beneficio económico, salvo

		la comisión de los delitos previstos en la presente Ley, - Desarrolla uno o más mecanismos, programas informáticos, dispositivos, contraseñas, códigos de acceso o cualquier otro dato informático, específicamente diseñados para la comisión de los delitos previstos en la presente Ley, - Vende uno o más mecanismos, programas informáticos, dispositivos, contraseñas, códigos de acceso o cualquier otro dato informático, específicamente diseñados para la comisión de los delitos previstos en la presente Ley, - Facilita uno o más mecanismos, programas informáticos, dispositivos, contraseñas, códigos de acceso o cualquier otro dato informático, específicamente diseñados para		en los delitos que prevén dicha circunstancia. 4. El delito compromete fines asistenciales, la defensa, la seguridad y la soberanía nacionales.

		la comisión de los delitos previstos en la presente Ley, - Distribuye uno o más mecanismos, programas informáticos, dispositivos, contraseñas, códigos de acceso o cualquier otro dato informático, específicamente diseñados para la comisión de los delitos previstos en la presente Ley, - Importa u obtiene para su utilización, uno o más mecanismos, programas informáticos, dispositivos, contraseñas, códigos de acceso o cualquier otro dato informático, específicamente diseñados para la comisión de los delitos previstos en la presente Ley. - Ofrece o presta servicio que contribuya a ese propósito.		

Anexo N° 3

CUADRO SEGÚN CÓDIGO PENAL PERUANO

CODIGO PENAL	BIEN JURÍDICO PROTEGIDO	ELEMENTOS OBJETIVOS	ELEMENTOS SUBJETIVOS	AGRAVANTES
PORNOGRAFÍA INFANTIL	La indemnidad sexual de los niños menores de 14 años. La libertad sexual de las personas de 18 años.	- Posee por cualquier medio objetos, libros, escritos, imágenes, videos o audios, o realiza espectáculos en vivo de carácter sexual, en los cuales participen menores de dieciocho años de edad - Promueve por cualquier medio objetos, libros, escritos, imágenes, videos o audios, o realiza espectáculos en vivo de carácter sexual, en los cuales participen menores de dieciocho años de edad - Fabrica por cualquier medio objetos, libros, escritos, imágenes, videos o audios, o realiza	Dolo	- La víctima tenga menos de catorce años de edad. - El material se difunda a través de cualquier tecnología de la información o de la comunicación o cualquier otro medio que genere difusión masiva. - El agente actúe como miembro o integrante de una banda u organización criminal.

		espectáculos en vivo de carácter sexual, en los cuales participen menores de dieciocho años de edad - Distribuye por cualquier medio objetos, libros, escritos, imágenes, videos o audios, o realiza espectáculos en vivo de carácter sexual, en los cuales participen menores de dieciocho años de edad - Exhibe por cualquier medio objetos, libros, escritos, imágenes, videos o audios, o realiza espectáculos en vivo de carácter sexual, en los cuales participen menores de dieciocho años de edad - Ofrece por cualquier medio objetos, libros, escritos, imágenes, videos o audios, o realiza espectáculos en vivo de carácter sexual, en los cuales participen		

		menores de dieciocho años de edad -Comercializa por cualquier medio objetos, libros, escritos, imágenes, videos o audios, o realiza espectáculos en vivo de carácter sexual, en los cuales participen menores de dieciocho años de edad - Publicita por cualquier medio objetos, libros, escritos, imágenes, videos o audios, o realiza espectáculos en vivo de carácter sexual, en los cuales participen menores de dieciocho años de edad - Publica por cualquier medio objetos, libros, escritos, imágenes, videos o audios, o realiza espectáculos en vivo de carácter sexual, en los cuales participen menores de dieciocho años de edad		

