UNIVERSIDAD ANDINA DEL CUSCO

FACULTAD DE DERECHO Y CIENCIA POLÍTICA

ESCUELA PROFESIONAL DE DERECHO

TESIS

"LA INCIDENCIA DE LAS NUEVAS TECNOLOGÍAS EN EL DELITO DE FRAUDE INFORMÁTICO Y SU APLICACIÓN EN LA LEY N° 30096 EN EL PERÚ"

Presentado por

- Luiggi Jesús Cajigas Moreano

0009-0007-5548-710X

- Gonzalo Lizardo Pérez Chirinos

0009-0009-2792-8742

Para optar al Título Profesional de Abogado.

Asesor:

Mgt. Sixto Madison Barreto Jara

0000-0002-1894-1728

Línea de Investigación:

Política Jurisdiccional

Problemas y actualidad de la justicia penal

CUSCO-PERÚ

2023

Metadatos

Datos del autor	
Nombres y apellidos	LUIGGI JESUS CAJIGAS MOREANO
Número de documento de identidad	70584347
URL de Orcid	https://orcid.org/0009-0007-5548-710X
Datos del asesor	
Nombres y apellidos	SIXTO MADISON BARRETO JARA
Número de documento de identidad	23884200
URL de Orcid	https://orcid.org/0000-0002-1894-1728
Datos del jurado	
Presidente del jurado (jurado 1)	
Nombres y apellidos	FERNANDO RIVERO YNFANTAS
Número de documento de identidad	23818798
Jurado 2	
Nombres y apellidos	JUVENAL CERECEDA VÁSQUEZ
Número de documento de identidad	06809463
Jurado 3	
Nombres y apellidos	BORIS GERMAIN MUJICA PAREDES
Número de documento de identidad	23944252
Jurado 4	
Nombres y apellidos	CARLOS EDUARDO JAYO SILVA
Número de documento de identidad	40114932
Datos de la investigación	
Línea de investigación de la Escuela Profesional	POLITICA JURISDICCIONAL PROBLEMAS Y ACTUALIDAD DE LA JUSTICIA PENAL

“LA INCIDENCIA DE LAS NUEVAS TECNOLOGÍAS EN EL DELITO DE FRAUDE INFORMÁTICO Y SU APLICACIÓN EN LA LEY N° 30096 EN EL PERÚ”

por Luiggi Jesús Y Gonzalo Lizardo Cajigas Moreano Y Pérez Chirinos

UNIVERSIDAD ANDINA DEL CUSCO

FACULTAD DE DERECHO Y CIENCIA POLÍTICA

ESCUELA PROFESIONAL DE DERECHO

TESIS

"LA INCIDENCIA DE LAS NUEVAS TECNOLOGÍAS EN EL DELITO DE FRAUDE INFORMÁTICO Y SU APLICACIÓN EN LA LEY N° 30096 EN EL PERÚ"

Presentado por los Bachilleres en Derecho:

- Luiggi Jesús Cajigas Moreano
- Gonzalo Lizardo Pérez Chirinos

Para optar al Título Profesional de Abogado.

Asesor: Mgt. Sixto Madison Barreto Jara

Línea de Investigación:

Política Jurisdiccional

Problemas y actualidad de la justicia penal

CUSCO-PERÚ

2023

Abog. Madison Barreto Jara
CAC 1537

DE FRAUDE INFORMÁTICO Y SU APLICACIÓN EN LA LEY N° 30096 EN EL PERÚ"

INFORME DE ORIGINALIDAD

25%	25%	2%	12%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	hdl.handle.net Fuente de Internet	3%
2	Submitted to Universidad Andina del Cusco Trabajo del estudiante	2%
3	repositorio.pucp.edu.pe Fuente de Internet	2%
4	repositorio.unasam.edu.pe Fuente de Internet	1%
5	Submitted to Universidad Tecnológica Indoamerica Trabajo del estudiante	1%
6	www.unheval.edu.pe Fuente de Internet	1%
7	dspace.ucuenca.edu.ec Fuente de Internet	1%
8	docplayer.es Fuente de Internet	1%

Abog. Madison Barreto Jara
CAC 1537

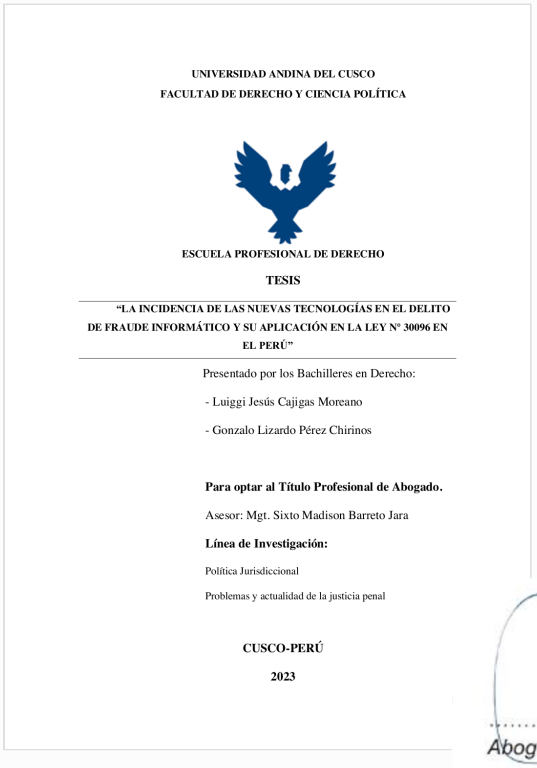
turnitin

Recibo digital

Este recibo confirma quesu trabajo ha sido recibido por Turnitin. A continuación podrá ver la información del recibo con respecto a su entrega.

La primera página de tus entregas se muestra abajo.

Autor de la entrega:	Luiggi Jesús Y Gonzalo Lizardo Cajigas Moreano Y Pérez Chiri...
Título del ejercicio:	"LA INCIDENCIA DE LAS NUEVAS TECNOLOGÍAS EN EL DELITO...
Título de la entrega:	"LA INCIDENCIA DE LAS NUEVAS TECNOLOGÍAS EN EL DELITO...
Nombre del archivo:	TESIS_CAJIGAS_Y_PEREZ.docx
Tamaño del archivo:	774.52K
Total páginas:	76
Total de palabras:	16,586
Total de caracteres:	91,727
Fecha de entrega:	23-jun.-2023 04:48p. m. (UTC-0500)
Identificador de la entre...	2121593473



UNIVERSIDAD ANDINA DEL CUSCO
FACULTAD DE DERECHO Y CIENCIA POLÍTICA

ESCUELA PROFESIONAL DE DERECHO

TESIS

"LA INCIDENCIA DE LAS NUEVAS TECNOLOGÍAS EN EL DELITO DE FRAUDE INFORMÁTICO Y SU APLICACIÓN EN LA LEY N° 30096 EN EL PERÚ"

Presentado por los Bachilleres en Derecho:

- Luiggi Jesús Cajigas Moreano
- Gonzalo Lizardo Pérez Chirinos

Para optar al Título Profesional de Abogado.

Asesor: Mgt. Sixto Madison Barreto Jara

Línea de Investigación:

Política Jurisdiccional

Problemas y actualidad de la justicia penal

CUSCO-PERÚ

2023

Abog. Madison Barreto Jara
CAC 1537

AGRADECIMIENTOS

Agradezco a mi familia por el apoyo e impulso para crecer en mi vida, quienes siempre están en todo momento y a quienes debo mi gratitud y todo mi cariño. Asimismo, agradezco a Milena Oyola, la persona que me demostró un amor y apoyo incondicional, quien siempre estuvo conmigo en la luz y en la oscuridad, gracias por ser mi inspiración. Agradecer a Dios y a la Virgen María por darme la fortaleza en todo el desarrollo de mi vida.

Luiggi Cajigas

Quiero expresar mi gratitud de manera muy especial hacia mi familia, quienes siempre me han brindado su incondicional apoyo, amor y motivación en todo momento. Además, agradezco a mi apreciada enamorada Ingrid Fernández, quien ha estado presente en los momentos difíciles y me ha animado a seguir adelante. Asimismo, deseo manifestar mi agradecimiento a todas las personas que contribuyeron en la investigación de esta tesis, por su tiempo, disposición y colaboración en la recolección de los datos necesarios. Finalmente, quiero agradecer a Dios por brindarme la fuerza y la perseverancia necesarias para concluir este proyecto, y por bendecirme con las oportunidades y herramientas requeridas para llevarlo a cabo.

Gonzalo Perez

DEDICATORIA

Dedico este trabajo a mis padres Ricardo y Milagros que gracias a ellos pude completar este punto importante en mi vida, siempre estaré eternamente agradecido, de igual forma a mis hermanos Kevin y Vanesa, que son mi motivo de superación personal y las personas que me inspiran a seguir creciendo cada día. Asimismo, dedicar a mi abuela Natividad que siempre estuvo orgullosa de mí y hoy siempre la tengo presente, a Milena Alexandra, quien siempre me demuestra su apoyo incondicional y me enseñó que después de la tempestad llega la calma. A ellos, mis mejores sentimientos y dedicatoria.

Luiggi Cajigas

Quiero dedicar estas líneas a mis padres Lizardo y Nicolasa, y también a mi querida hermana Liz Almendra quienes han sido la fuente de mi inspiración y motivación en todo momento. Gracias por inculcarme valores tan importantes como la perseverancia, el esfuerzo y la dedicación, los cuales me han llevado a culminar esta etapa en mi vida. Gracias por brindarme su apoyo incondicional, su amor y por ser mi fuente de fortaleza en los momentos más difíciles. Este logro no habría sido posible sin su constante aliento y confianza en mí. ¡Gracias por todo!

Gonzalo Perez

RESUMEN

En el mundo de hoy, la tecnología avanza a pasos inimaginables, nuevas computadoras, robots, medicina o sistemas cada vez más inteligentes y capaces de simplificarnos la vida, pero tengamos en cuenta que, así como se crean sistemas complejos con mayor capacidad, también a la par se crean sistemas o programas diseñados para el mal, es decir, sistemas utilizados para poder delinquir, robar, extorsionar, coaccionar, atacar, engañar, etc. Es por ello que la población cada vez más se encuentra en constante peligro, en el Perú estas prácticas ya son ejercidas en diferentes plataformas o sistemas, estas prácticas son conocidas en el mundo como Phishing, Vishing, Smishing, entre otras, debemos tener en cuenta que la población peruana es consciente del avance de la tecnología, pero no todos estamos preparados para los fraudes o engaños con los nuevos sistemas o modalidades de fraude informático.

Actualmente ya se registró muchísimas denuncias en nuestro país sobre delitos informáticos, debido a que la tecnología se utiliza de manera abusiva para llevar a cabo actividades ilegales, como la difusión de desinformación, la creación de pánico, experimentos irresponsables, fraudes cibernéticos, acoso en línea y violaciones de los derechos humanos, así mismo como inciden diferentes factores para la comisión de este tipo penal, la exposición imprudente de datos personales en internet y en otras transacciones electrónicas aumenta el riesgo de fraude informático, un problema que se extiende a nivel mundial. En Perú, el fraude informático ha aumentado debido a la necesidad de utilizar medios electrónicos durante la pandemia. Es posible que la legislación peruana sobre delitos informáticos “Ley N° 30096” necesite ser actualizada para adaptarse a los cambios tecnológicos y prevenir actividades ilícitas. Nuestra investigación se centrará en los siguientes problemas: ¿Es posible prevenir actividades ilícitas en el ámbito tecnológico mediante una reforma adecuada de la legislación de delitos informáticos en el Perú?, ¿Es necesario modificar el artículo 8 de la Ley N° 30096 “Ley de Delitos Informáticos” para adaptarlo a las modalidades actuales de fraude informático?, Cuales son los factores que influyen en la comisión de delitos de

fraude informático en la población peruana debido a la aplicación de nuevas tecnologías y su regulación en La Ley N°30096.

Finalmente, la justificación de esta investigación es determinar cómo el aumento de los delitos de fraude informático se relaciona con la evolución de la tecnología a su vez considerando una carente y paupérrima regulación penal de la legislación actual la cual no es adecuada para prevenir y sancionar estas nuevas actividades. Esperando que el presente trabajo contribuya con la comunidad científica jurídica, y sea del agrado del lector.

PALABRAS CLAVE

Fraude informático, ley de delitos informáticos, ciberdelincuencia, ciberseguridad.

ABSTRACT

In today's world, technology advances at unimaginable steps, new computers, robots, medicine or increasingly intelligent systems capable of simplifying our lives, but keep in mind that just as complex systems with greater capacity are created, so too Even systems or programs designed for evil are created, that is, systems used to commit crimes, steal, extort, coerce, attack, deceive, etc. That is why the population is increasingly in constant danger, in Peru these practices are already carried out on different platforms or systems, these practices are known in the world as Phishing, Vishing, Smishing, among others, we must take into account that the Peruvian population is aware of the advancement of technology, but not all of us are prepared for fraud or deception with the new systems or modalities of computer fraud.

Currently, many complaints have already been registered in our country about computer crimes, due to the fact that technology is used abusively to carry out illegal activities, such as the dissemination of disinformation, the creation of panic, irresponsible experiments, cyber fraud, online harassment and violations of human rights, just as different factors affect the commission of this type of crime, the reckless exposure of personal data on the Internet and in other electronic transactions increases the risk of computer fraud, a problem that extends worldwide. In Peru, computer fraud has increased due to the need to use electronic means during the pandemic. It is possible that the Peruvian legislation on computer crimes (Law No. 30096) needs to be updated to adapt to technological changes and prevent illegal activities. Our investigation will focus on the following problems: Is it possible to prevent illegal activities in the technological field through an adequate reform of the cybercrime legislation in Peru? Is it necessary to modify article 8 of Law No. 30096 - Computer Crime Law to adapt it to the current modalities of computer fraud? What are the factors that influence the commission of computer fraud crimes in the Peruvian population due to the application of new technologies and its regulation in Law No. 30096.

Finally, the justification of this investigation is to determine how the increase in computer fraud crimes is related to the evolution of technology, in turn considering a lacking and very poor criminal regulation of current legislation, which is not adequate to prevent and

punish these crimes. new activities. Hoping that this work contributes to the legal scientific community, and is to the reader's liking.

KEY WORDS

Computer fraud, computer crimes law, cybercrime, cybersecurity.

INDICE

CAPÍTULO I

1. INTRODUCCIÓN

1.1 Planteamiento del Problema.

En la segunda década del siglo XXI la tecnología viene desarrollándose a niveles nunca antes calculados, teniendo en cuenta que China viene posicionándose como la nueva potencia mundial gracias a sus masivos avances tecnológicos. Ante los grandes avances tecnológicos de hoy en día podemos afirmar que nuestra vida está condicionada de manera fundamental por la tecnología que nos rodea, aunque de esa forma viene siendo desde los orígenes del hombre teniendo en cuenta que el desarrollo tecnológico logró que el hombre pueda dominar el fuego, suceso que permitió en ese entonces modificar el contexto en que los humanos vivían el día a día, gracias a tal descubrimiento la civilización de ese entonces pudo aprender a cocinar sus alimentos, brindarse calor en temporadas de invierno, incluso se convirtió en la primera fuente de iluminación artificial que descubrieron los seres humanos.

Sin embargo así como surgen nuevas cosas para bien y para el progreso de la humanidad, de igual manera la tecnología se convirtió en un instrumento para obrar el mal, por parte de los humanos; sin apartarnos del tema respecto al desarrollo tecnológico del fuego, se tiene que destacar que existieron los humanos denominados incendiarios, quienes fueron aquellos que usaron el fuego como un arma con la finalidad de causar daños a las personas o incluso a sus propiedades, por lo tanto el origen del mal de la tecnología se remonta desde la Génesis del mismo.

Por lo tanto para ninguna persona es novedad que la tecnología viene evolucionando a niveles exorbitantes, sin embargo su uso aun no logra alcanzar una madurez en la sociedad dado que cada vez se incrementa el mal uso de los medios

tecnológicos, gente inescrupulosa que usa tales medios para desinformar a las demás personas, incluso llegando a generar pánico en la sociedad, igualmente se vienen haciendo experimentos sociales sin un mínimo de empatía por los demás, fraudes cibernéticos, extorsiones informáticas, ciberacoso y muchas más acciones que incluso llegan a configurar como delitos acorde a la normativa nacional, e internacional por la vulneración a los derechos humanos.

Se tiene que tener en cuenta que se incurre en mayor riesgo de ser víctima de fraude informático con la divulgación inescrupulosa de datos personales en internet, redes sociales, compras y transacciones por internet en páginas de internet no cifradas o inseguras, llamadas telefónicas, mensajes de texto. Este problema viene extendiéndose por todo el planeta, Rusia, que es uno de los países con registros de mayor ciber-delincuencia tuvo que incrementar su seguridad informática después de diversos ataques al mismo gobierno, es por ello que en nuestro continente este tema debe tomarse con más seriedad y visión.

Finalmente en el Perú, se ha visto cómo han ido aumentando desmesuradamente la comisión de los delitos de fraude informático, más aún con la necesidad en que se vieron los peruanos de hacer usos de los medios electrónicos para realizar sus actividades diarias ante la presente pandemia generada por el COVID 19, ya iniciada la era tecnológica en nuestro país seguirá su curso de manera imparable, por lo tanto es necesario e importante tener leyes adecuadas y actualizadas a la nueva realidad tecnológica que adopta nuestro país.

Son esas consideraciones que nos motivan a realizar el presente trabajo.

1.2 Formulación del Problema

1.2.1 Problema General

¿Se encuentra adecuada a nuestra realidad tecnológica actual la tipificación del delito de Fraude informático regulado en el artículo 8 de la Ley N° 30096 – Ley de Delitos Informáticos?

1.2.2 Problemas Específicos

1. ¿Se puede prevenir las actuales conductas ilícitas del ámbito tecnológico mediante una adecuada reforma a la legislación de delitos informáticos en el Perú?

2. ¿La Ley N°30096, “Ley de Delitos Informáticos” cuenta con un tratamiento especial acorde al convenio de Budapest?
3. ¿Cuáles son los factores que inciden en la comisión del delito de fraude informático en la población peruana a raíz de la aplicación de las nuevas tecnologías y su regulación en la Ley N° 30096?

1.3 Justificación de la Investigación

1.3.1 Conveniencia

El presente trabajo de investigación es adecuado y conveniente porque con él se podrá determinar de qué manera repercute la evolución de las nuevas tecnologías en el incremento de los delitos de fraude informático, y de la misma manera se apreciará si este delito está siendo aplicado correctamente por la Ley N°30096 “Ley de Delitos Informáticos”, en el presente trabajo somos partidarios de una modificatoria en sentido aclarativo al tipo penal especifico de Fraude Informático, debido a su desactualización e inexactitud con la realidad social.

1.3.2 Relevancia Social

El estudio de este trabajo permitirá ayudar a conocer la gran problemática que viene generando el aumento de los delitos informáticos en la sociedad; a nivel mundial los seres humanos se ven dependientes de la tecnología para realizar sus actividades diarias, trabajos, estudios, negocios, actividades de ocio, etc. A raíz de la pandemia generada por el COVID 19, y centrándonos específicamente en el Perú las quejas y denuncias públicas fueron muchas, sobre todo respecto al delito de fraude informático. Cada vez se incrementan más el número de personas que son víctimas de los ciberdelincuentes que innovan nuevas formas y modalidades para delinquir aprovechando que la actual ley de los delitos informáticos no está ajustada a la coyuntura en que estamos viviendo.

1.3.3 Implicancia Práctica

De igual forma se pretende determinar el rol actual de la Fiscalía en la investigación especializada referente a la ciberdelincuencia, teniendo en cuenta que la Fiscalía de la Nación dispuso la creación de la Red de fiscales en ciberdelincuencia a nivel nacional, que serán los puntos de contacto entre los Distritos Fiscales y la mencionada unidad. Cabe precisar que todos ellos integran la red en adición a las funciones que actualmente vienen desempeñando. Dicha unidad teniendo competencia nacional tiene entre sus objetivos específicos

efectuar la orientación técnico-jurídica en las investigaciones de los delitos cometidos por medios tecnológicos, desde la identificación y preservación de la evidencia digital, el Estado Peruano con la suscripción del Convenio de Budapest, el Ministerio Público dispuso –en diciembre de 2020– la creación de la Unidad Fiscal Especializada en Ciberdelincuencia.

1.3.4 Valor Teórico

En el presente trabajo de investigación se desarrollará el delito del fraude informático y su actual aplicación en la legislación nacional, dicha investigación será un aporte para estudios futuros referentes a los temas de la ciberdelincuencia y la tecnología, no sólo en el ámbito del derecho, sino también para sus ramas afines.

Los efectos adversos que genera el Fraude son diversos, entre los principales que se ha detectado que causa pérdidas de dinero, de información personal de los usuarios, etc. Ante esta grave problemática que de continuar incrementándose desmesuradamente cabe la posibilidad que repercuta dañinamente sobre los usuarios que hacen uso de internet, a razón de que cada vez irán generando emociones que conllevan a la incertidumbre, preocupación, ansiedad y desdicha, dado que no se sentirán seguros al momento de hacer uso de los sitios web de internet destinados para el uso de redes sociales, compras o transacciones de sumas de dinero y todas aquellas actividades que involucren datos personales de los usuarios.

1.3.5 Unidad Metodológica

El presente trabajo será una pauta para otros estudios respecto de este tema, asimismo contribuirá con la evolución y mejoramiento de nuestro ordenamiento jurídico y su correcta imputación a casos futuros.

1.4 Objetivos de la Investigación

1.4.1 Objetivo general

Determinar si se encuentra adecuada a nuestra realidad tecnológica actual la tipificación del delito de Fraude Informático regulado en el artículo 8 de la Ley N° 30096 – Ley de Delitos Informáticos

1.4.2 Objetivos Específicos

1. Señalar sí es posible prevenir las actuales conductas ilícitas del ámbito tecnológico mediante una adecuada reforma a la legislación de delitos informáticos en el Perú.
2. Determinar si, la Ley N°30096, ¿"Ley de Delitos Informáticos" cuenta con un tratamiento acorde al convenio de Budapest
3. Determinar los factores que inciden en la comisión del delito de fraude informático en la población peruana.

1.4.3 Delimitación Espacial

El presente trabajo de investigación se realizó en la ciudad del Cusco, pero se circunscribe al ámbito nacional.

1.4.4 Delimitación Temporal

El presente trabajo de investigación abarca los siguientes periodos: desde julio del año 2021, hasta el mes de febrero del año 2023.

CAPÍTULO II

2. MARCO TEÓRICO

2.1 Antecedentes de estudio

Como antecedentes tenemos:

2.1.1 Antecedentes Internacionales

Antecedente N° 01.

Trabajo de tesis presentada por Carolin Anabel Ruiz Cruz para optar por el título de abogado, en la Universidad Nacional de Loja – Ecuador, año 2016, dicho trabajo tiene el siguiente nombre: *"ANÁLISIS DE LOS DELITOS INFORMÁTICOS Y SU VIOLACIÓN DE LOS DERECHOS CONSTITUCIONALES DE LOS CIUDADANOS"* (Ruiz Cruz, 2016, págs. 93,94).

Las conclusiones principales son:

1. En la actualidad, la necesidad de comunicación de las personas, ha contribuido al avance vertiginoso de las tecnologías de la información y la comunicación, permitiendo con la misma celeridad los delitos informáticos.
2. La falta de conocimientos de las tecnologías de la información y la comunicación, es la causa principal para que profesionales del derecho y magistrados, y los reformadores de la legislación penal en materia informática, para que se haya obviado algunos elementos que deberían incluirse en la legislación ecuatoriana.

Antecedente N°02

El segundo antecedente internacional del presente trabajo, es la tesis de investigación cuyo título es: *"EL FRAUDE COMO DELITO INFORMÁTICO"* trabajo desarrollado por Ana Maribel Chungata Cabrera, presentado ante la

Universidad de Cuenca, para obtener el título de Abogado, Cuenca, Ecuador, año 2015. (Chungata Cabrera, 2015, págs. 70,71),

Las conclusiones del trabajo refieren:

1. La tecnología puede ser utilizada como medio o como fin para el cometimiento de un hecho delictivo, así como medio se utiliza un ordenador para perpetrar el delito, por ejemplo, utilizando una computadora se falsifica documentos. En tanto que, como fin, se establece como blanco del delito el ordenador, los circuitos, colapsar un sistema, etc.
2. A los delitos informáticos les caracteriza por ser considerados de cuello blanco, esto es, que quien comete el mismo no puede ser cualquier persona, tendrá que ser un individuo con cierta preparación o educación en tecnología, informática, sistemas computacionales, etc. Inclusive el perfil criminológico de estos delincuentes.
3. Hoy en día las modalidades de fraude más usuales son el phishing y pharming, que se lo realiza principalmente con miras a obtener información confidencial del usuario por medios fraudulentos como una página web falsa, cuya finalidad es usar dicha información para obtener beneficios económicos a favor del ciberdelincuente.

2.1.2 Antecedentes Nacionales

Antecedente N° 01.

Como primer antecedente de nuestro trabajo de investigación tomaremos de referencia la tesis cuyo título es *"INCONSISTENCIAS Y AMBIGÜEDADES EN LA LEY DE DELITOS INFORMÁTICOS LEY Nº 30096 Y SU MODIFICATORIA LEY Nº 30171, QUE IMPOSIBILITAN SU EFICAZ CUMPLIMIENTO"*. La autora de dicha tesis es Karina Joselin Zorrilla Tocto, tesis que fue presentada en el año 2018, con la finalidad de optar por el título de abogado en la Universidad Nacional De Ancash "Santiago Antúnez De Mayolo", tesis que tiene una de las siguientes conclusiones que consideramos más importantes.

"1. Se evidencia, luego del análisis crítico de la ley de Delitos Informáticos Ley N° 3096 y su modificatoria Ley N° 30171, evidentes artículos que presentan

imprecisiones en su redacción los cuales originan confusión tanto en los operadores de justicia como en los justiciables, ocasionando muchas veces que estos graves delitos no se denuncien o en su defecto que, posterior a ser denunciado, no se pueda hallar a los verdaderos culpables.

2. La superposición de tipos penales a los cuales se hace referencia en la presente tesis, solo demuestra que los legisladores están siguiendo una línea errada al pretender legislar los medios por los cuales se consuma un delito y no regular las CONDUCTAS. Cayendo equivocadamente en pretender regular conductas que ya están propiamente tipificadas en nuestro Código Penal." (Zorrila Tocto, 2018, pág. 97).

Antecedente N° 02.

Como segundo antecedente tenemos el trabajo de investigación realizado por Elías Gilberto Chávez Rodríguez, tesis de título "*EL DELITO CONTRA DATOS Y SISTEMAS INFORMÁTICOS EN EL DERECHO FUNDAMENTAL A LA INTIMIDAD PERSONAL EN LA CORTE SUPERIOR DE JUSTICIA DE LIMA NORTE, 2017"*, tesis que fue presentada el año 2018, para optar el grado académico de Doctor en Derecho, en la Universidad Nacional Federico Villareal, teniendo como conclusión más relevante para nuestro tema de investigación, el siguiente:

"Primera. Es oportuno señalar que el Estado a través del poder judicial brinde capacitaciones constantes a los operadores del derecho de la Corte Superior de Justicia de Lima Norte en relación a los principios generales de protección de la información pública y privada (información sensible, de control, limitación a la información personal, a la verdad actualizada, seguridad personal, indemnización civil), esto con la finalidad de garantizar la protección de los derechos fundamentales a la intimidad personal y familiar por actos ilícitos cometidos utilizando la informática" (Gilberto, 2018, pág. 128).

2.1.3 Antecedente Local

Antecedente Nº01

Como antecedente local tenemos la tesis de investigación cuyo título es: *"LOS DELITOS INFORMATICOS EN PERÚ Y LA SUSCRIPCIÓN DEL CONVENIO*

DE BUDAPEST", trabajo desarrollado por Marleny Yudy Huamán Cruz, presentado ante la Universidad Andina del Cusco, para obtener el título de Abogada, Cusco, Perú, año 2020. (Huamán Cruz, 2020, pág. 121)

En el referido trabajo de investigación, se hace referencia a la dificultad sobre la identificación y ubicación del sujeto activo de estos delitos, así mismo reafirma el preocupante crecimiento de estos delitos en el Perú, ya que nuestro país ocupa el tercer lugar en ataques a la ciberseguridad en Latinoamérica. Así lo expresa textualmente la autora en su tercera conclusión;

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

2.2 Bases teóricas

2.2.1 Historia de la criminalidad informática

La aparición de la revolución industrial y la era digital nos ha enseñado que existen diferentes métodos de comunicación, como las aplicaciones y redes sociales que han hecho más sencilla la interacción entre personas. En un principio, en 1969, nadie se imaginó que esto sería el comienzo de una nueva era que nos ha ofrecido muchas comodidades para nuestras actividades diarias e incluso para el ámbito social. Asimismo, la digitalización ha tenido un gran impacto en nuestra sociedad, lo que ha llevado a un cambio en la forma tradicional en que realizábamos nuestras actividades cotidianas. Como resultado, también han surgido nuevas formas de cometer delitos y perpetuarlos, y esto ha dado lugar a nuevas figuras delictivas que antes no conocíamos. Todo esto ha sido posible gracias a la evolución de nuestra realidad y sociedad debido a la digitalización.

La protección de la información sigue siendo un tema complejo, ya que el ciberespacio es un mundo digital en constante expansión que presenta nuevas

formas de delitos que afectan tanto a los derechos físicos como emocionales. La evolución del mundo digital ha llevado a que cada vez sea más difícil proteger la información, y esto se debe a que los delitos en línea son cada vez más sofisticados y difíciles de prevenir.

2.2.2 Delitos Informáticos

La ingeniería informática fue evolucionando en forma exponencial con el pasar del tiempo, pero una evolución y crecimiento del conocimiento sobre nuevas tecnologías informáticas no traerá únicamente desarrollo y progreso, este avance también conlleva nuevas formas de utilizar estas herramientas para fines ilícitos, es por ello que al ser la ley un cuerpo normativo cuya finalidad es regular las conductas de las personas la cual debe estar acorde a la realidad social actual, en nuestro país mediante la ley N° 30096, se logra introducir a nuestro ordenamiento la regulación para los delitos informáticos, pues estos delitos no son más que aquellos que mediante el uso de tecnologías de información o con la ayuda de sistemas maliciosos que desbloquean o "hackean" datos informáticos privados de las personas, logrando así inducir al engaño o al error para apoderarse de algún beneficio el cual puede ser dinerario, claro ejemplo es la clonación de tarjetas de crédito, asimismo Ramiro Salinas Siccha menciona que:

> "La definición de la delincuencia informática no resulta una tarea fácil ya que se trata de una realidad criminal mutable en el tiempo que ha ido configurándose con la influencia de las nuevas tecnologías" (Salinas Siccha, 2013, págs. 1302-1303).

2.2.3 Sabotaje Informático

Según Luis Azaola Calderón en su libro Delitos Informáticos y Derecho Penal define el sabotaje informático de la siguiente manera "Consiste básicamente, en borrar, suprimir o modificar (alterar) sin autorización funciones o datos de las computadoras con intención de obstaculizar el funcionamiento normal del sistema, que se conoce comúnmente como (virus informático)" (Azaola Calderón, 2010, pág. 69). Mientras que para (Marchena Gomez, 2001, pág. 356) el "sabotaje informático es la conducta que consiste en la destrucción o en la producción generalizada de daños". Finalmente, para (Morant Vidal, 2003,

págs. 46-47) “el sabotaje informático se dirige a inutilizar los sistemas informáticos causando daños a los programas”.

Las técnicas que permiten cometer sabotaje informático son las siguientes según (Azaola Calderón, 2010, pág. 70):

- Bomba lógica.- introducción de un programa de un conjunto de instrucciones indebidas que van a actuar en determinada fecha, destruyendo datos del ordenador, distorsionando el funcionamiento del sistema o paralizando el mismo.
- Rutinas cáncer.- Son distorsiones al funcionamiento del programa, la característica es la auto reproducción.
- Gusanos.- Se infiltran en los programas ya sea para modificar o destruir los datos, pero a diferencia de los virus estos no pueden regenerarse.
- Virus informático y malware.- Elementos informáticos que destruyen el uso de ciertos antivirus (Mata Barranco, 2009, pág. 311) . Como puede ser borrar los antecedentes policiales, judiciales y penales de una persona; alterar la deuda real de un cliente; cambiar la clave secreta o eliminar la cuenta electrónica (correo, twitter, Facebook) para impedir al titular el acceso a su cuenta.

2.2.4 Surgimiento de los delitos informáticos

La historia y evolución del delito cibernético es fácil de identificar y coinciden con la evolución del propio internet. Los primeros crímenes fueron, por supuesto, simples vulneraciones a los sistemas informáticos “hackeos”, con la finalidad de vulnerar la información privada pertenecientes a usuarios de sistemas informáticos, al respecto (Rinaldi, Paola, 2017) en el artículo web “¿De dónde viene del delito cibernético? origen y evolución del delito cibernético” hace mención a la siguiente evolución:

- Mientras que el delito cibernético existía antes de esto, la primera gran ola de delitos cibernéticos llegó con la proliferación del correo electrónico a finales de los años 80. Permitió que una gran cantidad de fraudes y/o malware se enviaran a tu bandeja de entrada.

- La siguiente ola en la línea de tiempo de la historia del delito cibernético llegó en los años 90 con el avance de los navegadores web. En ese momento había una multitud para elegir, muchos más que hoy, y la mayoría eran vulnerables a los virus. Los virus eran enviados a través de conexiones a internet siempre que se visitaban sitios web cuestionables. Algunos causaban que tu computadora funcionara lentamente, otros causaban que la aparición de publicidad molesta invadiera tu pantalla o la redirigiera a los sitios pornográficos indeseables.
- El delito cibernético realmente empezó a despegar a principios del 2000 cuando las redes sociales cobraron vida. La oleada de gente que, poniendo toda la información que podía en una base de datos del perfil, creó una inundación de información personal y el aumento del robo de identidad. Los ladrones utilizaban la información de varias maneras, incluyendo el acceso a cuentas bancarias, la creación de tarjetas de crédito u otros fraudes financieros.
- La última ola es el establecimiento de una industria criminal global que suma casi medio mil millones de dólares anuales. Estos criminales operan en pandillas, utilizan métodos bien establecidos y apuntan a cualquier cosa y a todos los que tienen presencia en la web.

El primer caso en el que se cometió un delito a través de una red de ordenadores es imposible de identificar. Siendo más adecuado remontarnos al primer gran ataque de una red digital, para luego usar ello como punto de referencia en la evolución de los delitos cibernéticos.

2.2.5 Tratados y acuerdos internacionales sobre delitos informáticos

Los medios informáticos y cibernéticos se constituyen en herramientas de especial eficacia para alcanzar una serie de propósitos delictivos. En tal sentido, tomando en cuenta que “estamos ante una delincuencia que genera efectos lesivos de contenidos cuantitativos y cualitativos significativos, y cuya operatividad traspasa las fronteras nacionales, se considera que debe ser afrontada a través de mecanismos de cooperación judicial internacional y de la suscripción de tratados y convenios internacionales sobre la materia” (Peña Cabrera Freyre, pág. 155).

"Debido a la dimensión transnacional de la criminalidad informática, en el marco de la Unión Europea se firmó el Convenio sobre Ciberdelincuencia, también conocido como el Convenio de Budapest sobre ciberdelincuencia; este convenio es el primer tratado primer tratado internacional que buscó hacer frente a los delitos informáticos y los delitos en internet mediante la armonización de leyes nacionales, la mejoras de las técnicas de investigación y el aumento de la cooperación entre las naciones. Dicho convenio de fecha 23 de noviembre de 2001" (Pérez López, 2019, pág. 91)

Respecto a la cooperación internación, la disposición séptima complementaria final de la Ley N° 30096 " Ley de Delitos Informáticos" estipula lo siguiente:

> "El Estado peruano realiza acciones conjuntas con otros Estados a fin de poner en marcha acciones y medidas concretas destinadas a combatir el fenómeno de los ataques masivos contra las infraestructuras informáticas y establece los mecanismos de prevención necesarios, incluyendo respuestas coordinadas e intercambio de información y buenas prácticas" (Ley N°30096 "Ley de Delitos Informáticos", 2013).

2.3 Fraude Informático

Para comprender el fraude cibernético o informático, debemos considerar el significado de la palabra "fraude", la cual es definida por la real academia española: "*Acción contraria a la verdad y a la rectitud, que perjudica a la persona contra quien se comete, realizado a través del uso de una computadora o del Internet"* (RAE, 2022). Pues esta es el uso ilegal de las herramientas de la informática (hacking), la cual resulta una forma común de fraude, esto consta en que el delincuente usa herramientas tecnológicas sofisticadas para acceder a distancia a una computadora con información confidencial.

Así pues, entendemos que el sujeto activo del delito vendría a ser un experto en tecnologías de la información el cual mediante sus conocimientos induce a error a personas mediante el engaño.

2.3.1 Fraude informático y su regulación en el Perú

Dentro del ámbito de la tutela al patrimonio económico, el artículo 8 de la (Ley N°30096 "Ley de Delitos Informáticos", 2013), modificado por el artículo 1

de la (Ley N° 30171, 2014), publicada el 10 de marzo de 2014, tipifica la modalidad delictiva rotulada con el *nomen iuris* de "fraude informático", la que se encuentra descrita de la siguiente manera:

"El que, deliberadamente 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 patrimonio del Estado destinado a fines asistenciales o a programas de apoyo social"

Este tipo penal coincide con lo normado por el artículo 8 de la Convención de Budapest, el mismo que señala lo siguiente:

"Las partes adoptaran 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:

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

La tipicidad de las conductas contra el patrimonio, utilizando medios informáticos, refleja algunas complejidades, Prías Bernal señala que "los medidos especiales utilizados para lograr este resultado tienen la virtualidad de convertir estos comportamientos en delitos no presenciales, al menos a los ojos de la víctima, además de diferir la producción de los efectos en el tiempo y de realizar las maniobras engañosas mediatamente a través de la información contendida en una base de datos" (Prías Bernal, 2016, pág. 30).

Recalcando que la Ley N° 30096 sufrió modificaciones a través de la Ley N° 30171, en la cual se agregó y modificó algunos tipos penales, tales como: el

acceso ilícito (artículo 2º), atentado a la integridad de datos informáticos y sistemas informáticos (artículos 3º y 4º), interceptación de datos informáticos (artículo 7º), fraude informático (artículo 8º), abuso de mecanismos y dispositivos informáticos (artículo 10º), también se agregaron en el mismo artículo antes mencionado, las palabras "deliberada e ilegítimamente, finalmente en dicha ley se derogó el artículo 6º que tipificaba el tráfico ilegal de datos.

Ahora bien, es importante señalar que nuestros legisladores al momento de elaborar la mencionada ley, utilizaron como base el "Convenio sobre la Ciberdelincuencia" o más conocido como el "Convenio de Budapest". Dicho Convenio – que se firmó en el año 2001 y entró en vigor internacionalmente en el año 2004- es un tratado internacional creado por los países miembros del Consejo de Europa "con el fin de hacer frente a los delitos informáticos a través de mecanismos de homologación de normas de derecho penal sustantivo, estandarización de procesos penales y cooperación internacional". (Guerrero Argote, 2018, pág. 4).

Al respecto de este convenio, es muy curioso que recién en el año 2019 el Poder Legislativo lo haya aprobado por Resolución Legislativa N° 30913, de fecha 12 de febrero de 2019, y con fecha 10 de marzo de ese mismo año el Poder Ejecutivo lo ratificó mediante Decreto Supremo N.º 010-2019-RE, cuando desde el año 2013 ya existía una Ley de Delitos Informáticos en el país y donde el mencionado Convenio hubiera sido de mucha utilidad para que los operadores de justicia puedan tomar conciencia sobre la protección de la seguridad informática y la cultura digital que debe existir en el país.

De la redacción del tipo penal del fraude informático, se advierte que este ilícito es genérico dado que sobre el agente no pesan especiales deberes de actuación, sino que se trata de la configuración del ámbito de organización del usuario dentro de la red, y en cuanto al sujeto pasivo también es genérico, lo será el titular del derecho patrimonial vulnerado.

Esta figura penal se clasifica como un delito de resultado, toda vez que no basta con realizar las conductas típicas mencionadas, sino que además es necesario que esa acción vaya seguida de un resultado separado de la misma conducta el cual es causar un perjuicio económico.

La redacción del tipo penal, deliberada e ilegítimamente, nos evidencia que únicamente se puede cometer de forma dolosa, no cabiendo la comisión por culpa; es decir, el agente debe tener la conciencia y voluntad de diseñar, introducir, alterar, borrar, suprimir, clonar, interferir o manipular de forma ilegítima un sistema informático.

2.3.2 Análisis del tipo objetivo

2.3.2.1 Sujeto activo

El sujeto activo en este delito podrá ser cualquier tipo de persona, no es necesario que tenga conocimientos especiales sobre informática o un experto en computadoras, es necesario recordar que estamos ante un delito de hurto agravado lo cual obliga desestimar como posible autor al propietario del bien mueble, existen dos casos que (Bramont- Arias Torres, 1997) describe como autores del delito:

> *1 º) Aquellos en los que el sujeto actúa sobre un sistema informático ajeno, esto es, directamente sobre los elementos lógicos o sobre el soporte físico, o por comunicación electrónica, desde otra computadora y a distancia. En estos casos el agente es un tercero, extraño al sistema afectado, aunque frecuentemente se tratará de un empleado o de alguien vinculado a la entidad titular de los datos electrónicos.*

> *2º) Aquellos en que es el propio titular del sistema afectado quien lleva a cabo la manipulación fraudulenta en perjuicio de terceros - entidad bancaria, compañía de seguros, empresa, administración tributaria. Por otro lado, en estos supuestos, lo normal es que el empresario, directivo o comerciante, por ejemplo, que se sirve en su actividad de un equipo informático cuyo funcionamiento técnico desconoce, necesite de personal especializado para materializar sus órdenes, decisiones o actos dispositivos a través de las máquinas.*

2.3.2.2 Sujeto pasivo

En el presente delito tenemos como sujeto pasivo al titular del bien jurídico protegido, el cual vendría a ser el titular del patrimonio afectado por medio de la

manipulación informática, este sujeto podrá ser una persona natural o jurídica, comúnmente eran las empresas corporativas de grandes capitales, pero en estos años esto fue cambiando, puesto que estos fraudes informáticos se practicaron con mayor frecuencia a personas naturales, personas con poco conocimiento en la informática o personas adultas que no están muy asociadas a prácticas con la tecnología, las cuales son más propensas a sufrir fraude.

2.3.2.3 Bien Jurídico Protegido.

El bien jurídico protegido en este delito es el patrimonio del cual es titular el sujeto pasivo, es decir tendrá que ser un bien mueble necesariamente el cual es sustraído por el sujeto activo mediante el uso de algún medio informático, debido a que este bien jurídico al encontrarse en forma virtual y no física es pasible de ser objetivo de un fraude informático, (Bramont- Arias Torres, 1997), en su libro sobre los delitos informáticos nos indica que:

> *"El objeto material sobre el que recae el delito ha de ser, por tanto, un bien mueble. No se admiten como objeto material del delito los bienes inmateriales ni los que no tengan un valor económico".*

2.3.3 Análisis del tipo subjetivo.

2.3.3.1 Dolo

Resulta indispensable el elemento de dolo, es decir el ánimo de lucrar, con el ánimo de adquirir un provecho ilícito, es decir que mediante el uso de la informática con la intención de obtener un beneficio económico o provecho. Es imposible pensar que en este tipo de delitos no se tiene intención o existe culpabilidad, esto debido a que el tipo penal exige la intención para la comisión de este delito.

2.3.4 Grados de ejecución del delito.

2.3.4.1 Consumación y Tentativa

Entendiendo que este tipo penal se comete con la finalidad de un provecho o beneficio económico, debemos tener en cuenta que la consumación será considerada cuando el sujeto activo logra tener disponibilidad o acceso del bien jurídico protegido, es decir cuando la persona que realiza el fraude informático y logra su objetivo haciendo que su víctima otorgue-ya sea-con engaño, por un ataque informático o por otro medio informático, adquiere la capacidad de disponer de este bien mueble. Al respecto (Bramont- Arias Torres, 1997) refiere que:

> *El objeto material del delito, en este caso, vendría constituido por el dinero, y quedaría consumado con el acceso a la cuenta a través de la violación de la clave secreta, siendo indiferente el hecho de que con posterioridad se devuelva o no la tarjeta. Por el contrario, cuando la modalidad delictiva consista en el empleo de la telemática, en general, el delito girará en torno al acceso del sistema informático o red o cadena informática con el ánimo de causar un perjuicio económico, de suerte que la consumación tiene lugar con el simple acceso - siempre que concurran los demás elementos, y en especial la intención de obtener un lucro-, sin que sea precisa la apropiación efectiva de los fondos u otros bienes.*

2.3.5 Fraude Informático en el ámbito local

El presente trabajo será realizado en la Provincia del Cusco es por ello que analizaremos la problemática de la adecuada regulación del delito de Fraude Informático, recogida en la ley N° 30096, pero desde la óptica de la realidad de la provincia del Cusco, como este delito se viene produciendo y aquejando a la población cusqueña, ya que muchísima gente ha ido sufriendo atentados contra sus datos personales, como claves de seguridad bancaria, engañados por el desconocimiento de las nuevas formas de robo de información personal.