		-Importa por cualquier medio objetos, libros, escritos, imágenes, videos o audios, o realiza espectáculos en vivo de carácter sexual, en los cuales participen menores de dieciocho años de edad -Exporta por cualquier medio objetos, libros, escritos, imágenes, videos o audios, o realiza espectáculos en vivo de carácter sexual, en los cuales participen menores de dieciocho años de edad.		
DELITOS RELACIONADOS CON INFRACCIONES DE LA PROPIEDAD INTELECTUAL Y DE LOS DERECHOS AFINES	Derecho de Autor Propiedad Industrial.	**DELITO DE VIOLACIÓN DEL DERECHO DE AUTOR.** -No mencione en los ejemplares el nombre del autor o traductor; -Estampe el nombre con adiciones o supresiones que afecten la reputación del autor como tal ;	Dolo	No tiene agravantes, ya que el Código Penal Peruano no lo establece.

		-Publique la obra con abreviaturas ,adiciones o supresiones sin el consentimiento del titular ; -Publique separadamente varias obras, cuando la autorización se haya conferido para publicarlas en conjunto, cuando solamente se le haya autorizado la publicación de ellas por separado. **DELITO DE REPRODUCCIÓN, DIFUSIÓN, DISTRIBUCIÓN DE LA OBRA SIN AUTORIZACIÓN DEL AUTOR.** -Modifica una obra, una interpretación, etc., sin la autorización del autor. -Distribuya mediante venta, una obra, una interpretación, etc., sin la autorización del autor.		- Se dé a conocer al público una obra inédita o no divulgada, que haya recibido en confianza del titular del derecho de autor o de alguien en su nombre, sin el consentimiento del titular. - La reproducción, distribución o comunicación pública se realiza con fines comerciales u otro tipo de ventaja económica, o alterando o suprimiendo el nombre o seudónimo del autor,

		-Reproduce una obra, una interpretación, etc., sin la autorización del autor.		productor o titular de los derechos." - Conociendo el origen ilícito de la copia o reproducción, la distribuya al público, por cualquier medio, la almacene, oculte, introduzca en el país o la saque de éste. - Se fabrique, ensamble, importe, exporte, modifique, venda, alquile, ofrezca para la venta o alquiler, o ponga de cualquier otra manera en circulación dispositivos, sistemas tangibles o intangibles, esquemas o equipos capaces de soslayar otro dispositivo destinado a impedir o restringir la realización de copias de obras, o a menoscabar la calidad de las copias realizadas, o capaces de permitir o fomentar la recepción de un programa

		DELITO DE PLAGIO. -Difunde una obra como propia copiándola o reproduciéndola textualmente atribuyéndose o atribuyendo a otra la autoría o titularidad ajena.		codificado, radiodifundido o comunicado en otra forma al público, por aquellos que no están autorizados para ello." - Se inscriba en el Registro del Derecho de Autor la obra, interpretación, producción o emisión ajenas, o cualquier otro tipo de bienes intelectuales, como si fueran propios, o como de persona distinta del verdadero titular de los derechos." - Quien se atribuya falsamente la calidad de titular originario o derivado, de cualquiera de los derechos protegidos en la legislación del derecho de autor y derechos conexos y, con esa

				indebida atribución, obtenga que la autoridad competente suspenda el acto de comunicación, reproducción o distribución de la obra, interpretación, producción, emisión o de cualquier otro de los bienes intelectuales protegidos. - Quien realice actividades propias de una entidad de gestión colectiva de derecho de autor o derechos conexos, sin contar con la autorización debida de la autoridad administrativa competente. - El que presente declaraciones falsas en cuanto certificaciones de ingresos; asistencia de público; repertorio utilizado; identificación de los autores; autorización supuestamente obtenida; número de ejemplares producidos,