Así pues, en el año 2020 la periodista del medio de comunicación “Diario La República” Maribel Mamani, emitió un reportaje periodístico en su portal web mencionando lo siguiente:

"Los delincuentes intentaron adaptarse a la nueva normalidad. Ya no utilizan un arma para asaltar a sus víctimas sino los hackean para vaciarle sus cuentas. Los ciberdelitos o fraude informático, aumentó en 51.5% este año en comparación al 2019. El confinamiento hizo que muchas personas privilegien las operaciones digitales con el riesgo que ello significa.

El jefe del área de Alta Tecnología Informática de la División de Investigación Criminal - Divincri, brigadier PNP Harry Ordoñez, indica que los casos se incrementaron significativamente. Este año se denunciaron 861 casos de fraude.

Las modalidades más frecuentes son el phishing, primer contacto con la víctima para direccionarlo a una página falsa en donde ingresa sus datos. También figura el Smishing y el Vishing, cuando la persona es contactada por mensaje o llamada y brinda la clave de su tarjeta. El Skimming, también es de las más recurrentes, cuando acceden a números que figuran en la tarjeta de alguna entidad bancaria para proceder con el fraude" (Maribel, 2020).

En el año 2021, el grupo periodístico "Exitosa", mediante su portal de la red social Facebook, mencionó un incremento de estos casos y destacó un caso con la minera las bambas, indicando lo siguiente:

> "*DIARIAMENTE SE REPORTAN DELITOS DE FRAUDE INFORMÁTICO EN EL CUSCO*
> *El suboficial especialista en delitos de alta tecnología PNP, Harry Ordóñez, dio a conocer que el índice de casos de delitos de fraude informático y estafas virtuales está en aumento en el Cusco, siendo la incidencia de estos reportes de forma diaria en los que las víctimas sufren la perdida de sumas importantes de dinero, señalando un caso que se viene investigando de una empresa que labora con la minera Las Bambas que habría perdido más de un millón de soles.*
> *La modalidad que utilizan los ampones para delinquir suele ser enviar un mensaje de texto en el que indican que la persona ha realizado una transacción de dinero y que si desea revertir esto se redirija a un enlace web (link) el cual es falso mediante el cual se instala un software que roba su dinero.*

El brigadier PNP refirió que en todos estos casos se está trabajando para dar con la ubicación de estas redes criminales que operan desde la clandestinidad" (Exitosa Noticias, 2021).

Es a razón del quejar de la población respecto de un delito el cual en la mayoría de casos no se realiza una correcta investigación, ya sea por parte de la fiscalía como de la policía especializada, en consecuencia, de ello queda como un "delito impunible", todo ello por la ausencia de una correcta adecuada y actualizada regulación del delito en mención.

2.4 Hipótesis del Trabajo

2.4.1 Hipótesis General

La actual tipificación del fraude informático regulado en el artículo 8 de la Ley N°30096 – Ley de Delitos Informáticos no se encuentra adecuada a nuestra realidad tecnológica actual.

2.4.2 Hipótesis especificas

1. No es posible prevenir las actuales conductas ilícitas del ámbito tecnológico únicamente mediante una adecuada reforma a la legislación de Delitos Informáticos "Ley N° 30096".
2. La Ley N°30096, "Ley de Delitos Informáticos" no cuenta con un tratamiento especial acorde al convenio de Budapest.
3. La falta de conocimiento de los ciudadanos sobre las nuevas tecnologías y la imprecisión normativa son factores que inciden en la comisión de fraude informático.

2.5 Definición de términos

Es fundamental establecer una definición exhaustiva de los términos técnicos y complejos utilizados en la investigación, así como aquellos propios del lenguaje informático. La intención de esto es lograr una comprensión más completa de la investigación llevada a cabo.

- **Delito Informático:** Se entiende por delito informático a la comisión de un acto ilegal que se lleva a cabo mediante el uso de un medio o herramienta informática.

- **Virus:** Se trata de una serie de instrucciones de programación que pueden adherirse a programas legítimos y propagarse a otros programas de computadora. Los virus informáticos pueden infiltrarse en un sistema a través de un software original infectado, así como empleando la técnica conocida como Caballo de Troya.

- **Malware:** El vocablo "malware" deriva del idioma inglés y surge de la combinación de las palabras "malicious software" o software malicioso. En consecuencia, se refiere a un tipo de programa o aplicación informática que busca dañar el dispositivo en el cual ha logrado alojarse, instalarse o infiltrarse, sin importar si se trata de un ordenador, teléfono móvil o cualquier otro dispositivo electrónico (Fernandez, Malware: qué es, qué tipos hay y cómo evitarlo, 2020).

- **Pharming:** Es un tipo de ataque informático que se produce a través de un código malicioso, a menudo en forma de troyano, que se instala en el ordenador durante una descarga. Este código permite que el usuario sea redirigido a una página web falsa cuando ingresa la dirección de una página web deseada. Esta página falsa está diseñada para parecerse a la página real, pero su objetivo es engañar al usuario y recopilar información personal o financiera.

- **Phishing:** Técnica que se basa en el envío de correos electrónicos fraudulentos a los usuarios, en los cuales se finge ser una entidad reconocida y seria, como por ejemplo un banco. Estos correos engañosos solicitan al usuario que actualice o verifique sus datos personales como cliente, y suelen incluir un enlace que lleva a una página web falsa que simula ser la entidad suplantada. Una vez que el usuario proporciona sus datos, los delincuentes o estafadores pueden utilizarlos para llevar a cabo diversas acciones ilegales o fraudulentas.

- **Vishing:** Es una modalidad de engaño mediante técnicas de ingeniería social que se lleva a cabo a través de llamadas telefónicas en las que el atacante se hace pasar por una organización o persona confiable con el fin de obtener información personal o sensible de la víctima. El objetivo final es la obtención de información privada que pueda ser

utilizada para cometer fraudes financieros o cualquier otra actividad ilícita.

- **Smishing:** Táctica utilizada por los ciberdelincuentes que se basa en el envío de mensajes de texto a usuarios, haciéndose pasar por una entidad legítima, como un banco, una red social o una institución pública, con el fin de obtener información personal o financiera o incluso realizar cargos económicos. Estos mensajes suelen incluir una solicitud para que el usuario llame a un número de teléfono o haga clic en un enlace a una página web falsa, todo bajo un pretexto aparentemente legítimo.
- **Skimming:** Es el robo de información de tarjetas de crédito o débito, ocurre cuando se intercepta y se recopila información confidencial de la tarjeta en el momento en que se utiliza en un cajero electrónico. El objetivo principal de esta práctica es reproducir o clonar la tarjeta para poder usarla fraudulentamente.

CAPÍTULO III

3. MARCO METODOLÓGICO

3.1 Diseño Metodológico

Enfoque de la Investigación	Cualitativo Documental. - Se aplicará dicha técnica porque el análisis y estudio del mismo se encuentra basado en documentos, libros, y diversa información que será recabada de pruebas documentales ya investigadas y desarrolladas con anterioridad por otros estudiosos de la materia.
Tipo de Investigación Jurídica	Dogmática Propositiva. - Es una investigación crítica al artículo de 8 Ley N°30096 "Ley de Delitos Informáticos" y su aplicación específicamente al delito de Fraude Informático, motivo de ello se planteará propuestas de reforma a dicha legislación, adecuada a la nueva realidad tecnológica.

Teniendo en cuenta que la metodología viene a ser parte del proceso de investigación donde a través de pasos y fases se llega a analizar, buscar respuestas a las preguntas que el investigador se plantea y poder comprobar los supuestos implícitos de los cuales partió.

Se tiene que tener en cuenta que la Investigación Cualitativa es la ciencia y arte de poder describir a un grupo o cultura, esta tarea viene a ser similar a la labor

de un periodista investigativo que entrevista a personas, revisa récords, redacta artículos para grupos y organizaciones específicas, de igual manera de temas de interés para sus colegas. La investigación Cualitativa es un enfoque particularmente valioso porque problematiza las formas en que los individuos y los grupos que constituyen e interpretar las organizaciones y las sociedades, de igual manera se tiene que tener en cuenta que este tipo de investigación facilita el aprendizaje de culturas y estructuras organizacionales porque provee al investigador forma de examinar el conocimiento, el comportamiento y los artefactos que los participantes comparten y usan para interpretar sus experiencias (Schwartzman, 1993)

3.2 Diseño Contextual

La investigación a desarrollar tendrá un diseño no experimental, descriptivo, transversal ya que no habrá manipulación de variables, sólo se describirán los hechos del fenómeno observado y la información se levantará en un solo espacio de tiempo.

La metodología adoptada para la realización de la investigación se fundamenta en analizar la Ley N°30096 "Ley de Delitos Informáticos" y su aplicación específicamente al delito de Fraude Informático.

Para la realización del análisis, se consultará leyes, normas legales, libros jurídicos, trabajos científicos referentes a la problemática del fraude informático. Asimismo, se identificarán propuestas de reformas al artículo 8 de la Ley de Delitos Informáticos adecuadas a la nueva realidad tecnológica.

3.3 Técnicas e instrumentos de recolección de datos

TECNICAS	INSTRUMENTOS
• **Análisis Documental**	• Análisis documental y bibliográfica
• **Encuesta**	• Cuestionario de Preguntas a ciudadanos peruanos.

La recolección de datos se realizará mediante la consulta a diversas fuentes de información enfocadas a los delitos informáticos, el fraude informático, las nuevas tecnologías y la legislación peruana, los cuales son los siguientes: Análisis Documental (Estudio de información de diversas fuentes documentales y virtuales), Análisis Jurídico a la Ley N°30096 "Ley de Delitos Informáticos", Análisis Jurídico a la Ley Nº 30171 modificatoria a la "Ley de Delitos Informáticos", Análisis al Convenio de Budapest, Análisis del libro "Derecho Informático", del Dr. Julio Tellez Valdés, Análisis de del libro " Manual de Derecho Informático ", del Dr. Horacio Fernández Delpech, Análisis Ciberdelincuencia en el Perú: "Pautas para una buena investigación Fiscal Especializada", de la Oficina de Análisis Estratégico del Ministerio Publico, Análisis a las propuestas del Tratamiento Judicial del Ciberdelito expuesto por el Consejo Ejecutivo del Poder Judicial.

Encuestas breves a 15 ciudadanos peruanos, con la intención de saber sí dichos ciudadanos que hacen uso del internet, fueron víctimas de fraude informático y además si los usuarios más frecuentes de internet se sienten seguros navegando por la web y finalmente si conocen algunas medidas preventivas para evitar ser víctimas de la ciberdelincuencia.

3.3.1 Técnicas para la recolección de datos

Técnica de observación, para el desarrollo de la investigación se utilizará la técnica de información indirecta, utilizando trabajos de investigación científica y académica que ya fueron desarrollados respecto a los delitos informáticos.

3.3.2 Instrumentos para la recolección de datos

En cuanto a los instrumentos de recolección, se utilizarán bibliotecas virtuales, libros físicos, internet, redes sociales, sitios web para consultar la opinión de las personas respecto a los riesgos que conocen del internet.

3.4 Procedimiento de la Investigación

- Recolección, ordenamiento y procesamiento de la información bibliográfica y documental.
- Revisión y análisis de la legislación nacional.
- Búsqueda, revisión y análisis de los trabajos de Investigación realizados previamente referentes a los Delitos Informáticos.

- Elaboración de los Instrumentos
- Encuestas referentes a las nuevas tecnologías y delitos informáticos.
- Aplicación del instrumento
- Recolección, ordenamiento y análisis de toda la información.

CAPITULO IV

4. DESARROLLO TEMÁTICO

4.1 Legislación Comparada

PAÍS	LEY O NORMATIVA	DEFINICIÓN DE FRAUDE INFORMÁTICO	SANCIONES
ESTADOS UNIDOS	Computer Fraud and Abuse Act	Acceso no autorizado a sistemas de computadora, robo de información, espionaje, daño a sistemas informáticos	Multas, prisión, compensación económica, libertad condicional
REINO UNIDO	Computer Misuse Act	Acceso no autorizado a sistemas de computadora, alteración de información, creación y distribución de malware y virus	Multas, prisión, confiscación de bienes
ESPAÑA	Ley Orgánica de Protección de Datos Personales y Garantía de Derechos Digitales	Acceso no autorizado a sistemas informáticos, interceptación de comunicaciones, daño a sistemas informáticos	Multas, prisión, inhabilitación temporal o permanente, compensación económica
MÉXICO	Ley Federal de Delitos Informáticos	Acceso no autorizado a sistemas de computadora, daño a sistemas informáticos, creación y distribución de malware y virus	Multas, prisión, reparación del daño, confiscación de bienes
ARGENTINA	Ley de Delitos Informáticos	Acceso no autorizado a sistemas de computadora, daño a sistemas informáticos, creación y distribución de malware y virus	Multas, prisión, inhabilitación, decomiso de bienes, reparación del daño

4.1.1 El fraude informático en España.

El artículo 248 del Código Penal español establece lo siguiente:

"1. El que, con ánimo de lucro y valiéndose de engaño bastante, en las cosas que se definen a continuación, indujere a otro a realizar un acto de disposición en perjuicio propio o ajeno, será castigado con la pena de prisión de seis meses a tres años o multa de seis a doce meses" (Congreso de España , 1995).

Las conductas a que se refiere el apartado anterior son:

a) La obtención de bienes, servicios o cualquier tipo de utilidad, ya sea para sí o para otro, mediante la utilización de tarjetas de crédito o débito, o de cualquier otro medio de pago similar, o la utilización de cheques de viaje o similares, o de identificadores o claves de acceso o de cualquier otro medio de identificación o autenticación de titularidad ajena.

b) La realización de operaciones de cualquier clase en perjuicio del titular de los medios mencionados en el párrafo anterior, o la obtención de descuentos o beneficios de cualquier clase en perjuicio ajeno.

c) La utilización de datos identificativos de otra persona o la invención de una identidad, para solicitar productos o servicios, para formalizar contratos o para llevar a cabo cualquier otra clase de actividades empresariales.

d) La simulación de hechos falsos o la ocultación de los verdaderos, de manera que, induciendo a error a otros, se logre un lucro ilegítimo propio o ajeno.

e) El empleo de cualquier otro engaño similar.

En este artículo se incluye el phishing como una de las conductas tipificadas como delito de estafa, en la que se utiliza el engaño para inducir a otra persona a realizar un acto de disposición en perjuicio propio o ajeno.

4.2 Fundamentación jurídica para la correcta tipificación del Fraude Informático

4.2.1 La Taxatividad de la Ley

Este principio nos hace referencia a obligatoriedad que tiene el legislador de redactar con precisión el tipo penal, así es que este principio resulta en consecuencia del principio de legalidad esto requiere que el legislador redacte las leyes que definen los delitos con precisión. Por lo tanto, los tipos penales deben ser lo más precisos posible, y es necesario establecer con certeza los requisitos que hacen que una conducta sea susceptible de ser penalizada.

4.2.2 El principio de Legalidad

En la concepción actual del Derecho Penal, se considera que uno de los principios fundamentales de todo sistema jurídico es el principio de legalidad. Este principio se puede resumir en la famosa frase en latín "nulla crimen, nulla poena sine lege" propuesta por Ansel von Feuerbach, que significa que no puede haber delito ni castigo sin ley. Este principio garantiza que el Estado solo puede castigar a una persona si se ha violado una ley escrita, clara y previa. Es una protección individual que exige que la ley sea el requisito previo para la imposición de una pena.

4.2.3 La prohibición de la Analogía

Este principio también se encuentra relacionado con el principio de legalidad puesto que es la mera manifestación y asimismo la injerencia de este en la labor interpretativa de los jueces, al respecto (TerrerosVillavicencio, 2006) manifiesta que:

> "Puede ser entendida como el proceso por el cual son resueltos los casos no previstos por la ley, extendiéndoles a ellos las disposiciones previstas para casos semejantes (analogía legis) o están deducidos de los principios generales del derecho (analogía juris)"

No obstante, es importante destacar que existe un tipo de analogía que sí está permitido en nuestro sistema jurídico, que se conoce como "analogía in bonam partem". Esta analogía se aplica cuando se busca eximir o reducir una pena y permite hacer una comparación entre casos similares para determinar si la persona en cuestión debería recibir una pena menos severa o ninguna pena en absoluto.

Por otra parte, el principio de prohibición de la analogía sustenta la inmediata necesidad de tipificar correctamente el delito de Fraude Informático redactado en la ley 30096, ya que demuestra que el actual texto, no es suficiente para tipificar ampliamente el Fraude Informático. No se puede hacer una interpretación que ajuste los verbos rectores a los supuestos de las modalidades del fraude informático como el Smishing, ya que esto sería una analogía "*in malam partem*", algo que está prohibido por este principio.

4.3 Modalidades más denunciadas en el Perú

En el Perú, se han investigado diversas modalidades de fraude informático, las cuales han sido objeto de atención por parte de las autoridades encargadas de combatir este tipo de delitos, dicha información fue recaba del sitio web Andina "Agencia peruana de noticias", articulo redactado por Sofia Pichiua quien tomo como fuente principal los datos estadísticos de la DIVINDAT, artículo que titula "¡Cuidado con los fraudes informáticos! Estas son las modalidades más denunciadas en Perú" (Pichiua, 2023)

a) Phishing.

Durante el año 2022, la técnica de phishing se posicionó como la modalidad de fraude informático más denunciada, alcanzando un total de 720 registros. Esta práctica consiste en la creación de una página web falsa, normalmente de entidades bancarias, con el propósito de engañar al usuario para que proporcione información personal como nombre, número de teléfono, DNI e incluso contraseñas de servicios financieros.

Según el coronel PNP, una vez que la víctima proporciona sus datos, reciben una llamada telefónica de la supuesta entidad financiera, en la que se les informa de un intento fallido de ingreso a su cuenta y se les solicita que entreguen el token que reciben en su celular para verificar su identidad. Además, los delincuentes utilizan los datos personales previamente registrados para ganar la confianza del usuario y aumentar las posibilidades de éxito.

Finalmente, con el token en su poder, los ciberdelincuentes realizan transferencias bancarias ilegales y cometen el fraude cibernético.

b) Carding

La segunda técnica más reportada es el "carding", con 472 casos, que consiste en la realización de compras en línea ilegales utilizando tarjetas de crédito robadas. Los delincuentes suelen hacer compras de montos pequeños para evitar llamar la atención y ser descubiertos de inmediato por la víctima.

Además, también se utiliza la suplantación de identidad de personas con un historial crediticio positivo y fondos suficientes en sus tarjetas para realizar compras de gran valor, especialmente en sitios web internacionales de comercio electrónico.

c) SIM Swapping.

La tercera modalidad más denunciada por fraude informático en Perú es el SIM Swapping, con 238 casos registrados. De acuerdo con el coronel PNP, la entidad más afectada por esta modalidad es el Banco de la Nación. Este tipo de fraude comienza cuando los estafadores obtienen los datos personales de sus víctimas a través de mecanismos fraudulentos y luego se comunican con las empresas de telefonía móvil para bloquear la tarjeta SIM de la víctima. Al duplicar la tarjeta SIM y tener los datos personales de la víctima, los delincuentes pueden acceder a su banca en línea y realizar transacciones fraudulentas como transferencias, retiros de dinero o solicitudes de préstamos.

Según el jefe de Divindat, esta modalidad es difícil de prevenir, por lo que es importante que los usuarios informen a su proveedor de telecomunicaciones ante cualquier problema con su línea telefónica, como una forma de evitar ser víctima de estos fraudes informáticos.

d) Thief Transfer.

La cuarta modalidad más denunciada en la Divindat es el Thief Transfer, con un total de 210 denuncias registradas. Esta forma de fraude informático implica el uso de teléfonos celulares robados o perdidos por los delincuentes para cometer el delito.

Los ciberdelincuentes aprovechan cuando el usuario bloquea su móvil por una pérdida o robo, para extraer la tarjeta SIM y colocarla en otro dispositivo, con el fin de obtener toda la información necesaria y así llevar a cabo el fraude.

Además de las modalidades de fraude informático mencionadas anteriormente, también existe el vishing. En esta modalidad, los estafadores hacen llamadas fraudulentas para engañar a las víctimas y obtener información personal y confidencial. Para llevar a cabo el fraude, se suplanta la identidad de una empresa, organización o persona de confianza. Durante el 2022, esta modalidad generó 181 denuncias. Las otras modalidades de fraude informático no mencionadas anteriormente, representaron un total de 561 denuncias.

4.4 Análisis de Delito Computacional y Delito Informático

4.4.1 Delito informático

Son las acciones delictivas dirigidas específicamente hacia los bienes informáticos en sí, no como medio para cometer otro delito, se consideran delitos informáticos. Por ejemplo, los delitos informáticos incluyen el daño al software causado por un virus, el acceso no autorizado a una computadora o la piratería de software (copia ilegal). Sin embargo, debe tenerse en cuenta que el robo o daño físico del hardware de un sistema informático no se considera un delito informático.

4.4.2 Delito computacional

Por delito computacional se entiende a las acciones delictivas convencionales contempladas en nuestro Código Penal que utilizan los medios informáticos como herramienta para cometer el delito. Por ejemplo, se protegen los bienes jurídicos tradicionales, como el patrimonio, cuando se realizan estafas, robos o hurtos a través de una computadora conectada a una red bancaria. De manera similar, el robo o el acceso no autorizado a correos electrónicos viola la privacidad de las personas.

4.4.3 Diferenciación

Como podemos ver, hay una clara distinción entre las dos categorías. Los delitos informáticos afectan tanto a los delitos tradicionales como a los delitos de nueva generación que a menudo se utilizan en la vida cotidiana y requieren un mayor nivel de sofisticación. Los delitos computacionales, por otro lado, se refiere a acciones ilegales que tienen como objetivo perjudicar la funcionalidad de una computadora al alterar el orden y la secuencia de los datos que contiene.

4.5 Similitudes y diferencias entre cracker y hacker.

Debemos tener en cuenta que en el mundo globalizado donde vivimos ahora, existen personas que tienen diferentes capacidades intelectuales y con el avance de la tecnología estas capacidades se pueden expandir a un más, pero no siempre estas capacidades son utilizadas para el avance de la humanidad, muchas veces son en beneficio de intereses oscuros o para el crimen. Entendemos que para el delito de Fraude Informático algunos agentes gozan de estas capacidades intelectuales para cometer este delito, por ejemplo, tenemos que definir al Hacker y al Cracker y comparar según sus capacidades y objetivos de cada uno.

4.5.1 Hacker

Entendemos a este como aquella persona que aprovecha sus conocimientos para mejorar un sistema en el aspecto de seguridad, además tiene la capacidad de generar su propio código y poder arreglar su código de seguridad, esta persona se introduce en sistemas que son ajenos con el fin de verificar la seguridad.

4.5.2 Cracker

Esta persona al igual que el Hacker logra ingresar a los sistemas ajenos, pero la gran diferencia es que lo hace con fines maliciosos, usan un software informático que tiene la tarea de buscar puntos débiles en la seguridad de un sistema y con ello se infiltran dentro de este, logrando robar o destruir información, también suelen vender la información obtenida generando daño y explotan vulnerabilidades compartiendo en la Dark Web.

CAPITULO V

5. RESULTADO Y ANALISIS DE LOS HALLAZGOS

5.1 Resultados de estudio

Una adecuada reforma a la legislación de delitos informáticos en el Perú puede ser una herramienta efectiva para prevenir comportamientos ilegales en el ámbito tecnológico. La actualización de las leyes puede mejorar la identificación y el enjuiciamiento de los delitos informáticos, así como el establecimiento de sanciones más duras para los infractores.

No obstante, reformar la legislación no es la única solución. Es importante considerar también la implementación de medidas educativas y de conciencia sobre la utilización responsable de la tecnología, la protección de la información personal y la prevención del ciberacoso, entre otros temas.

Asimismo, cabe destacar que el éxito de cualquier reforma legal dependerá de la capacidad del Estado para aplicarla y hacerla cumplir, lo que implica contar con los recursos y la voluntad política necesarios para combatir la delincuencia en línea y garantizar la seguridad en la red.

La pertinencia de la tipificación del delito de Fraude Informático contemplado en el artículo 8 de la Ley N° 30096, a la luz de la realidad tecnológica actual, es un tema que puede ser objeto de debate. A pesar de que la ley es relativamente reciente y se promulgó en 2013, en una época de constante evolución tecnológica, es importante tener en cuenta que el delito de fraude informático sigue siendo un comportamiento común en la actualidad y la tipificación de dicho delito sigue siendo relevante.

El artículo 8 de la Ley N° 30096 define el delito de Fraude Informático como aquel que comete una persona que, con el objetivo de obtener un beneficio ilícito para sí o para otros, realice cualquier acción tendente a engañar a una persona

o entidad utilizando medios informáticos. A pesar de esto, es posible que la legislación necesite ser revisada y actualizada para garantizar que siga siendo efectiva en la prevención de los delitos informáticos.

Por lo tanto, es importante llevar a cabo evaluaciones periódicas de las leyes existentes para asegurarse de que sigan siendo adecuadas y eficaces en la protección de los ciudadanos contra los delitos informáticos.

5.2 Análisis de los hallazgos

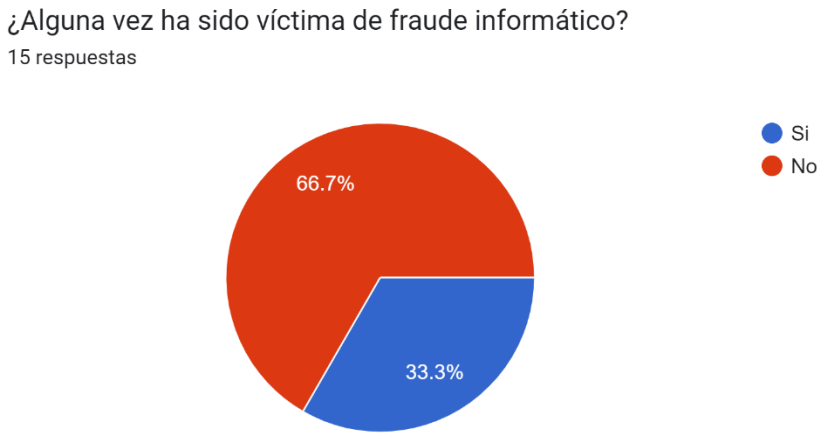


Figura 1

Fuente: Elaboración de los autores

De la figura 1, que representa la siguiente pregunta: ¿Alguna vez ha sido víctima de fraude informático?, se realizó una encuesta utilizando Google Formularios a 15 ciudadanos peruanos, se compartió el cuestionario mediante redes sociales, en la cual se obtuvo el siguiente resultado: 10 personas refirieron NO haber sido víctimas de Fraude Informático equivalente al 66.7%, y 5 personas refirieron SI haber sido víctimas del referido delito, equivalente al 33.3% del total de encuestados.

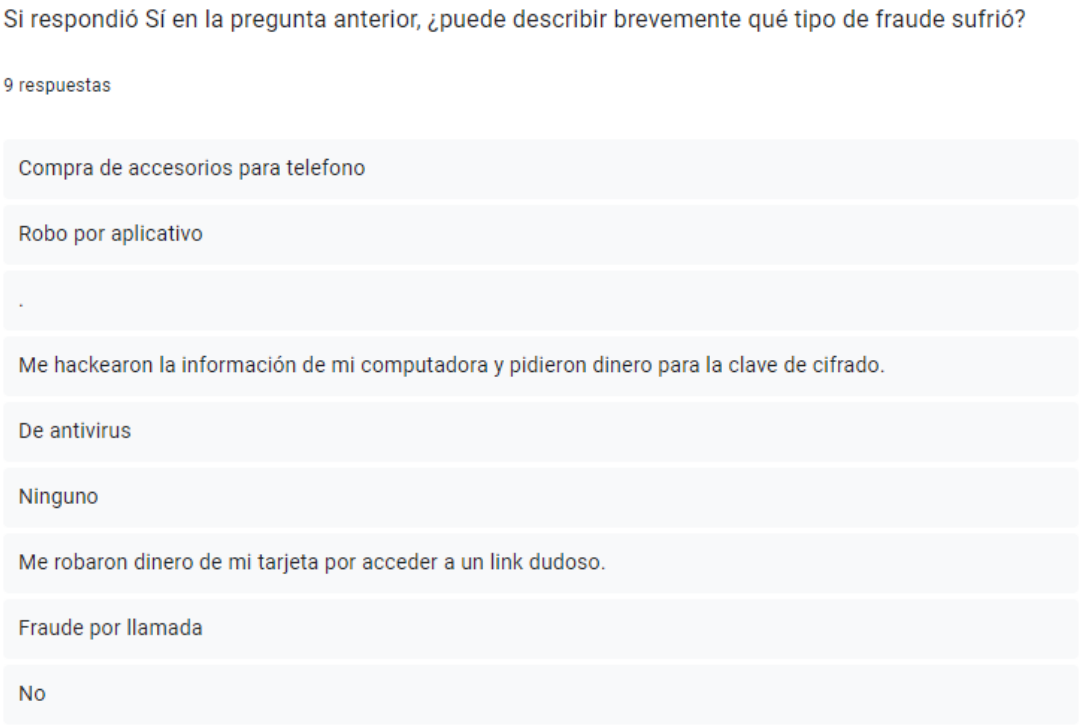


Figura 2

Fuente: Elaboración de los autores

De la figura 2, que representa la siguiente pregunta: Si respondió Sí en la pregunta anterior, ¿puede describir brevemente qué tipo de fraude sufrió?, se realizó una encuesta utilizando Google Formularios a 15 ciudadanos peruanos, se compartió el cuestionario mediante redes sociales, en la cual se obtuvo el siguiente resultado:

Las personas que fueron víctimas del delito informático describieron algunas modalidades por las que fueron víctimas:

- Compra de accesorios para teléfono
- Robo por aplicativo
- Me hackearon la información de mi computadora y pidieron dinero para la clave de cifrado.
- De antivirus
- Me robaron dinero de mi tarjeta por acceder a un link dudoso.
- Fraude por llamada

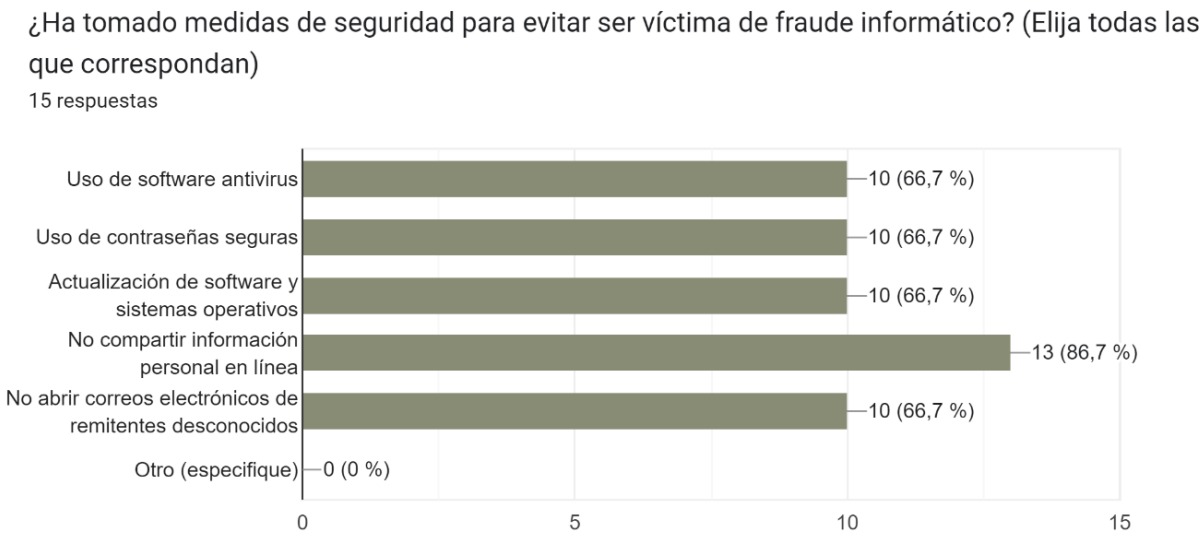


Figura 3

Fuente: Elaboración de los autores

De la figura 3, que representa la siguiente pregunta: ¿Ha tomado medidas de seguridad para evitar ser víctima de fraude informático?

Se realizó una encuesta utilizando Google Formularios a 15 ciudadanos peruanos, se compartió el cuestionario mediante redes sociales, obteniéndose el siguiente resultado: En la pregunta 3 se permitió brindar respuestas múltiples:

- 10 personas refirieron que hacen Uso de software antivirus
- 10 personas refirieron que hacen uso de contraseñas seguras
- 10 personas refirieron que tienen como medida de seguridad la actualización de software y sistemas operativos
- 13 personas refirieron que prefieren no compartir información personal en línea
- 10 personas refirieron que como medida de seguridad no abren correos electrónicos de remitentes desconocidos.

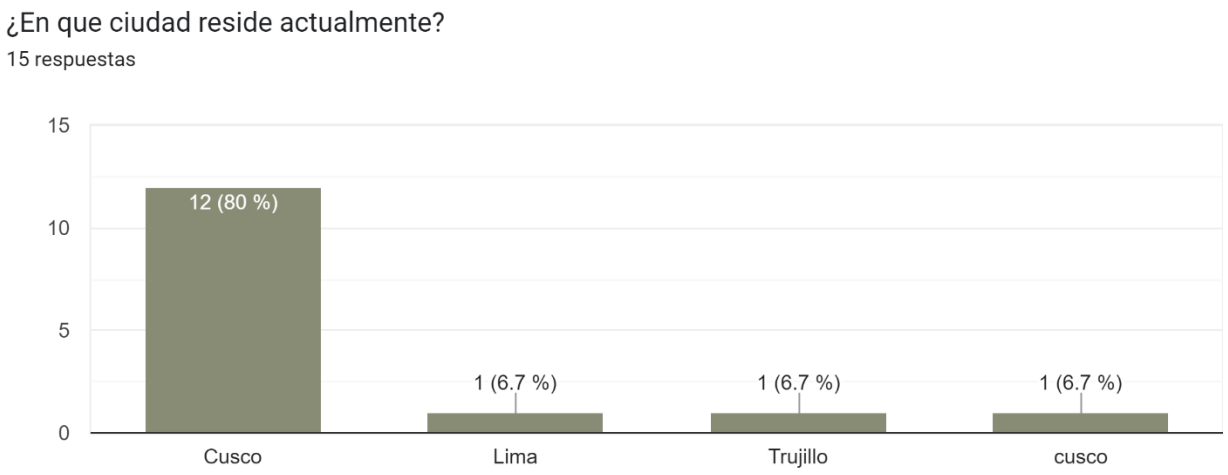


Figura 4

Fuente: Elaboración de los autores

De la figura 4, que representa la siguiente pregunta: ¿En qué ciudad reside actualmente?, se realizó una encuesta utilizando Google Formularios a 15 ciudadanos peruanos, se compartió el cuestionario mediante redes sociales, en la cual se obtuvo el siguiente resultado: 13 personas refirieron residir en la ciudad del Cusco equivalente al 80%, 1 persona en la ciudad de Lima, 1 persona en la ciudad de Trujillo, equivalentes al 6.7% respectivamente.

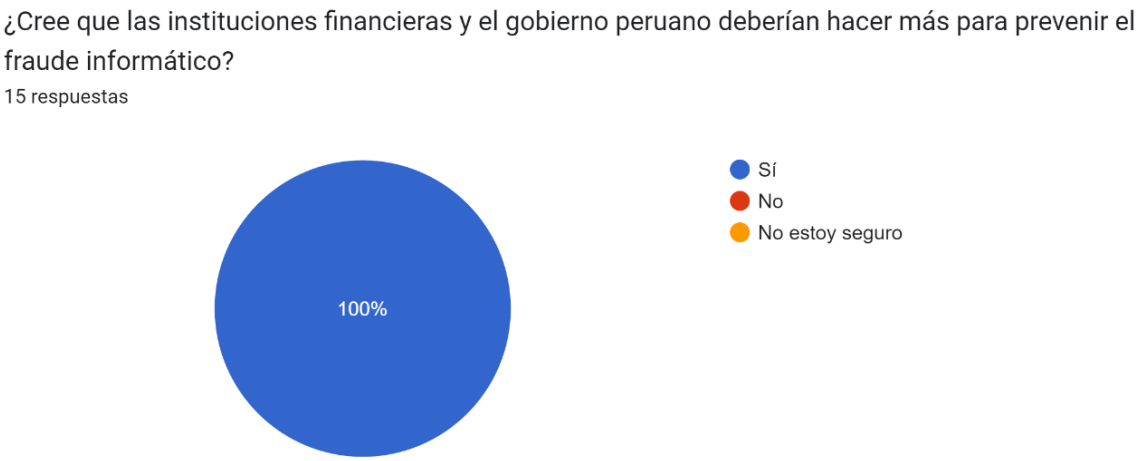


Figura 5

Fuente: Elaboración de los autores

De la figura 5, que representa la siguiente pregunta: ¿Cree que las instituciones financieras y el gobierno peruano deberían hacer más para prevenir el fraude informático?

Se realizó una encuesta utilizando Google Formularios a 15 ciudadanos peruanos, se compartió el cuestionario mediante redes sociales, en la cual se obtuvo el siguiente resultado unánime: las 15 personas encuestadas refirieron que las instituciones financieras y el gobierno peruano SI deberían hacer mas esfuerzo para prevenir el fraude informático, siendo una respuesta unánime equivalente al 100% de encuestados.

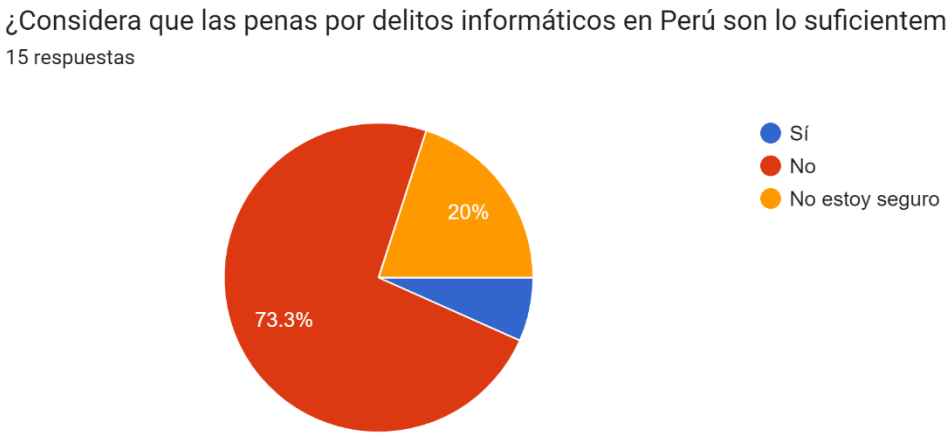


Figura 6

Fuente: Elaboración de los autores

De la figura 6, que representa la siguiente pregunta: ¿Considera que las penas por delitos informáticos en Perú son lo suficientemente duras?, se realizó una encuesta utilizando Google Formularios a 15 ciudadanos peruanos, se compartió el cuestionario mediante redes sociales, en la cual se obtuvo el siguiente resultado: 11 personas refirieron que no consideraban que las penas actuales para el delito de fraude informático son muy ínfimas este resultado equivalente al 73.3%, mientras que 3 personas equivalentes al 20% refirieron que no estaban seguros, por otro lado 1 persona dijo que si considera que las penas actuales son lo suficientemente duras, este último equivalente al 6.7% del total de encuestados.

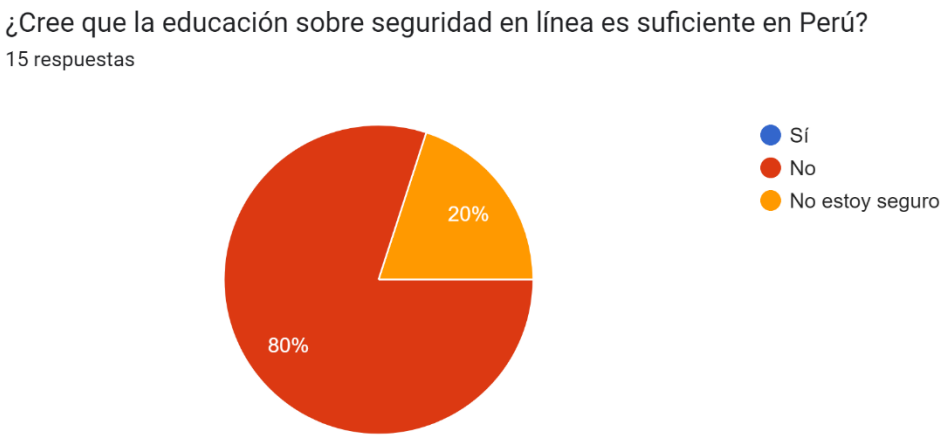


Figura 7

Fuente: Elaboración de los autores

De la figura 7, que representa la siguiente pregunta: ¿Cree que la educación sobre seguridad en línea es suficiente en Perú?

Se realizó una encuesta utilizando Google Formularios a 15 ciudadanos peruanos, se compartió el cuestionario mediante redes sociales, obteniéndose el siguiente resultado 12 personas (80%) respondieron que NO es suficiente la educación respecto a la seguridad en línea, mientras que 3 personas (20%) respondieron NO ESTOY SEGURO.

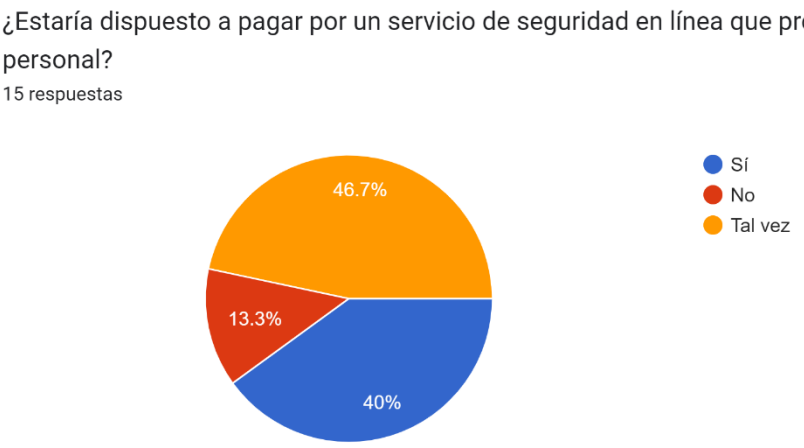


Figura 8

Fuente: Elaboración de los autores

De la figura 8, que representa la siguiente pregunta: ¿Estaría dispuesto a pagar por un servicio de seguridad en línea que proteja su información personal?, se realizó una encuesta utilizando Google Formularios a 15 ciudadanos peruanos, se compartió

el cuestionario mediante redes sociales, en la cual se obtuvo el siguiente resultado: 7 personas refirieron que tal vez estarían dispuestos a pagar por la seguridad informática, equivalente al 46.7%, 6 personas confirmaron que si están dispuestos a pagar lo cual equivale al 40%, y por ultimo 2 personas mencionaron que no estarían dispuestas a pagar por la seguridad informática equivalente al 13.3%.