		DELITO DE USO NO AUTORIZADO DE PRODUCTO. -Utiliza con fines económicos, de cualquier forma, un producto amparado por una patente de invención, modelo de utilidad o diseño industrial. **DELITO DE USO O VENTA NO AUTORIZADA DE DISEÑO INDUSTRIAL.** -Fabrique etiquetas, sellos o envases que contengan marcas registradas; cuando retiren o utilicen etiquetas, sellos o envases que contengan marcas originales para utilizarlos en productos de		vendidos o distribuidos gratuitamente o toda otra adulteración de datos susceptible de causar perjuicio a cualquiera de los titulares del derecho de autor o conexos. - Si el agente que comete el delito integra una organización destinada a perpetrar los ilícitos previstos en el presente capítulo. - Si el agente que comete cualquiera de los delitos previstos en el presente capítulo, posee la calidad de funcionario o servidor público." No tiene agravantes, ya que el Código Penal Peruano no lo establece.

		distinto origen; o cuando envasen y/o comercialicen productos empleando envases identificados con marcas cuya titularidad corresponde a terceros. -Comercialice etiquetas, sellos o envases que contengan marcas registradas; cuando retiren o utilicen etiquetas, sellos o envases que contengan marcas originales para utilizarlos en productos de distinto origen; o cuando envasen y/o comercialicen productos empleando envases identificados con marcas cuya titularidad corresponde a terceros. -Distribuya etiquetas, sellos o envases que contengan marcas registradas; cuando retiren o utilicen etiquetas, sellos o envases que contengan marcas originales para utilizarlos en productos de distinto origen; o cuando envasen y/o comercialicen productos empleando envases identificados		No tiene agravantes, ya que el Código Penal Peruano no lo establece.

		con marcas cuya titularidad corresponde a terceros. -Almacene etiquetas, sellos o envases que contengan marcas registradas; cuando retiren o utilicen etiquetas, sellos o envases que contengan marcas originales para utilizarlos en productos de distinto origen; o cuando envasen y/o comercialicen productos empleando envases identificados con marcas cuya titularidad corresponde a terceros.		

Anexo N° 4

CUADRO SEGÚN CONVENIO CONTRA EL CIBERCRIMEN - BUDAPEST

CONVENIO CONTRA EL CIBERCRIMEN - BUDAPEST	BIEN JURÍDICO PROTEGIDO	ELEMENTOS OBJETIVOS	ELEMENTOS SUBJETIVOS	AGRAVANTES
ACCESO ILÍCITO (ART. 2):	La confidencialidad, la integridad, y la disponibilidad de los datos y sistemas informáticos.	- Acceso deliberado e ilegítimo a un sistema informático. - Acceso deliberado e ilegítimo a un sistema informático. Infringiendo medidas de seguridad, en relación con un sistema informático conectado a otro sistema informático.	Dolo	No tiene agravantes, ya que el Convenio de Budapest (cibercrimen) no lo establece.
	La confidencialidad, la integridad, y la disponibilidad de los datos informáticos.	-interceptación deliberada e ilegítima por medios técnicos de datos informáticos en transmisiones no públicas dirigidas a un sistema	Dolo	No tiene agravantes, ya que el Convenio de Budapest (cibercrimen) no lo establece.

INTERCEPTACIÓN ILÍCITA (ART. 3)		informático, originadas en un sistema informático o efectuadas dentro del mismo, incluidas las emisiones electromagnéticas provenientes de un sistema informático que transporte dichos datos informáticos.		
ATAQUES A LA INTEGRIDAD DE LOS DATOS (ART. 4)	La confidencialidad, la integridad, y la disponibilidad de los datos informáticos.	- Dañe datos informáticos. - Borre datos informáticos. - Deteriore datos informáticos. - Altere datos informáticos. - Suprima datos informáticos.	Dolo	No tiene agravantes, ya que el Convenio de Budapest (cibercrimen) no lo establece.
ATAQUES A LA INTEGRIDAD DEL SISTEMA (ART. 5)	La confidencialidad, la integridad, y la disponibilidad de los sistemas informáticos.	- Introducción datos informáticos que obstaculice el funcionamiento de un sistema informático. - Transmisión datos informáticos que obstaculice el funcionamiento de un sistema informático. - Daño datos informáticos que obstaculice el funcionamiento de un sistema informático.	Dolo	No tiene agravantes, ya que el Convenio de Budapest (cibercrimen) no lo establece.