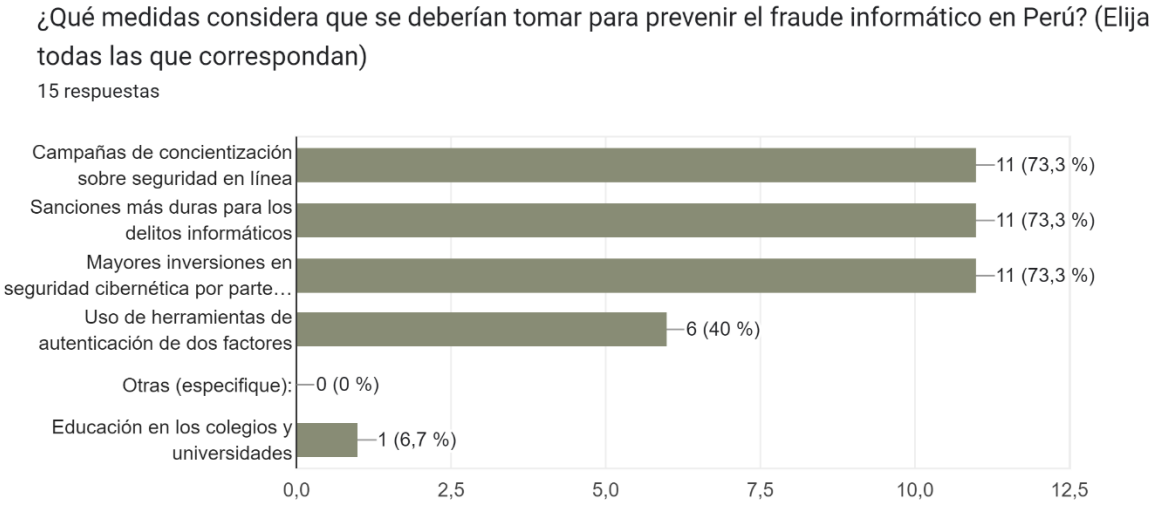


Figura 9

Fuente: Elaboración de los autores

De la figura 9, que representa la siguiente pregunta: ¿Qué medidas considera que se deberían tomar para prevenir el fraude informático en Perú?

Se realizó una encuesta utilizando Google Formularios a 15 ciudadanos peruanos, se compartió el cuestionario mediante redes sociales, siendo la pregunta numero 9 con alternativas de respuesta múltiple, obteniéndose el siguiente resultado:

- 11 personas sugirieron que se implemente Campañas de concientización sobre seguridad en línea.
- 11 personas sugirieron sanciones más duras para los delitos informáticos.
- 11 personas sugirieron que se deben generar mayores inversiones en seguridad cibernética por parte del gobierno y empresas privadas.

- 6 personas sugirieron la implementación del uso de herramientas de autenticación de dos factores.
- 1 persona considero la Educación en los colegios y universidades.

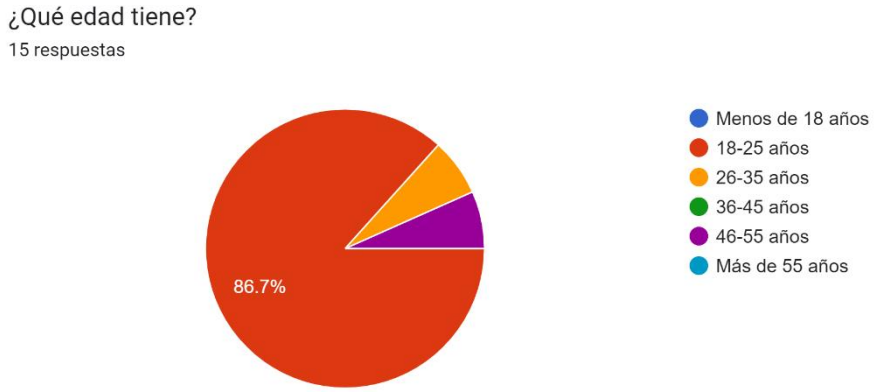


Figura 10

Fuente: Elaboración de los autores

De la figura 10, que representa la siguiente pregunta: ¿Qué edad tiene?, se realizó una encuesta utilizando Google Formularios a 15 ciudadanos peruanos, se compartió el cuestionario mediante redes sociales, en la cual se obtuvo el siguiente resultado: Del total de encuestados 13 personas indicaron que tienen de 18 a 25 años de edad siendo esto equivalente al 86.7%, 1 persona indico tener de 26 a 35 años de edad y 1 persona de 46 a 55 años de edad equivalente a 6.7%.

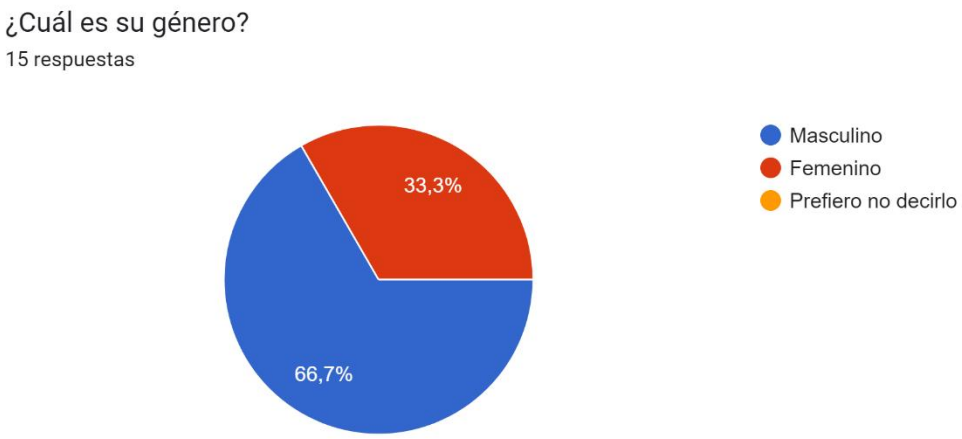


Figura 11

Fuente: Elaboración de los autores

De la figura 11, que representa la siguiente pregunta: ¿Cuál es su género?

Se realizó una encuesta utilizando Google Formularios a 15 ciudadanos peruanos, se compartió el cuestionario mediante redes sociales, obteniéndose el siguiente resultado 10 personas del género masculino (66.7%) respondieron la encuesta, frente a 5 personas del género femenino (33.3%).

Obtener datos acerca de las disparidades y coincidencias en las vivencias y enfoques de las personas según su género es fundamental. Este tipo de información puede ser significativa para la investigación en diversas áreas. Agregar preguntas sobre el género en la encuesta podría propicia un mayor conocimiento sobre las desigualdades de género y a su vez, fomentar la igualdad de género en la sociedad.

5.3 . Discusión y contrastación teórica de los hallazgos

EL PROBLEMA	**General:** ¿Se encuentra adecuada a nuestra realidad tecnológica actual la tipificación del delito de Fraude informático regulado en el artículo 8 de la Ley N° 30096 – Ley de Delitos Informáticos? **Especificas:** 1. ¿Se puede prevenir las actuales conductas ilícitas del ámbito tecnológico mediante una adecuada reforma a la legislación de delitos informáticos en el Perú? 2 ¿La Ley N°30096, "Ley de Delitos Informáticos" cuenta con un tratamiento especial acorde al convenio de Budapest? 3. ¿Cuáles son los factores que inciden en la comisión del delito de fraude informático en la población peruana a raíz de la aplicación de las nuevas tecnologías y su regulación en la Ley N° 30096?
OBJETIVO	**General:** Determinar si se encuentra adecuada a nuestra realidad tecnológica actual la tipificación del delito de Fraude Informático regulado en el artículo 8 de la Ley N° 30096 – Ley de Delitos Informáticos. **Especificas:** 1.Señalar sí es posible prevenir las actuales conductas ilícitas del ámbito tecnológico mediante una adecuada reforma a la legislación de delitos informáticos en el Perú. 2. Determinar si, la Ley N°30096, "Ley de Delitos Informáticos" cuenta con un tratamiento acorde al convenio de Budapest.

	3.Determinar los factores que inciden en la comisión del delito de fraude informático en la población peruana.
HIPOTESIS	**General:** La actual tipificación del fraude informático regulado en el artículo 8 de la Ley N°30096 – Ley de Delitos Informáticos no se encuentra adecuada a nuestra realidad tecnológica actual. **Especificas:** 1. No es posible prevenir las actuales conductas ilícitas del ámbito tecnológico únicamente mediante una adecuada reforma a la legislación de Delitos Informáticos "Ley N° 30096". 2. La Ley N°30096, "Ley de Delitos Informáticos" no cuenta con un tratamiento especial acorde al convenio de Budapest. 3.La falta de conocimiento de los ciudadanos sobre las nuevas tecnologías y la imprecisión normativa son factores que inciden en la comisión de fraude informático.

Al respecto del Planteamiento del Problema, Objetivos y la Hipótesis, respectivamente, se logró comprobar que, el artículo 8 de la Ley N° 30096, que regula el delito de fraude informático, tiene una interpretación vaga e imprecisa que se desvincula de la realidad tecnológica actual. Además, que este no incluye tipos penales específicos por fraude informático. Los datos estadísticos de la División de Investigación de Delitos de Alta Tecnología (DIVINDAT) muestran un aumento en los informes de nuevas formas de fraude informático, incluidos el Phishing y el Carding, que son los más frecuentes en Perú. Luego de revisar la Ley peruana en materia de delitos informáticos, se determina que un cambio legislativo por sí solo no es capaz de prevenir por completo las conductas tecnológicas ilegales, considerándose que esta no es la mejor manera de prevenir el fraude informático.

Así mismo, también se encontró deficiencias en la legislación peruana sobre delitos informáticos, entre ellas la falta de partes específicas de tratamiento y la falta de definiciones precisas. Estas omisiones dificultan la comprensión y aplicación adecuada de la ley, especialmente si se tiene en cuenta la trascendencia tecnológica de los delitos informáticos. De acuerdo con la realidad tecnológica actual y el Convenio de Budapest, que fue ratificado por Perú en marzo de 2019, consideramos que la ley Nº30096 debe incluir definiciones precisas, distinciones entre delitos informáticos y delitos computacionales, también la ley debería incluir procedimiento separado para investigar e identificar a los autores de delitos informáticos por su complejidad.

Finalmente, el desconocimiento de los ciudadanos sobre las nuevas tecnologías y la falta de precisión en las normas son factores que contribuyen a la comisión del fraude informático. Estos factores dificultan la tipificación adecuada de los delitos en la legislación vigente y contribuyen a que existan más víctimas.

Recomendamos promover campañas de sensibilización y educación para fomentar el uso responsable de la tecnología y la protección de la información personal. Para disminuir el aumento de los delitos informáticos entre los ciudadanos peruanos, es fundamental mejorar la educación sobre el uso seguro de las tecnologías de la información y la comunicación.

5.4 Propuesta legislativa

Motivación de la propuesta legislativa

El avance de la tecnología ha desencadenado una serie de actos legales e ilegales y hoy en día la gran mayoría de personas utiliza los medios tecnológicos para comunicarse, trabajar, resolver problemas financieros y es en esta situación donde los crackers, que son personas expertas en informática las cuales se encargan de infiltrarse en sistemas informáticos o utilizando los medios tecnológicos en forma engañosa, dañando la seguridad y obteniendo información para venderla u/o cometer similares delitos con la información obtenida.

El delito de Fraude informático regulado en el artículo 8 de la Ley N°30096, Ley de delitos informáticos, se encuentra descrito de forma imprecisa, generando así confusión en los operadores del derecho y en consecuencia muchas veces se cae en impunidad, para el presente trabajo de investigación, resulta importante incluir las nuevas modalidades más denunciadas en el Perú que según la DIVINDAT son; el Phishing y Carding.

Entonces en beneficio de la persecución del delito se propone la inclusión al texto normativo vigente de las nuevas modalidades y con esta inclusión logramos una mejor tipificación de los hechos denunciados en nuestro país.

Desarrollo de la propuesta legislativa:

Proyecto de Ley N° …….

PROPUESTA LEGISLATIVA QUE INCORPORA EL ART. 8-A 8-B EN LA LEY N° 30096 "LEY DE DELITOS INFORMÁTICOS" PARA PENALIZAR LA MODALIDAD DE PHISHING Y CARDING EN EL DELITO DE FRAUDE INFORMÁTICO

Los Bachilleres de la Escuela Profesional de Derecho de la Universidad Andina del Cusco, haciendo ejercicio del Derecho de iniciativa Legislativa que confiere el Articulo N. ° 107 de la Constitución Política del Perú, y conforme a lo establecido en el Artículo 75° y 76° del Reglamento del Congreso de la República, presentan la siguiente propuesta legislativa.

FORMULA LEGAL

LEY QUE INCORPORA EL ART. 8-A Y 8-B EN LA LEY 30096 "LEY DE DELITOS INFORMÁTICOS" PARA PENALIZAR LA MODALIDAD DE PHISHING Y CARDING EN EL DELITO DE FRAUDE INFORMÁTICO

Artículo 1.- Objeto

Incorporación del art. 8-A y 8-B en la Ley 30096 "Ley de delitos informáticos, para penalizar la modalidad de phishing y carding en el delito de fraude informático.

Artículo 2.- Modificatoria

Modifíquese e incorpórese en el artículo 8 de la Ley N°300096 "Ley Delitos Informáticos".

Artículo 8. Fraude informático

El que, a través de las tecnologías de la información o de la comunicación, procura para sí o para otro un provecho ilícito en perjuicio de tercero mediante el diseño, introducción, alteración, borrado, supresión, clonación de datos informáticos o cualquier interferencia o manipulación en el funcionamiento de un sistema informático, será reprimido con una

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

Incorpórese:

Artículo 8-A.- Phishing

El que, haciendo uso de las tecnologías de información o de la comunicación diseña sistemas informáticos engañosos valiéndose de su pericia tecnológica a través del envío de correos electrónicos o mensajes de texto que suplantan la identidad de compañías u organismos con la finalidad de solicitar información personal y/o bancaria del usuario, será reprimido con pena privativa de libertad no menor de cuatro años ni mayor de 8 años y con ochenta a ciento sesenta días multa.

Articulo 8-B.- Carding

El que, haciendo uso de las tecnologías de información obtiene los datos de una tarjeta bancaria con la finalidad de realizar compras online, suplantando la identidad del usuario, será reprimido con pena privativa de libertad, no menor de cuatro años ni mayor de 8 años y con sesenta a ciento cincuenta días multa.

DISPOCISIONES COMPLEMENTARIAS

Primera: Adecuación de la normativa, La presente ley estará en concordancia con la normativa nacional, en un plazo no mayor de 60 días calendarios.

Segundo: Vigencia La presente ley entrara en vigencia al día siguiente de su publicación. Comuníquese al Señor presidente de la Republica para su promulgación.

CONCLUSIONES DE LA PROPUESTA

La inclusión de los métodos de fraude electrónico conocidos como Phishing y Carding ayuda en la capacidad de identificar nuevos métodos de fraude informático que van surgiendo, más aún con el avance de la tecnología en la actual situación de pandemia, pues se prevé que esta incorporación facilitará la identificación del autor y se podrá delimitar de manera más precisa el acto ilícito.

ANÁLISIS COSTO BENEFICIO

La propuesta no contempla gastos estatales; más bien, llama a cambiar las leyes para mejorar la persecución penal y aplicar castigos de acuerdo con los delitos cometidos. Por ello, se intenta añadir el Phishing y Carding como nuevas modalidades delictivas al ya existente fraude informático, que conlleva una dura sanción para cualquier conducta ilegal de robo informático.

CONCLUSIONES

PRIMERA.- Del presente trabajo de investigación se concluye que, la tipificación del delito de Fraude Informático regulado en el artículo 8 de la Ley N° 30096 "Ley de delitos informáticos" resulta genérica e imprecisa, motivo por el cual no se encuentra adecuada a la realidad tecnológica actual, teniendo en cuenta que desde el año 2014, año en el cual dicha ley sufrió su última modificación, no se especificó modalidades delictivas para el delito de fraude informático; se consultó los datos estadísticos de la División de Investigación de Delitos de Alta Tecnología (DIVINDAT), los cuales dieron como resultado, que en los últimos años se incrementó las denuncias de nuevas modalidades de Fraude Informático denominadas con el nombre de Phishing y Carding, las cuales resultaron ser las modalidades más usuales en el Perú. Consideramos que es fundamental que la ley de Delitos Informáticos Ley Nº 30096 necesita una redacción más precisa, para de esta manera se pueda garantizar una mejor identificación y persecución de los delitos informáticos, cumpliendo con la finalidad persecutora de la ley, y que las nuevas modalidades de fraude informático no queden impunes. Así mismo es necesario que las nuevas modalidades de fraude informático sean abarcadas dentro del tipo penal de forma más específica, cumplimento con el principio de Taxatividad de la Ley, y teniendo por finalidad contar con un texto normativo moderno y adecuado a la realidad tecnológica actual.

SEGUNDA. – Una reforma a la legislación de delitos informáticos en el Perú no puede prevenir comportamientos ilegales en el ámbito tecnológico, a pesar que su última modificatoria se remonta 9 años atrás, por la Ley 30171 en el año 2014. Inicialmente se evaluó plantear una modificatoria y con el desarrollo del trabajo de investigación se concluyó que para reducir los índices de criminalidad en el fraude informático la vía más eficiente para prevenir que se siga incrementando la comisión de este delito no es la modificación del artículo 8, dado que consideramos que el aumento de las penas y regulación de delitos no es la vía más idónea para la prevención, el aumento de los delitos, las penas y las prisiones resultaron ser ineficientes en el tiempo, ya que en algunos países ha resultado más costoso y poco efectivo en la prevención, readaptación, reinserción o resocialización de los transgresores de la ley penal, En nuestra opinión la mejor

alternativa para la reducción de índices de criminalidad es la inversión en educación tecnológica nacional.

TERCERA.- Tras el análisis, concluimos que, en marzo del año 2019 el Perú ratificó mediante Decreto supremo la aprobación del Convenio de Budapest y teniendo en cuenta que en el mencionado convenio adopta diferentes aspectos relevantes para estos delitos, como mayor definición, mayor amplitud. En la ley peruana no existe definiciones exactas, así mismo no esta incluido la importante diferenciación entre delito informático y delito computacional, estas omisiones generan deficiencia en la comprensión y tratamiento de la Ley, en el mismo sentido la ley no comprende la parte procesal especifica que debería de tener debido a la relevancia tecnológica de los delitos informáticos, estos no deben ser tratados con las mismas técnicas de investigación de los delitos comunes, sino que deberían de tener un procedimiento especial, esto debido a que son más complicados de investigar y poder identificar al sujeto activo. Se necesita incluir dentro del texto normativo las definiciones exactas, la diferenciación de los delitos comunes, especificación y un tratamiento especial de los delitos informáticos acorde a la realidad tecnológica actual y al convenio de Budapest.

CUARTA.- Finalmente concluimos que la falta de conocimiento de los ciudadanos sobre las nuevas tecnologías y la imprecisión normativa son los factores más predominantes que inciden en la comisión de fraude informático, debido a que las nuevas modalidades son cada vez más ingeniosas y su desconocimiento permite que existan más víctimas, así mismo la imprecisión normativa no permite una correcta tipificación de los tipos penales descritos en la Ley. Es necesario promover campañas educativas y de concientización para fomentar el uso responsable de la tecnología y la protección de la información personal. Es necesario mejorar la educación en el uso seguro de las tecnologías de la información y la comunicación, de esta manera se logrará reducir el incremento del delito en la población peruana.

RECOMENDACIONES O SUGERENCIAS

PRIMERA.- Como primera y principal recomendación, recomendamos una redacción más precisa del artículo 8 de la Ley N°30096, "Ley de Delitos Informáticos" en la cual se deba abarcar las modalidades de Phishing y Carding por ser de las más denunciadas en nuestro país, mediante un proyecto de modificación legislativa a dicho artículo, la cual permita una mayor adaptabilidad a las nuevas modalidades de fraude informático, evitando así la impunidad de los mismos.

SEGUNDA.- Como recomendación, sería conveniente que las autoridades peruanas establezcan convenios con especialistas en tecnología y ciberseguridad, para la educación y capacitación de la Policía Nacional, del Ministerio Publico y Jueces, para mejorar la identificación y el enjuiciamiento de los delitos informáticos. Se deben implementar campañas educativas y de concientización para promover el uso responsable de la tecnología y la protección de la información personal. También es esencial que el Estado tenga los recursos y la voluntad política necesarios para prevenir la ciberdelincuencia y garantizar la seguridad en línea.

TERCERA.-Es recomendable que se lleve a cabo una revisión de la legislación actual del Perú en relación con los delitos informáticos porque consideramos crucial la incorporación de definiciones precisas y claras que diferencien los delitos informáticos de los delitos computacionales. Además, se debe evaluar la creación de una parte procesal especifica en la ley de delitos informáticos, parte procesal que si tienen otras leyes especiales como la ley de lavado de activos o la ley de crimen organizado. De igual manera resulta importante cumplir con los estándares establecidos en el Convenio de Budapest, ya que Perú lo ratificó en marzo de 2019. Esto ayudará a mejorar la comprensión y la atención de los delitos informáticos de acuerdo con las normas internacionales.

CUARTA.-Con la finalidad de protección a la población peruana recomendamos realizar campañas de concientización y difusión dirigidas a la población para que estén más informados sobre las nuevas tecnologías y los riesgos asociados al uso de las mismas, como es por ejemplo disponer que las empresas de telefonía constantemente emitan mensajes preventivos de alertas de precaución de las nuevas modalidades, también se

debería establecer medidas de prevención y detección temprana de posibles casos de fraude informático, a través de la implementación de políticas de seguridad informática en empresas y organizaciones, así mismo para la problemática de imprecisión normativa que exista una mejor coordinación entre el legislador y los operadores del derecho.

BIBLIOGRAFÍA

Azaola Calderón, L. (2010). Delitos Informaticos y Derecho Penal. UBIJUS.

Bramont- Arias Torres, L. (1997). El Delito Informático. En L. Bramont- Arias Torres, *El Delito Informático* (pág. 73). Lima: Editorial de la Pontificia Universidad Catolica del Perú.

Chungata Cabrera, A. M. (2015). *UCUENCA*. Obtenido de http://dspace.ucuenca.edu.ec/handle/123456789/21321

Congreso de España . (10 de 1995). Codigo Penal Español. Madrid.

Exitosa Noticias. (6 de agosto de 2021). *Facebook*. Obtenido de Facebook: https://www.facebook.com/CuscoExitosa/photos/a.102801104836983/3586210259216555/

Fernandez, Y. (2 de Junio de 2020). *Xataka*. Obtenido de https://www.xataka.com/basics/malware-que-que-tipos-hay-como-evitarlos

Fernandez, Y. (2 de Junio de 2020). *Xataka Basics*. Obtenido de https://www.xataka.com/basics/malware-que-que-tipos-hay-como-evitarlos

Gilberto, C. R. (2018). *EL DELITO CONTRA DATOS Y SISTEMAS INFORMÁTICOS EN EL DERECHO*. Lima.

Guerrero Argote, C. (2018). Análisis sobre el proceso de implementación del Convenio de Ciberdelincuencia impacto en el corto, mediano y largo plazo. Lima: Derechos Digitales América Latina.

Huamán Cruz, M. Y. (2020). LOS DELITOS INFORMATICOS EN PERÚ Y LA SUSCRIPCIÓN DEL CONVENIO DE BUDAPEST. Cusco.

Ley N° 30171. (14 de Marzo de 2014). Ley N° 30171 "Ley que modifica la Ley 30096, Ley de los Delitos Informaticos".

Ley N°30096 "Ley de Delitos Informáticos". (22 de Octubre de 2013). Obtenido de https://busquedas.elperuano.pe/normaslegales/ley-de-delitos-informaticos-ley-n-30096-1003117-1/

Marchena Gomez, M. (2001). El sabotaje informático: entre los delitos de daños y desordenes públicos. Madrid: Cuadernos de Derecho Judicial .

Maribel, M. (27 de diciembre de 2020). *La Republica.pe*. Obtenido de La Republica.pe: https://larepublica.pe/sociedad/2020/12/27/aumentan-los-fraudes-informaticos-en-cusco-lrsd/

Mata Barranco, N. (2009). El delito de daños informativos: una tipificacion defectuosa . Madrid: Estudios penales y criminologicos.

Morant Vidal, J. (2003). Protección penal de la intimidad frente a las nuevas tecnologías. Valencia : Ractica de Derecho.

Peña Cabrera Freyre, A. R. (s.f.). Los delitos informaticos: el uso de instrumentos digitales en las redes infromaticas y en el ciberespacio. Gaceta Penal & Procesal Penal N°76.

Pérez López, J. (2019). Delitos regulados en leyes penales especiales . En J. Pérez López. Lima: Gaceta Juridica .

Pichiua, S. (12 de febrero de 2023). *Andina agencia peruana de noticias*. Obtenido de https://andina.pe/agencia/noticia-cuidado-los-fraudes-informaticos-estas-son-las-modalidades-mas-denunciadas-peru-928425.aspx%22

Prías Bernal, J. C. (2016). Aproximación al estudio de los delitos informáticos. En *Derecho Penal Contemporáneo Revista Internacional N° 17* (pág. 30).

RAE. (2022). *Fraude*. Obtenido de REAL ACADEMIA ESPAÑOLA: https://dle.rae.es/fraude

Rinaldi, Paola. (27 de abril de 2017). *Le-vpn.com*. Obtenido de Le-vpn.com: https://www.le-vpn.com/es/delito-cibernetico-origen-evolucion/

Ruiz Cruz, C. A. (2016). Analisis de los Delitos Informaticos y su Violacion de los Derechos Constitucionales de los ciudadanos . *Tesis* . Loja, Ecuador : Universidad Nacional de Loja.

Salinas Siccha, R. (2013). *Derecho Penal, Parte Especial.* Lima: Grijley.

Schwartzman, H. (1993). *Ethnography in organizations.* California : Sage.

TerrerosVillavicencio, F. (2006). Derecho Penal Parte General. En F. Villavicencio Terreros, *Derecho Penal Parte General* (pág. 90). Editora y Librería Jurídica Grijley.

Zorrila Tocto, ,. K. (2018). Tesis para optar por el titulo profesional de abogado. *INCONSISTENCIAS Y AMBIGÜEDADES EN LA LEY DE DELITOS INFORMATICOS LEY N°30096 Y SU MODIFICATORIA LEY N°30171*. Ancash, Huaraz, Peru.

LINKOGRAFIA

Azaola Calderón, L. (2010). Delitos Informaticos y Derecho Penal. UBIJUS.

Bramont- Arias Torres, L. (1997). El Delito Informático. En L. Bramont- Arias Torres, *El Delito Informático* (pág. 73). Lima: Editorial de la Pontificia Universidad Catolica del Perú.

Chungata Cabrera, A. M. (2015). *UCUENCA.* Obtenido de http://dspace.ucuenca.edu.ec/handle/123456789/21321

Congreso de España . (10 de 1995). Codigo Penal Español. Madrid.

Exitosa Noticias. (6 de agosto de 2021). *Facebook*. Obtenido de Facebook: https://www.facebook.com/CuscoExitosa/photos/a.102801104836983/358621025921655/

Fernandez, Y. (2 de Junio de 2020). *Xataka.* Obtenido de https://www.xataka.com/basics/malware-que-que-tipos-hay-como-evitarlos

Fernandez, Y. (2 de Junio de 2020). *Xataka Basics*. Obtenido de https://www.xataka.com/basics/malware-que-que-tipos-hay-como-evitarlos

Gilberto, C. R. (2018). *EL DELITO CONTRA DATOS Y SISTEMAS INFORMÁTICOS EN EL DERECHO*. Lima.

Guerrero Argote, C. (2018). Análisis sobre el proceso de implementación del Convenio de Ciberdelincuencia impacto en el corto, mediano y largo plazo. Lima: Derechos Digitales América Latina.

Huamán Cruz, M. Y. (2020). LOS DELITOS INFORMATICOS EN PERÚ Y LA SUSCRIPCIÓN DEL CONVENIO DE BUDAPEST. Cusco.

Ley N° 30171. (14 de Marzo de 2014). Ley N° 30171 "Ley que modifica la Ley 30096, Ley de los Delitos Informaticos".

Ley N°30096 "Ley de Delitos Informáticos". (22 de Octubre de 2013). Obtenido de https://busquedas.elperuano.pe/normaslegales/ley-de-delitos-informaticos-ley-n-30096-1003117-1/

Marchena Gomez, M. (2001). El sabotaje informático: entre los delitos de daños y desordenes públicos. Madrid: Cuadernos de Derecho Judicial .

Maribel, M. (27 de diciembre de 2020). *La Republica.pe*. Obtenido de La Republica.pe: https://larepublica.pe/sociedad/2020/12/27/aumentan-los-fraudes-informaticos-en-cusco-lrsd/

Mata Barranco, N. (2009). El delito de daños informativos: una tipificacion defectuosa . Madrid: Estudios penales y criminologicos.

Morant Vidal, J. (2003). Protección penal de la intimidad frente a las nuevas tecnologías. Valencia : Ractica de Derecho.

Peña Cabrera Freyre, A. R. (s.f.). Los delitos informaticos: el uso de instrumentos digitales en las redes infromaticas y en el ciberespacio. Gaceta Penal & Procesal Penal N°76.

Pérez López, J. (2019). Delitos regulados en leyes penales especiales . En J. Pérez López. Lima: Gaceta Juridica .

Pichiua, S. (12 de febrero de 2023). *Andina agencia peruana de noticias*. Obtenido de https://andina.pe/agencia/noticia-cuidado-los-fraudes-informaticos-estas-son-las-modalidades-mas-denunciadas-peru-928425.aspx%22

Prías Bernal, J. C. (2016). Aproximación al estudio de los delitos informáticos. En *Derecho Penal Contemporáneo Revista Internacional N° 17* (pág. 30).

RAE. (2022). *Fraude*. Obtenido de REAL ACADEMIA ESPAÑOLA: https://dle.rae.es/fraude

Rinaldi, Paola. (27 de abril de 2017). *Le-vpn.com*. Obtenido de Le-vpn.com: https://www.le-vpn.com/es/delito-cibernetico-origen-evolucion/

Ruiz Cruz, C. A. (2016). Analisis de los Delitos Informaticos y su Violacion de los Derechos Constitucionales de los ciudadanos . *Tesis* . Loja, Ecuador : Universidad Nacional de Loja.

Salinas Siccha, R. (2013). *Derecho Penal, Parte Especial.* Lima: Grijley.

Schwartzman, H. (1993). *Ethnography in organizations.* California : Sage.

TerrerosVillavicencio, F. (2006). Derecho Penal Parte General. En F. Villavicencio Terreros, *Derecho Penal Parte General* (pág. 90). Editora y Librería Jurídica Grijley.

Zorrila Tocto, ,. K. (2018). Tesis para optar por el titulo profesional de abogado. *INCONSISTENCIAS Y AMBIGÜEDADES EN LA LEY DE DELITOS INFORMATICOS LEY N°30096 Y SU MODIFICATORIA LEY N°30171*. Ancash, Huaraz, Peru.

LEGISLACIÓN

Budapest. (2001). Convenio sobre la Ciberdelincuencia.

Ley N°30096 "Ley de Delitos Informaticos". (22 de Octubre de 2013). Obtenido de https://busquedas.elperuano.pe/normaslegales/ley-de-delitos-informaticos-ley-n-30096-1003117-1/

Ley N° 30171. (14 de Marzo de 2014). Ley N° 30171 "Ley que modifica la Ley 30096, Ley de los Delitos Informaticos".

ANEXOS

Matriz de consistencia

TITULO: LA INCIDENCIA DE LAS NUEVAS TECNOLOGÍAS EN EL DELITO DE FRAUDE INFORMÁTICO Y SU APLICACIÓN EN LA LEY N° 30096 EN EL PERÚ"

EL PROBLEMA	OBJETIVOS	HIPÓTESIS	CATEGORIAS DE ESTUDIO	METODOLOGÍA
General: ¿Se encuentra adecuada a nuestra realidad tecnológica actual la tipificación del delito de Fraude informático regulado en el artículo 8 de la Ley N° 30096 – Ley de Delitos Informáticos?	**General:** Determinar si se encuentra adecuada a nuestra realidad tecnológica actual la tipificación del delito de Fraude Informático regulado en el artículo 8 de la Ley N° 30096 – Ley de Delitos Informáticos	**General:** La actual tipificación del fraude informático regulado en el artículo 8 de la Ley N°30096 – Ley de Delitos Informáticos no se encuentra adecuada a nuestra realidad tecnológica actual.	– Nuevas tecnologías: • impacto en el delito de fraude informático • evolución • tendencias. – Ley peruana de delitos informáticos (Ley N° 30096): antecedentes • Contenido • alcance y aplicación en casos de fraude informático.	**Diseño Metodológico** **Tipo** – Dogmático Propositivo **Enfoque** - Cualitativo **Diseño Contextual** La investigación a desarrollar tendrá un diseño no experimental, descriptivo, transversal ya que no habrá manipulación de variables, sólo se describirán los hechos del fenómeno

Problemas Específicos 1.¿Se puede prevenir las actuales conductas ilícitas del ámbito tecnológico mediante una adecuada reforma a la legislación de delitos informáticos en el Perú? 2 ¿La Ley N°30096, "Ley de Delitos Informáticos" cuenta con un tratamiento especial acorde al convenio de Budapest? 3.¿Cuáles son los factores que inciden en la comisión del	**Objetivos Específicos** 1.Señalar sí es posible prevenir las actuales conductas ilícitas del ámbito tecnológico mediante una adecuada reforma a la legislación de delitos informáticos en el Perú. 2. Determinar si, la Ley N°30096, "Ley de Delitos Informáticos" cuenta con un tratamiento acorde al convenio de Budapest	**Hipótesis especificas** 1. No es posible prevenir las actuales conductas ilícitas del ámbito tecnológico únicamente mediante una adecuada reforma a la legislación de Delitos Informáticos "Ley N° 30096". 2. La Ley N°30096, "Ley de Delitos Informáticos" no cuenta con un tratamiento especial acorde al convenio de Budapest.	– Ciberseguridad: • Concepto • medidas de prevención y detección de fraude informático • gestión de riesgos y buenas prácticas. – Casos de fraude informático en Perú: • análisis de casos y estadísticas relevantes • consecuencias y sanciones. – Perspectiva comparada: • Análisis comparativo del marco legal y	observado y la información se levantará en un solo espacio de tiempo Para la realización del análisis, se consultará leyes, normas legales, libros jurídicos, trabajos científicos referentes a la problemática del fraude informático. Asimismo, se identificarán propuestas de reformas al artículo 8 de la Ley de Delitos Informáticos adecuadas a la nueva realidad tecnológica.

delito de fraude informático en la población peruana a raíz de la aplicación de las nuevas tecnologías y su regulación en la Ley N° 30096?	3.Determinar los factores que inciden en la comisión del delito de fraude informático en la población peruana.	3.La falta de conocimiento de los ciudadanos sobre las nuevas tecnologías y la imprecisión normativa son factores que inciden en la comisión de fraude informático.	casos relevantes en otros países de la región o del mundo. – Propuestas de mejora: • recomendaciones para mejorar la prevención • detección y sanción del fraude informático en el Perú • Incluyendo cambios en la legislación	

			• Prácticas de ciberseguridad.	

Modelo de encuesta realizada a ciudadanos, mediante google formularios

Percepción ciudadana sobre el fraude informático en el Perú

1. Lea cuidadosamente cada pregunta y seleccione la opción que mejor refleje su opinión o experiencia en relación al fraude informático.
2. Asegúrese de responder todas las preguntas.
3. Sus respuestas son confidenciales y solo se utilizarán con fines de investigación académica.
4. La encuesta tomará aproximadamente 10 minutos en completarse.
5. Gracias por su colaboración.

Correo electrónico *

Correo electrónico válido

Este formulario recopila correos electrónicos. Cambiar la configuración

¿Alguna vez ha sido víctima de fraude informático? *

- Si
- No

Si respondió Sí en la pregunta anterior, ¿puede describir brevemente qué tipo de fraude sufrió?

Texto de respuesta largo

*

¿Ha tomado medidas de seguridad para evitar ser víctima de fraude informático? (Elija todas las que correspondan)

- [ ] Uso de software antivirus
- [ ] Uso de contraseñas seguras
- [ ] Actualización de software y sistemas operativos
- [ ] No compartir información personal en línea
- [ ] No abrir correos electrónicos de remitentes desconocidos
- [ ] Otro (especifique)
- [ ] Otra...

¿En que ciudad reside actualmente? *

Texto de respuesta breve

¿Cree que las instituciones financieras y el gobierno peruano deberían hacer más para prevenir el fraude informático? *

- Sí
- No
- No estoy seguro

¿Considera que las penas por delitos informáticos en Perú son lo suficientemente duras? *

- Sí
- No
- No estoy seguro

¿Cree que la educación sobre seguridad en línea es suficiente en Perú? *

- Sí
- No
- No estoy seguro

¿Estaría dispuesto a pagar por un servicio de seguridad en línea que proteja su información personal? *

- Sí
- No

¿Cuál es su género? *

- Masculino
- Femenino
- Prefiero no decirlo

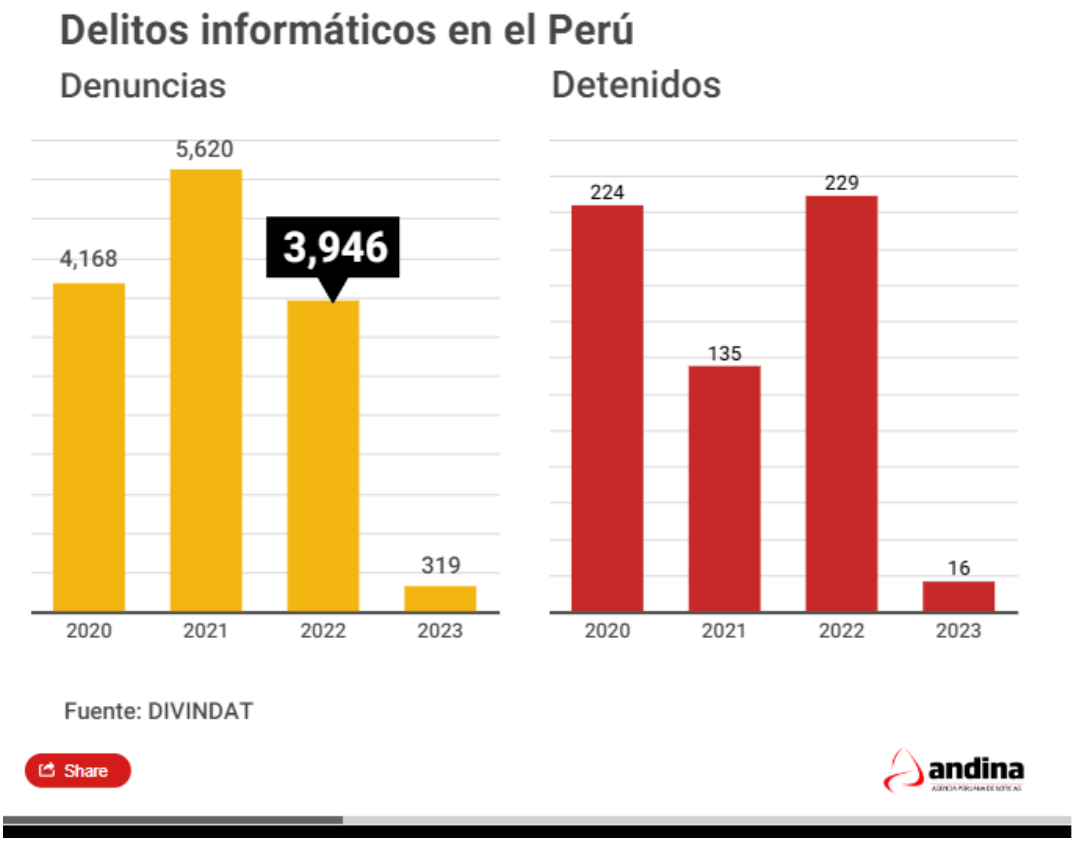
Cuadro de respuestas de formulario

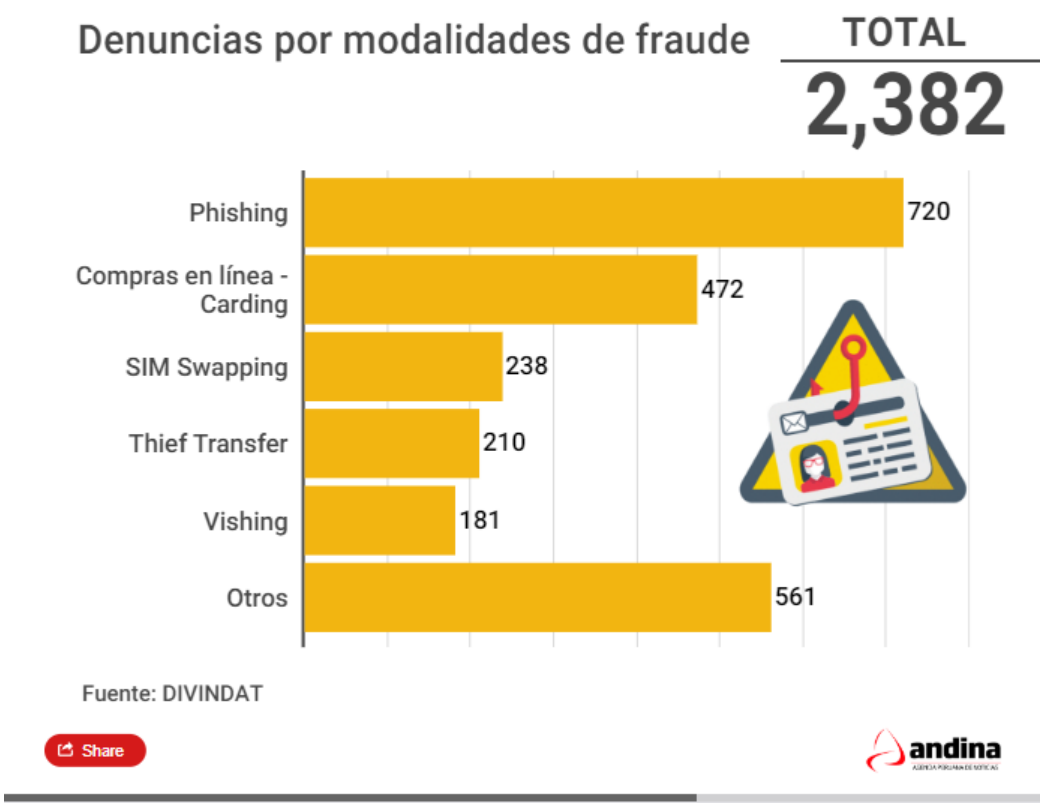
Marca temporal	Dirección de correo elec	¿Alguna vez ha sido víc	Si respondió Sí en la pr	¿Ha tomado medidas de	¿En que ciudad reside a
14/05/2023 0:28:57	alme201608@gmail.com	No		Uso de software antivirus	Cusco
14/05/2023 0:29:20	rc3carlos@gmail.com	Si	Compra de accesorios pa	Uso de contraseñas segu	Cusco
14/05/2023 0:34:34	015200736E@uandina.ec	Si	Robo por aplicativo	No compartir información	Cusco
14/05/2023 0:40:26	dennis_sckizizar@hotmai	No	.	Uso de contraseñas segu	cusco
14/05/2023 0:43:05	ferobh8@gmail.com	Si	Me hackearon la informac	Uso de contraseñas segu	Cusco
14/05/2023 0:57:39	ferloaso.doizasa.@gmail.	Si	De antivirus	Uso de software antivirus	Cusco
14/05/2023 1:19:21	davalos.arian@gmail.com	No		Uso de software antivirus	Lima
14/05/2023 1:28:37	nvalenzuela361@gmail.c	No	Ninguno	Uso de software antivirus	Cusco
14/05/2023 7:12:51	moreanozarate@gmail.co	No		Uso de software antivirus	Cusco
14/05/2023 7:26:16	ingridfernandezcarrillo@g	No		Uso de contraseñas segu	Cusco
14/05/2023 8:51:27	cajigaskevinn@gmail.com	No	Me robaron dinero de mi t	Uso de software antivirus	Cusco
14/05/2023 21:36:29	skyzizar6@gmail.com	No		Uso de software antivirus	Trujillo
14/05/2023 21:44:59	stephanofox14@gmail.co	Si	Fraude por llamada	Uso de software antivirus	Cusco
14/05/2023 21:48:12	alexfarfanmora11@gmail.	No	No	Uso de software antivirus	Cusco
14/05/2023 21:48:40	richivalens09@gmail.com	No		Uso de software antivirus	Cusco

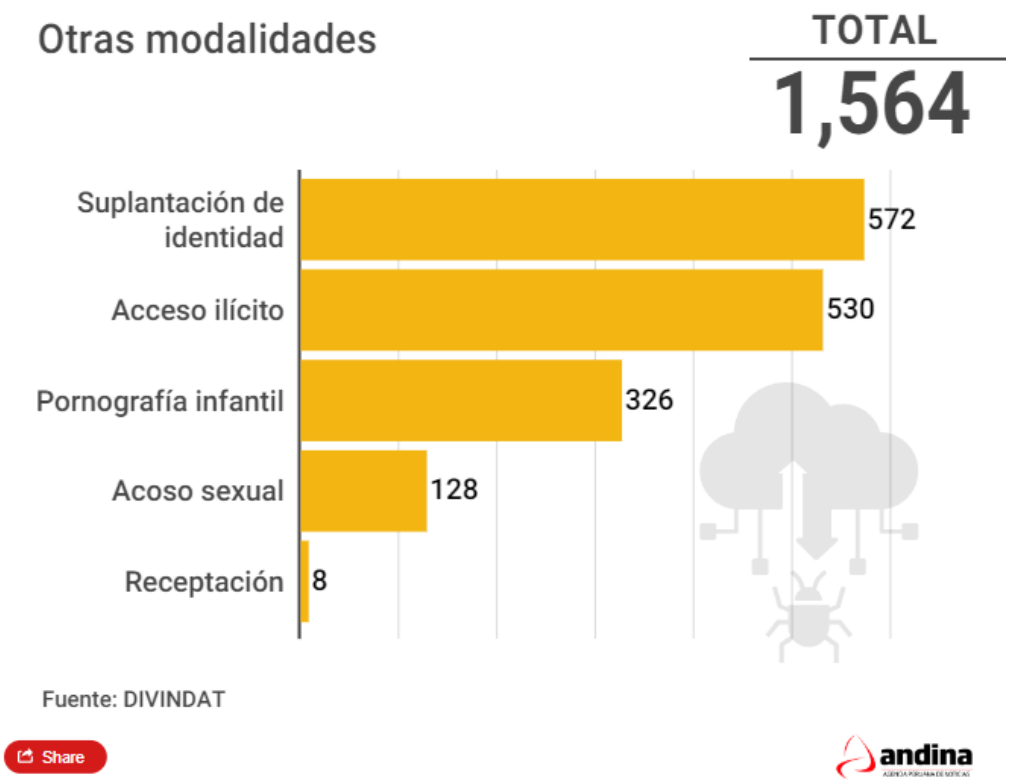
¿Cree que las institucio	¿Considera que las pen	¿Cree que la educación	¿Estaría dispuesto a pa	¿Qué medidas consider	¿Qué edad tiene?
Sí	No	No	Sí	Campañas de concientiza	18-25 años
Sí	No	No	No	Campañas de concientiza	18-25 años
Sí	No	No	Tal vez	Mayores inversiones en s	18-25 años
Sí	No	No	Tal vez	Campañas de concientiza	18-25 años
Sí	No	No	Tal vez	Campañas de concientiza	18-25 años
Sí	Sí	No	No	Sanciones más duras par	18-25 años
Sí	No	No	Tal vez	Campañas de concientiza	18-25 años
Sí	No	No	Sí	Campañas de concientiza	18-25 años
Sí	No	No	Sí	Campañas de concientiza	46-55 años
Sí	No	No	Tal vez	Campañas de concientiza	18-25 años
Sí	No estoy seguro	No estoy seguro	Tal vez	Campañas de concientiza	18-25 años
Sí	No estoy seguro	No	Sí	Campañas de concientiza	26-35 años
Sí	No estoy seguro	No estoy seguro	Sí	Sanciones más duras par	18-25 años
Sí	No	No	Tal vez	Campañas de concientiza	18-25 años
Sí	No	No estoy seguro	Sí	Sanciones más duras par	18-25 años

¿Cuál es su género?
Femenino
Masculino
Femenino
Masculino
Masculino
Masculino
Femenino
Masculino
Femenino
Femenino
Masculino
Masculino
Masculino
Masculino
Masculino

Datos obtenidos de pagina web andina, redactado por Sofia Pichiua.