		- Borrado datos informáticos que obstaculice el funcionamiento de un sistema informático. - Deterioro datos informáticos que obstaculice el funcionamiento de un sistema informático. - Alteración datos informáticos que obstaculice el funcionamiento de un sistema informático. - Supresión de datos informáticos que obstaculice el funcionamiento de un sistema informático.		
ABUSO DE LOS DISPOSITIVOS (ART. 6)	La confidencialidad, la integridad, y la disponibilidad de los datos informáticos.	- Producción de un dispositivo, incluido un programa informático, contraseña, código de acceso o datos informáticos similares que permitan tener acceso a	Dolo	No tiene agravantes, ya que el Convenio de Budapest (cibercrimen) no lo establece.

		la totalidad o a una parte de un sistema informático. - Venta de un dispositivo, incluido un programa informático, contraseña, código de acceso o datos informáticos similares que permitan tener acceso a la totalidad o a una parte de un sistema informático. - Obtención de un dispositivo, incluido un programa informático, contraseña, código de acceso o datos informáticos similares que permitan tener acceso a la totalidad o a una parte de un sistema informático. - Difusión u otra forma de puesta a disposición de un dispositivo, incluido un programa informático, contraseña, código de acceso o datos informáticos similares		

		que permitan tener acceso a la totalidad o a una parte de un sistema informático. - La posesión de alguno de los elementos contemplados en los anteriores apartados (i) o (ii).		
FALSIFICACIÓN INFORMÁTICA (ART. 7):	La reserva, la intimidad, y confidencialidad de los datos y sistemas informáticos.	Introducción 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, Alteración 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, Borrado de datos informáticos que dé lugar a datos no auténticos, con la intención de	Dolo	No tiene agravantes, ya que el Convenio de Budapest (cibercrimen) no lo establece.

		que sean tenidos en cuenta o utilizados a efectos legales como si se tratara de datos auténticos, Supresión 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 (ART. 8):	La confidencialidad, la integridad, y la disponibilidad de los datos informáticos.	-Introducción de datos informáticos -Alteración de datos informáticos -Borrado de datos informáticos -Supresión de datos informáticos -Interferencia en el funcionamiento de un sistema informático, con la intención fraudulenta o delictiva de obtener ilegítimamente un	Dolo	No tiene agravantes, ya que el Convenio de Budapest (cibercrimen) no lo establece.

		beneficio económico para uno mismo o para otra persona.		
DELITOS RELACIONADOS CON LA PORNOGRAFÍA INFANTIL (ART: 9):	La indemnidad sexual de los menores de edad de 16 años. La libertad sexual de las personas de 18 años de edad a más.	-producción de pornografía infantil con vistas a su difusión por medio de un sistema informático; -oferta o la puesta a disposición de pornografía infantil por medio de un sistema informático; -difusión o transmisión de pornografía infantil por medio de un sistema informático -adquisición de pornografía infantil por medio de un sistema informático para uno mismo o para otra persona; -posesión de pornografía infantil en un sistema informático o en un medio de almacenamiento de datos informáticos	Dolo	No tiene agravantes, ya que el Convenio de Budapest (cibercrimen) no lo establece.

DELITOS RELACIONADOS CON INFRACCIONES DE LA PROPIEDAD INTELECTUAL Y DE LOS DERECHOS AFINES (ART. 10):	Derecho de Autor Propiedad Industrial.	- Protección de las obras literarias y artísticas, del Acuerdo sobre los aspectos de los derechos de propiedad intelectual relacionados con el comercio sobre la propiedad intelectual, cuando esos actos se cometan deliberadamente, a escala comercial y por medio de un sistema informático. - Protección de los artistas intérpretes o ejecutantes, los productores de fonogramas y los organismos de radiodifusión sobre las obras de los intérpretes y ejecutantes y los fonogramas, cuando esos actos se cometan deliberadamente, a escala comercial y por medio de un sistema informático.		No tiene agravantes, ya que el Convenio de Budapest (cibercrimen) no lo establece.