Convenio sobre la Ciberdelincuencia de Budapest

DIARIO OFICIAL DEL BICENTENARIO

El Peruano

FUNDADO EL 22 DE OCTUBRE DE 1825 POR EL LIBERTADOR SIMÓN BOLÍVAR

AÑO DE LA LUCHA CONTRA LA CORRUPCIÓN Y LA IMPUNIDAD

Domingo 22 de setiembre de 2019

MINISTERIO DE RELACIONES EXTERIORES

Remite texto del "Convenio sobre la Ciberdelincuencia" y las declaraciones y reservas formuladas por la República del Perú al mencionado Convenio.

Serie de Tratados Europeos - N° 185

CONVENIO SOBRE LA CIBERDELINCUENCIA

Budapest, 23.XI.2001

NORMAS LEGALES

SEPARATA ESPECIAL

CONVENIO SOBRE LA CIBERDELINCUENCIA

Serie de Tratados Europeos - N° 185

Budapest, 23.XI.2001

Preámbulo

Los Estados miembros del Consejo de Europa y los demás Estados signatarios del presente Convenio,

Considerando que el objetivo del Consejo de Europa es lograr una unión más estrecha entre sus miembros;

Reconociendo el interés de intensificar la cooperación con los otros Estados Partes en el presente Convenio;

Convencidos de la necesidad de aplicar, con carácter prioritario, 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;

Conscientes de los profundos cambios provocados por la digitalización, la convergencia y la globalización continuas de las redes informáticas;

Preocupados por el riesgo de que las redes informáticas y la información electrónica sean utilizadas igualmente para cometer delitos y de que las pruebas relativas a dichos delitos sean almacenadas y transmitidas por medio de dichas redes;

Reconociendo la necesidad de cooperación entre los Estados y el sector privado en la lucha contra la ciberdelincuencia, así como la necesidad de proteger los intereses legítimos en la utilización y el desarrollo de las tecnologías de la información;

Estimando que la lucha efectiva contra la ciberdelincuencia requiere una cooperación internacional reforzada, rápida y eficaz en materia penal;

Convencidos de que el presente Convenio es necesario para prevenir los actos que pongan en peligro la confidencialidad, la integridad y la disponibilidad de los sistemas, redes y datos informáticos, así como el abuso de dichos sistemas, redes y datos, garantizando la tipificación como delito de dichos actos, tal como se definen en el presente Convenio, y la asunción de poderes suficientes para luchar eficazmente contra dichos delitos, facilitando su detección, investigación y sanción, tanto a nivel nacional como internacional, y estableciendo disposiciones materiales que permitan una cooperación internacional rápida y fiable;

Teniendo presente la necesidad de garantizar el debido equilibrio entre los intereses de la acción penal y el respeto de los derechos humanos fundamentales consagrados en el Convenio del Consejo de Europa para la Protección de los Derechos Humanos y de las Libertades Fundamentales (1950), el Pacto Internacional de Derechos Civiles y Políticos de las Naciones Unidas (1966) y otros tratados internacionales aplicables en materia de derechos humanos, que reafirman el derecho a defender la propia opinión sin interferencia, el derecho a la libertad de expresión, incluida la libertad de buscar, obtener y comunicar información e ideas de toda índole, sin consideración de fronteras, así como el respeto de la vida privada;

Conscientes igualmente del derecho a la protección de los datos personales, tal como se define, por ejemplo, en el Convenio de 1981 del Consejo de Europa para la protección de las personas con respecto al tratamiento informatizado de datos personales;

Teniendo presentes la Convención sobre los Derechos del Niño de las Naciones Unidas (1989) y el Convenio sobre las peores formas de trabajo infantil de la Organización Internacional del Trabajo (1999);

Teniendo en cuenta los convenios existentes del Consejo de Europa sobre cooperación en materia penal, así como otros tratados similares celebrados entre los Estados miembros del Consejo de Europa y otros Estados, y subrayando que el objeto del presente Convenio es completar dichos Convenios con el fin de incrementar la eficacia de las investigaciones y procedimientos penales relativos a los delitos relacionados con sistemas y datos informáticos, así como permitir la obtención de pruebas electrónicas de los delitos;

Congratulándose de las recientes iniciativas destinadas a mejorar el entendimiento y la cooperación internacionales en la lucha contra la delincuencia cibernética, y en particular las acciones organizadas por las Naciones Unidas, la OCDE, la Unión Europea y el G8;

Recordando las Recomendaciones del Comité de Ministros nº R (85) 10 relativa a la aplicación práctica del Convenio Europeo de Asistencia Judicial en Materia Penal en relación con las comisiones rogatorias para la vigilancia de las telecomunicaciones, nº R (88) 2 sobre medidas encaminadas a luchar contra la piratería en materia de propiedad intelectual y derechos afines, nº R (87) 15 relativa a la regulación de la utilización de datos de personales por la policía, nº R (95) 4 sobre la protección de los datos personales en el ámbito de los servicios de telecomunicaciones, con especial referencia a los servicios telefónicos, nº R (89) 9 sobre la delincuencia relacionada con la informática, que ofrece a los legisladores nacionales directrices para definir ciertos delitos informáticos, y nº R (95) 13 relativa a los problemas de procedimiento penal vinculados a la tecnología de la información;

Teniendo presente la Resolución nº 1, adoptada por los Ministros de Justicia europeos, en su XXI Conferencia (Praga, 10 y 11 de junio de 1997), que recomendaba al Comité de Ministros apoyar las actividades en relación con la ciberdelincuencia organizadas por el Comité Europeo para Problemas Criminales (CDPC) con el fin de aproximar las legislaciones penales nacionales y permitir la utilización de medios de investigación eficaces en materia de delitos informáticos, así como la Resolución nº 3, adoptada en la XXIII Conferencia de Ministros de Justicia europeos (Londres, 8 y 9 de junio de 2000), que exhortaba a las partes negociadoras a persistir en sus esfuerzos por encontrar soluciones que permitan al mayor número posible de Estados ser partes en el Convenio, y reconocía la necesidad de disponer de un mecanismo rápido y eficaz de cooperación internacional que tenga debidamente en cuenta las exigencias específicas de la lucha contra la ciberdelincuencia;

Teniendo asimismo en cuenta el plan de acción adoptado por los Jefes de Estado y de Gobierno del Consejo de Europa, con ocasión de su segunda Cumbre (Estrasburgo, 10 y 11 de octubre de 1997) con objeto de encontrar respuestas comunes ante el desarrollo de las nuevas tecnologías de la información, basadas en las normas y los valores del Consejo de Europa,

Han convenido en lo siguiente:

Capítulo I – Terminología

Artículo 1 – Definiciones

A los efectos del presente Convenio:

a. por "sistema informático" se entenderá todo dispositivo aislado o conjunto de dispositivos interconectados o

relacionados entre sí, cuya función, o la de alguno de sus elementos, sea el tratamiento automatizado de datos en ejecución de un programa;

b. por "datos informáticos" se entenderá toda representación de hechos, información o conceptos expresados de cualquier forma que se preste a tratamiento informático, incluidos los programas diseñados para que un sistema informático ejecute una función;

c. por "proveedor de servicios" se entenderá:

i. toda entidad pública o privada que ofrezca a los usuarios de sus servicios la posibilidad de comunicar a través de un sistema informático, y

ii. cualquier otra entidad que procese o almacene datos informáticos para dicho servicio de comunicación o para los usuarios del mismo;

d. por "datos relativos al tráfico" se entenderá todos los datos relativos a una comunicación realizada por medio de un sistema informático, generados por este último en tanto que elemento de la cadena de comunicación, y que indiquen el origen, el destino, la ruta, la hora, la fecha, el tamaño y la duración de la comunicación o el tipo de servicio subyacente.

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

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

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.

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

1. 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.

2. 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.

3. 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.

Título 2 – delitos informáticos

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:

a. la introducción, alteración, borrado o supresión de datos informáticos;

b. 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.

Título 3 – Delitos relacionados con el contenido

Artículo 9 – Delitos relacionados con la pornografía infantil

1. 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 la intención de difundirla a través de un sistema informático;

b. la oferta o la puesta a disposición de pornografía infantil a través de un sistema informático;
c. la difusión o la transmisión de pornografía infantil a través de un sistema informático;
d. la adquisición, para uno mismo o para otros, de pornografía infantil a través de un sistema informático;
e. la posesión de pornografía infantil en un sistema informático o en un dispositivo de almacenamiento de datos informáticos.

2. A los efectos del párrafo 1 anterior, se entenderá por «pornografía infantil» todo material pornográfico que contenga la representación visual de:

a. un menor adoptando un comportamiento sexualmente explícito;
b. una persona que parezca un menor adoptando un comportamiento sexualmente explícito;
c. imágenes realistas que representen a un menor adoptando un comportamiento sexualmente explícito.

3. 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.
4. 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.

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

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 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.
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 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.
3. 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.

Título 5 – Otras formas de responsabilidad y de sanción

Artículo 11 – Tentativa y complicidad

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno cualquier complicidad deliberada con vistas a la comisión de alguno de los delitos previstos en aplicación de los artículos 2 a 10 del presente Convenio, con la intención de que dicho delito sea cometido.
2. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno toda tentativa deliberada de cometer alguno de los delitos previstos en aplicación de los artículos 3 a 5, 7, 8, 9.1.a) y 9.1.c) del presente Convenio.
3. Las Partes podrán reservarse el derecho a no aplicar, en todo o en parte, el párrafo 2 del presente artículo.

Artículo 12 – Responsabilidad de las personas jurídicas

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para que pueda exigirse responsabilidad a las personas jurídicas por los delitos previstos en aplicación del presente Convenio, cuando éstos sean cometidos por cuenta de las mismas por una persona física, ya sea a título individual o como miembro de un órgano de dicha persona jurídica, que ejerza funciones directivas en su seno, en virtud de:

a. un poder de representación de la persona jurídica;
b. una autorización para tomar decisiones en nombre de la persona jurídica;
c. una autorización para ejercer funciones de control en el seno de la persona jurídica.

2. Además de los casos previstos en el párrafo 1 del presente artículo, Cada Parte adoptará las medidas necesarias para garantizar que pueda exigirse responsabilidad a una persona jurídica cuando la ausencia de vigilancia o de control por parte de cualquier persona física mencionada en el párrafo 1 haya permitido la comisión de un delito previsto en aplicación del presente Convenio por una persona física que actúe por cuenta de dicha persona jurídica y bajo su autoridad.
3. Dependiendo de los principios jurídicos de cada Parte, la responsabilidad de una persona jurídica podrá ser penal, civil o administrativa.
4. Dicha responsabilidad se entenderá sin perjuicio de la responsabilidad penal de las personas físicas que hayan cometido el delito.

Artículo 13 – Sanciones y medidas

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para que los delitos previstos en aplicación de los artículos 2 a 11 estén sujetos a sanciones efectivas, proporcionadas y disuasorias, incluidas penas privativas de libertad.
2. Las Partes garantizarán la imposición de sanciones o medidas penales o no penales efectivas, proporcionadas y disuasorias, incluidas sanciones pecuniarias, a las personas jurídicas consideradas responsables de conformidad con el artículo 12.

Sección 2 – Derecho procesal

Título 1 – Disposiciones comunes

Artículo 14 – Ámbito de aplicación de las disposiciones de procedimiento

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para establecer los poderes y procedimientos previstos en la presente Sección a los efectos de investigación o de procedimientos penales específicos.
2. Salvo que se establezca lo contrario en el artículo 21, cada Parte aplicará los poderes y procedimientos mencionados en el párrafo 1 del presente artículo:

a. a los delitos previstos en aplicación de los artículos 2 a 11 del presente Convenio;
b. a cualquier otro delito cometido por medio de un sistema informático; y
c. a la obtención de pruebas electrónicas de cualquier delito.

3. a. Las Partes podrán reservarse el derecho a aplicar las medidas mencionadas en el artículo 20 únicamente a los delitos o categorías de delitos especificados en su reserva, siempre que el repertorio de dichos delitos o categorías de delitos no sea más reducido que el de los delitos a los que dicha Parte aplique las medidas mencionadas en el artículo 21. Las Partes tratarán de limitar tal reserva de modo que sea posible la más amplia aplicación de la medida mencionada en el artículo 20.

b. Cuando, a causa de las restricciones que imponga su legislación vigente en el momento de la adopción del presente Convenio, una Parte no pueda aplicar las medidas previstas en los artículos 20 y 21 a las comunicaciones transmitidas dentro de un sistema informático de un proveedor de servicios:

i. que se haya puesto en funcionamiento para un grupo restringido de usuarios, y

ii. que no emplee las redes públicas de telecomunicación y no esté conectado a otro sistema informático, ya sea público o privado,

dicha Parte podrá reservarse el derecho a no aplicar dichas medidas a esas comunicaciones. Las Partes tratarán de limitar este tipo de reservas de modo que de modo que sea posible la más amplia aplicación de las medidas previstas en los artículos 20 y 21.

Artículo 15 – Condiciones y salvaguardias

1. Cada Parte se asegurará de que la instauración, ejecución y aplicación de los poderes y procedimientos previstos en la presente Sección se sometan a las condiciones y salvaguardias previstas en su derecho interno, que deberá garantizar una protección adecuada de los derechos humanos y de las libertades, y en particular de los derechos derivados de las obligaciones que haya asumido cada Parte en virtud del Convenio del Consejo de Europa para la Protección de los Derechos Humanos y de las Libertades Fundamentales (1950), el Pacto Internacional de Derechos Civiles y Políticos de las Naciones Unidas (1966) u otros instrumentos internacionales aplicables en materia de derechos humanos, y que deberá integrar el principio de proporcionalidad.

2. Cuando proceda, teniendo en cuenta la naturaleza del procedimiento o del poder de que se trate, dichas condiciones y salvaguardias incluirán una supervisión judicial u otra forma de supervisión independiente, los motivos que justifiquen su aplicación, así como la limitación del ámbito de aplicación y de la duración de dicho poder o procedimiento.

3. Siempre que sea conforme con el interés público, y en particular con la buena administración de la justicia, cada Parte examinará los efectos de los poderes y procedimientos mencionados en la presente Sección sobre los derechos, responsabilidades e intereses legítimos de terceros.

Título 2 – Conservación rápida de datos informáticos almacenados

Artículo 16 – Conservación rápida de datos informáticos almacenados

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para permitir a sus autoridades competentes ordenar o imponer de otro modo la conservación rápida de datos electrónicos específicos, incluidos los datos relativos al tráfico, almacenados por medio de un sistema informático, en particular cuando existan motivos para creer que dichos datos son particularmente susceptibles de pérdida o de modificación.

2. Cuando una Parte aplique lo dispuesto en el párrafo 1 anterior por medio de una orden impartida a una persona de que conserve determinados datos almacenados que se encuentren en poder o bajo el control de esa persona, la Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para obligar a dicha persona a conservar y a proteger la integridad de los datos durante el tiempo necesario, hasta un máximo de noventa días, con el fin de que las autoridades competentes puedan obtener su revelación. Las Partes podrán prever la renovación de dicha orden.

3. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para obligar a la persona que custodia los datos o a otra persona encargada de su conservación a mantener en secreto la ejecución de dichos procedimientos durante el tiempo previsto en su derecho interno.

4. Los poderes y procedimientos mencionados en el presente artículo estarán sujetos a lo dispuesto en los artículos 14 y 15.

Artículo 17 – Conservación y revelación parcial rápidas de los datos relativos al tráfico

1. Con el fin de garantizar la conservación de los datos relativos al tráfico, en aplicación del artículo 16, cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para:

a. garantizar la conservación rápida de los datos relativos al tráfico, ya sean uno o varios los proveedores de servicios que hayan participado en la transmisión de dicha comunicación; y

b. asegurar la revelación rápida a la autoridad competente de la Parte, o a una persona designada por dicha autoridad, de un volumen suficiente de datos relativos al tráfico para que dicha Parte pueda identificar tanto a los proveedores de servicios como la vía por la que la comunicación se ha transmitido.

2. Los poderes y procedimientos mencionados en el presente artículo estarán sujetos a lo dispuesto en los artículos 14 y 15.

Título 3 – Orden de presentación

Artículo 18 – Orden de presentación

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para facultar a sus autoridades competentes a ordenar:

a. a una persona presente en su territorio que comunique determinados datos informáticos que obren en su poder o bajo su control, almacenados en un sistema informático o en un dispositivo de almacenamiento informático; y

b. a un proveedor que ofrezca sus servicios en el territorio de dicha Parte, que comunique los datos que obren en su poder o bajo su control relativos a los abonados en relación con dichos servicios;

2. Los poderes y procedimientos mencionados en el presente artículo estarán sujetos a lo dispuesto en los artículos 14 y 15.

3. A los efectos del presente artículo, se entenderá por «datos relativos a los abonados» cualquier información, en forma de datos informáticos o de cualquier otro modo, que posea un proveedor de servicios y que se refiera a los abonados de sus servicios, diferentes de los datos relativos al tráfico o al contenido, y que permitan determinar:

a. el tipo de servicio de comunicación utilizado, las disposiciones técnicas adoptadas al respecto y el periodo de servicio;

b. la identidad, la dirección postal o situación geográfica y el número de teléfono del abonado, así como cualquier otro número de acceso y los datos relativos a la facturación y al pago, disponibles en virtud de un contrato o de un acuerdo de prestación de servicio;

c. cualquier otra información relativa al lugar en que se encuentren los equipos de comunicación, disponible en virtud de un contrato o de un acuerdo de prestación de servicio.

Título 4 – Registro y confiscación de datos informáticos almacenados

Artículo 19 – Registro y confiscación de datos informáticos almacenados

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para facultar a sus autoridades competentes a registrar o a tener acceso de un modo similar:

a. a todo sistema informático o a parte del mismo, así como a los datos informáticos en él almacenados; y
b. a todo dispositivo de almacenamiento informático que permita almacenar datos informáticos en su territorio.

2. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para asegurarse de que, cuando, de conformidad con el apartado 1.a), sus autoridades registren o tengan acceso de un modo similar a un sistema informático específico o a una parte del mismo y tengan motivos para creer que los datos buscados se hallan almacenados en otro sistema informático o en una parte del mismo situado en su territorio, y que dichos datos son legítimamente accesibles a partir del sistema inicial o están disponibles por medio de dicho sistema inicial, puedan extender rápidamente el registro o el acceso de un modo similar al otro sistema.
3. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para facultar a sus autoridades competentes a confiscar o a obtener de un modo similar los datos informáticos a los que se haya accedido en aplicación de los párrafos 1 o 2. Estas medidas incluirán las siguientes prerrogativas:

a. confiscar u obtener de un modo similar un sistema informático o una parte del mismo, o un dispositivo de almacenamiento informático;
b. realizar y conservar una copia de esos datos informáticos;
c. preservar la integridad de los datos informáticos almacenados pertinentes; y
d. hacer inaccesibles o suprimir dichos datos informáticos del sistema informático consultado.

4. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para facultar a sus autoridades competentes a ordenar a toda persona que conozca el funcionamiento de un sistema informático o las medidas aplicadas para proteger los datos informáticos que contiene, que proporcione toda la información necesaria, dentro de lo razonable, para permitir la aplicación de las medidas previstas en los párrafos 1 y 2.
5. Los poderes y procedimientos mencionados en el presente artículo estarán sujetos a lo dispuesto en los artículos 14 y 15.

Título 5 – Obtención en tiempo real de datos informáticos

Artículo 20 – Obtención en tiempo real de datos relativos al tráfico

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para facultar a sus autoridades competentes:

a. a obtener o grabar con medios técnicos existentes en su territorio, y
b. a obligar a cualquier proveedor de servicios, en la medida de sus capacidades técnicas:

i. a obtener o a grabar con medios técnicos existentes en su territorio, o
ii. a ofrecer a las autoridades competentes su colaboración y su asistencia para obtener o grabar

en tiempo real los datos relativos al tráfico asociados a comunicaciones específicas transmitidas en su territorio por medio de un sistema informático.
2. Cuando una Parte no pueda adoptar las medidas enunciadas en el apartado 1.a) por respeto a los principios establecidos en su ordenamiento jurídico interno, podrá, en su lugar, adoptar las medidas legislativas y de otro tipo que resulten necesarias para asegurar la obtención o la grabación en tiempo real de los datos relativos al tráfico asociados a comunicaciones específicas transmitidas en su territorio mediante la aplicación de medios técnicos existentes en dicho territorio.
3. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para obligar a un proveedor de servicios a mantener en secreto el hecho de que se haya ejercido cualquiera de los poderes previstos en el presente artículo, así como toda información al respecto.
4. Los poderes y procedimientos mencionados en el presente artículo estarán sujetos a lo dispuesto en los artículos 14 y 15.

Artículo 21 – Interceptación de datos relativos al contenido

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para facultar a sus autoridades competentes en lo que respecta a un repertorio de delitos graves que deberá definirse en su derecho interno a:

a. obtener o grabar con medios técnicos existentes en su territorio, y
b. obligar a un proveedor de servicios, en la medida de sus capacidades técnicas, a:

i. obtener o grabar con medios técnicos existentes en su territorio, o
ii. prestar a las autoridades competentes su colaboración y su asistencia para obtener o grabar,

en tiempo real los datos relativos al contenido de comunicaciones específicas transmitidas en su territorio por medio de un sistema informático.
2. Cuando una Parte no pueda adoptar las medidas enunciadas en el apartado 1.a) por respeto a los principios establecidos en su ordenamiento jurídico interno, podrá, en su lugar, adoptar las medidas legislativas y de otro tipo que resulten necesarias para asegurar la obtención o la grabación en tiempo real de los datos relativos al contenido de comunicaciones específicas transmitidas en su territorio con medios técnicos existentes en ese territorio.
3. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para obligar a un proveedor de servicios a mantener en secreto el hecho de que se haya ejercido cualquiera de los poderes previstos en el presente artículo, así como toda información al respecto.
4. Los poderes y procedimientos mencionados en el presente artículo estarán sujetos a lo dispuesto en los artículos 14 y 15.

Sección 3 – Jurisdicción

Artículo 22 – Jurisdicción

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para afirmar su jurisdicción respecto de cualquier delito previsto de conformidad con los artículos 2 a 11 del presente Convenio, cuando el delito se haya cometido:

a. en su territorio; o
b. a bordo de un buque que enarbole su pabellón; o
c. a bordo de una aeronave matriculada según sus leyes; o
d. por uno de sus nacionales, si el delito es susceptible de sanción penal en el lugar en el que se cometió o si ningún Estado tiene competencia territorial respecto del mismo.

2. Las Partes podrán reservarse el derecho a no aplicar, o a aplicar sólo en determinados casos o condiciones, las normas sobre jurisdicción establecidas en los apartados 1.b) a 1.d) del presente artículo o en cualquier parte de dichos apartados.

3. Cada Parte adoptará las medidas que resulten necesarias para afirmar su jurisdicción respecto de cualquier delito mencionado en el párrafo 1 del artículo 24 del presente Convenio cuando el presunto autor del mismo se halle en su territorio y no pueda ser extraditado a otra Parte por razón únicamente de su nacionalidad, previa demanda de extradición.

4. El presente Convenio no excluye ninguna jurisdicción penal ejercida por una Parte de conformidad con su derecho interno.

5. En el caso de que varias Partes reivindiquen su jurisdicción respecto de un presunto delito contemplado en el presente Convenio, las Partes interesadas celebrarán consultas, cuando ello sea oportuno, con el fin de decidir qué jurisdicción es más adecuada para entablar la acción penal.

Capítulo III – Cooperación internacional

Sección 1 – Principios generales

Título 1 – Principios generales relativos a la cooperación internacional

Artículo 23 – Principios generales relativos a la cooperación internacional

Las Partes cooperarán entre sí en la mayor medida posible de conformidad con las disposiciones del presente Capítulo, en aplicación de los instrumentos internacionales pertinentes sobre cooperación internacional en materia penal, de los acuerdos basados en legislación uniforme o recíproca y de su propio derecho interno, a efectos de las investigaciones o los procedimientos relativos a los delitos relacionados con sistemas y datos informáticos o para obtener pruebas en formato electrónico de los delitos.

Título 2 – Principios relativos a la extradición

Artículo 24 – Extradición

1. a. El presente artículo se aplicará a la extradición entre las Partes por los delitos definidos de conformidad con los artículos 2 a 11 del presente Convenio, siempre que sean castigados por la legislación de las dos Partes implicadas con una pena privativa de libertad de una duración de al menos un año, o con una pena más grave.

b. Cuando se aplique una pena mínima diferente en virtud de un tratado de extradición aplicable entre dos o más Partes, incluido el Convenio Europeo de Extradición (STE nº 24), o de un acuerdo basado en legislación uniforme o recíproca, se aplicará la pena mínima prevista en dicho tratado o acuerdo.

2. Se considerará que los delitos descritos en el párrafo 1 del presente artículo están incluidos entre los delitos que pueden dar lugar a extradición en todos los tratados de extradición concluidos entre o por las Partes. Las Partes se comprometerán a incluir dichos delitos entre los que pueden dar lugar a extradición en todos los tratados de extradición que puedan concluir.

3. Cuando una parte que condicione la extradición a la existencia de un tratado reciba una demanda de extradición de otra Parte con la que no ha concluido ningún tratado de extradición, podrá tomar el presente Convenio como fundamento jurídico de la extradición en relación con cualquiera de los delitos previstos en el párrafo 1 del presente artículo.

4. Las Partes que no condicionen la extradición a la existencia de un tratado reconocerán los delitos mencionados en el párrafo 1 del presente artículo como delitos que pueden dar lugar a extradición entre ellas.

5. La extradición estará sujeta a las condiciones previstas en el derecho interno de la Parte requerida o en los tratados de extradición vigentes, incluidos los motivos por los que la Parte requerida puede denegar la extradición.

6. Si se deniega la extradición por un delito mencionado en el párrafo 1 del presente artículo únicamente por razón de la nacionalidad de la persona reclamada o porque la Parte requerida se considera competente respecto de dicho delito, la Parte requerida deberá someter el asunto, a petición de la Parte requirente, a sus autoridades competentes a efectos de la acción penal pertinente, e informará, a su debido tiempo, de la conclusión del asunto a la Parte requirente. Dichas autoridades tomarán su decisión y realizarán sus investigaciones y procedimientos del mismo modo que para cualquier otro delito de naturaleza comparable, de conformidad con la legislación de dicha Parte.

7. a. Cada Parte comunicará al Secretario General del Consejo de Europa, en el momento de la firma o del depósito de su instrumento de ratificación, aceptación, aprobación o adhesión, el nombre y la dirección de cada autoridad responsable del envío o de la recepción de las demandas de extradición o de detención provisional, en ausencia de tratado.

b. El Secretario General del Consejo de Europa creará y mantendrá actualizado un registro de las autoridades designadas por las Partes. Cada Parte garantizará en todo momento la exactitud de los datos que figuren en el registro.

Título 3 – Principios generales relativos a la asistencia mutua

Artículo 25 – Principios generales relativos a la asistencia mutua

1. Las Partes se prestarán toda la ayuda mutua posible a efectos de las investigaciones o de los procedimientos relativos a los delitos relacionados con sistemas y datos informáticos o con el fin de obtener pruebas en formato electrónico de un delito.

2. Cada Parte adoptará asimismo las medidas legislativas y de otro tipo que resulten necesarias para cumplir con las obligaciones establecidas en los artículos 27 a 35.

3. Cada Parte podrá, en caso de urgencia, formular una solicitud de asistencia mutua, o realizar las comunicaciones relativas a la misma a través de medios de comunicación rápidos, como el fax o el correo electrónico, siempre que esos medios ofrezcan niveles suficientes de seguridad y de autenticación (incluido el criptado, en caso necesario), con confirmación oficial posterior si el Estado requerido así lo exige. El Estado requerido aceptará la solicitud y responderá a la misma por cualquiera de esos medios rápidos de comunicación.

4. Salvo en caso de que se disponga expresamente otra cosa en los artículos del presente Capítulo, la asistencia mutua estará sujeta a las condiciones establecidas en el derecho interno de la Parte requerida o en los tratados de asistencia mutua aplicables, incluidos los motivos sobre la base de los cuales la Parte requerida puede rechazar la cooperación. La Parte requerida no deberá ejercer su derecho a rehusar la asistencia mutua en relación con los delitos previstos en los artículos 2 a 11 únicamente porque la solicitud se refiera a un delito que dicha Parte considere de carácter fiscal.

5. Cuando, de conformidad con lo dispuesto en el presente Capítulo, la Parte requerida esté autorizada a condicionar la asistencia mutua a la existencia de doble tipificación penal, se considerará que dicha condición se satisface si el acto que constituye delito, y para el que se solicita la asistencia mutua, está tipificado como tal en su derecho interno, independientemente de que dicho derecho interno incluya o no el delito en la misma categoría o lo denomine o no con la misma terminología que la Parte requirente.

Artículo 26 – Información espontánea

1. Dentro de los límites de su derecho interno y sin que exista demanda previa, una Parte podrá comunicar a otra Parte información obtenida de sus propias investigaciones si considera que ello puede ayudar a la Parte destinataria a iniciar o a concluir investigaciones o procedimientos en relación con delitos previstos de conformidad con el presente Convenio, o cuando dicha información pueda conducir a una petición de cooperación de dicha Parte en virtud del presente Capítulo.

2. Antes de comunicar dicha información, la Parte que la proporciona podrá pedir que sea tratada de forma

confidencial o que sólo se utilice bajo ciertas condiciones. Si la Parte destinataria no puede atender a dicha petición, deberá informar de ello a la otra Parte, que decidirá a continuación si, no obstante, debe proporcionar la información. Si la Parte destinataria acepta la información bajo las condiciones establecidas, estará obligada a respetarlas.

Título 4 – Procedimientos relativos a las solicitudes de asistencia mutua en ausencia de acuerdos internacionales aplicables

Artículo 27 – Procedimientos relativos a las solicitudes de asistencia mutua en ausencia de acuerdos internacionales aplicables

1. En ausencia de tratado de asistencia mutua o de acuerdo basado en legislación uniforme o recíproca en vigor entre la Parte requirente y la Parte requerida, se aplicarán las disposiciones de los párrafos 2 a 9 del presente artículo. Dichas disposiciones no se aplicarán cuando exista un tratado, acuerdo o legislación de este tipo, a menos que las Partes implicadas decidan aplicar en su lugar la totalidad o una parte del resto del presente artículo.

2. a. Cada Parte designará una o varias autoridades centrales encargadas de enviar las solicitudes de asistencia mutua o de responder a las mismas, de ejecutarlas o de remitirlas a las autoridades competentes para su ejecución;

b. las autoridades centrales comunicarán directamente entre sí;

c. en el momento de la firma o del depósito de su instrumento de ratificación, aceptación, aprobación o adhesión, cada Parte comunicará al Secretario General del Consejo de Europa los nombres y direcciones de las autoridades designadas en aplicación del presente párrafo.

d. el Secretario General del Consejo de Europa creará y mantendrá actualizado un registro de las autoridades centrales designadas por las Partes. Cada Parte garantizará en todo momento la exactitud de los datos que figuren en el registro.

3. Las solicitudes de asistencia mutua en virtud del presente artículo se ejecutarán de conformidad con el procedimiento especificado por la Parte requirente, salvo cuando dicho procedimiento sea incompatible con la legislación de la Parte requerida.

4. Además de las condiciones o los motivos de denegación previstos en el párrafo 4 del artículo 25, la asistencia mutua puede ser denegada por la Parte requerida:

a. si la solicitud tiene que ver con un delito que la Parte requerida considera de carácter político o vinculado a un delito de carácter político; o

b. si la Parte requerida estima que acceder a la solicitud podría atentar contra su soberanía, seguridad, orden público u otros intereses esenciales.

5. La Parte requerida podrá aplazar su actuación en respuesta a una solicitud si dicha actuación puede perjudicar a investigaciones o procedimientos llevados a cabo por sus autoridades.

6. Antes de denegar o aplazar su cooperación, la Parte requerida estudiará, previa consulta con la Parte requirente cuando proceda, si puede atenderse la solicitud parcialmente o bajo las condiciones que considere necesarias.

7. La Parte requerida informará rápidamente a la Parte requirente del curso que prevé dar a la solicitud de asistencia. Deberá motivar toda denegación o aplazamiento de la misma. La Parte requerida informará asimismo a la Parte requirente de cualquier motivo que imposibilite la ejecución de la asistencia o que pueda retrasarla sustancialmente.

8. La Parte requirente podrá solicitar que la Parte requerida mantenga confidenciales la presentación y el objeto de cualquier solicitud formulada en virtud del presente Capítulo, salvo en la medida en que sea necesario para la ejecución de la misma. Si la Parte requerida no puede acceder a la petición de confidencialidad, deberá informar de ello sin demora a la Parte requirente, quien decidirá a continuación si, no obstante, la solicitud debe ser ejecutada.

9. a. En caso de urgencia, las autoridades judiciales de la Parte requirente podrán dirigir directamente a las autoridades homólogas de la Parte requerida las solicitudes de asistencia y las comunicaciones relativas a las mismas. En tales casos, se remitirá simultáneamente una copia a la autoridad central de la Parte requerida a través de la autoridad central de la Parte requirente.

b. Toda solicitud o comunicación en virtud del presente párrafo podrá formularse a través de la Organización Internacional de Policía Criminal (Interpol).

c. Cuando se formule una solicitud en aplicación del apartado a) del presente artículo y la autoridad no tenga competencia para tratarla, la remitirá a la autoridad nacional competente e informará directamente de ello a la Parte requirente.

d. Las solicitudes o comunicaciones realizadas en aplicación del presente párrafo que no impliquen medidas coercitivas podrán ser transmitidas directamente por las autoridades competentes de la Parte requirente a las autoridades competentes de la Parte requerida.

e. En el momento de la firma o del depósito de su instrumento de ratificación, aceptación, aprobación o adhesión, las Partes podrán informar al Secretario General del Consejo de Europa de que, en aras de la eficacia, las solicitudes formuladas en virtud del presente párrafo deberán dirigirse a su autoridad central.

Artículo 28 – Confidencialidad y restricciones de uso

1. En ausencia de tratado de asistencia mutua o de acuerdo basado en legislación uniforme o recíproca en vigor entre la Parte requirente y la Parte requerida, se aplicarán las disposiciones del presente artículo. Dichas disposiciones no se aplicarán cuando exista un tratado, acuerdo o legislación de este tipo, a menos que las Partes interesadas decidan aplicar en su lugar la totalidad o una parte del presente artículo.

2. La Parte requerida podrá supeditar la transmisión de información o de material en respuesta a una solicitud al cumplimiento de las siguientes condiciones:

a. que se preserve su confidencialidad cuando la solicitud de asistencia no pueda ser atendida en ausencia de dicha condición; o

b. que no se utilicen para investigaciones o procedimientos distintos a los indicados en la solicitud.

3. Si la Parte requirente no pudiera satisfacer alguna de las condiciones mencionadas en el párrafo 2, informará de ello sin demora a la Parte requerida, quien determinará a continuación si, no obstante, la información ha de ser proporcionada. Si la Parte requirente acepta esta condición, estará obligada a cumplirla.

4. Toda Parte que proporcione información o material supeditado a alguna de las condiciones mencionadas en el párrafo 2 podrá exigir a la otra Parte precisiones sobre el uso que haya hecho de dicha información o material en relación con dicha condición.

Sección 2 – Disposiciones específicas

Título 1 – Asistencia mutua en materia de medidas provisionales

Artículo 29 – Conservación rápida de datos informáticos almacenados

1. Una Parte podrá solicitar a otra Parte que ordene o imponga de otro modo la conservación rápida de datos almacenados por medio de sistemas informáticos que se encuentren en el territorio de esa otra Parte, y en relación con los cuales la Parte requirente tenga intención de presentar una solicitud de asistencia mutua con vistas al registro o al acceso por un medio similar, la confiscación o la obtención por un medio similar, o a la revelación de dichos datos.

2. En toda solicitud de conservación formulada en virtud del párrafo 1 deberá precisarse:

a. la autoridad que solicita la conservación;
b. el delito objeto de la investigación o de procedimientos penales y una breve exposición de los hechos relacionados con el mismo;
c. los datos informáticos almacenados que deben conservarse y su relación con el delito;
d. toda información disponible que permita identificar al responsable de la custodia de los datos informáticos almacenados o el emplazamiento del sistema informático;
e. la necesidad de la medida de conservación; y
f. que la Parte tiene intención de presentar una solicitud de asistencia mutua con vistas al registro o al acceso por un medio similar, a la confiscación o a la obtención por un medio similar, o a la revelación de los datos informáticos almacenados.

3. Tras recibir la solicitud de otra Parte, la Parte requerida deberá adoptar todas las medidas adecuadas para proceder sin demora a la conservación de los datos solicitados, de conformidad con su derecho interno. A los efectos de responder a solicitudes de este tipo no se requiere la doble tipificación penal como condición para proceder a la conservación.
4. Cuando una Parte exige la doble tipificación penal como condición para atender a una solicitud de asistencia mutua con vistas al registro o al acceso por un medio similar, a la confiscación o a la obtención por un medio similar o a la revelación de los datos almacenados en relación con delitos diferentes de los previstos de conformidad con los artículos 2 a 11 del presente Convenio, podrá reservarse el derecho a denegar la solicitud de conservación en virtud del presente artículo en caso de que tenga motivos para creer que, en el momento de la revelación de los datos, no se cumplirá la condición de la doble tipificación penal.
5. Asimismo, las solicitudes de conservación sólo podrán ser denegadas si:

a. la solicitud se refiere a un delito que la Parte requerida considera de carácter político o vinculado a un delito de carácter político; o
b. la Parte requerida considera que la ejecución de la solicitud podría atentar contra su soberanía, seguridad, orden público u otros intereses esenciales.

6. Cuando la Parte requerida considere que la conservación por sí sola de los datos no bastará para garantizar su disponibilidad futura, o que pondrá en peligro la confidencialidad de la investigación de la Parte requirente, o causará cualquier otro perjuicio a la misma, informará de ello rápidamente a la Parte requirente, quien determinará a continuación la conveniencia, no obstante, de dar curso a la solicitud.
7. Las medidas de conservación adoptadas en respuesta a solicitudes como la prevista en el párrafo 1 serán válidas por un periodo mínimo de 60 días, con el fin de que la Parte requirente pueda presentar una solicitud con vistas al registro o el acceso por un medio similar, la confiscación o la obtención por un medio similar, o la revelación de los datos. Una vez recibida la solicitud, los datos deberán conservarse hasta que se tome una decisión sobre la misma.

Artículo 30 – Revelación rápida de datos conservados

1. Si, al ejecutar una solicitud formulada de conformidad con el artículo 29 para la conservación de datos relativos al tráfico de una determinada comunicación la Parte requerida descubriera que un proveedor de servicios de otro Estado ha participado en la transmisión de dicha comunicación, dicha Parte revelará rápidamente a la Parte requirente un volumen suficiente de datos relativos al tráfico para que pueda identificarse al proveedor de servicios, así como la vía por la que la comunicación ha sido transmitida.
2. La revelación de datos relativos al tráfico en aplicación del párrafo 1 sólo podrá ser denegada si:

a. la solicitud se refiere a un delito que la Parte requerida considera de carácter político o vinculado a un delito de carácter político; o
b. la Parte requerida considera que la ejecución de la solicitud podría atentar contra su soberanía, seguridad, orden público u otros intereses esenciales.

Título 2 – Asistencia mutua en relación con los poderes de investigación

Artículo 31 – Asistencia mutua en relación con el acceso a datos almacenados

1. Una Parte podrá solicitar a otra Parte el registro o el acceso de un modo similar, la confiscación o la obtención de un modo similar o la revelación de datos almacenados por medio de un sistema informático que se encuentre en el territorio de esa otra Parte, incluidos los datos conservados de conformidad con el artículo 29.
2. La Parte requerida responderá a la solicitud aplicando los instrumentos internacionales, acuerdos y legislación mencionados en el artículo 23, así como de conformidad con las disposiciones pertinentes del presente Capítulo.
3. La solicitud deberá responderse lo más rápidamente posible en los siguientes casos:

a. cuando existan motivos para creer que los datos pertinentes están particularmente expuestos al riesgo de pérdida o de modificación; o
b. cuando los instrumentos, acuerdos o legislación mencionados en el párrafo 2 prevean una cooperación rápida.

Artículo 32 – Acceso transfronterizo a datos almacenados, con consentimiento o cuando sean accesibles al público

Una Parte podrá, sin autorización de otra:

a. tener acceso a datos informáticos almacenados accesibles al público (fuente abierta), independientemente de la ubicación geográfica de los mismos; o
b. tener acceso a datos informáticos almacenados en otro Estado, o recibirlos, a través de un sistema informático situado en su territorio, si dicha Parte obtiene el consentimiento lícito y voluntario de la persona legalmente autorizada a revelárselos por medio de ese sistema informático.

Artículo 33 – Asistencia mutua para la obtención en tiempo real de datos relativos al tráfico

1. Las Partes se prestarán asistencia mutua para la obtención en tiempo real de datos relativos al tráfico asociados a comunicaciones específicas transmitidas en su territorio por medio de un sistema informático. A reserva de las disposiciones del párrafo 2, dicha asistencia mutua estará sujeta a las condiciones y procedimientos previstos en el derecho interno.
2. Cada Parte prestará dicha asistencia al menos en relación con los delitos para los cuales sería posible la obtención en tiempo real de datos relativos al tráfico en situaciones análogas a nivel interno.

Artículo 34 – Asistencia mutua en relación con la interceptación de datos relativos al contenido

Las Partes se prestarán asistencia mutua, en la medida en que lo permitan sus tratados y leyes internas aplicables, para la obtención o el registro en tiempo real de datos relativos al contenido de comunicaciones específicas transmitidas por medio de un sistema informático.

Título 3 – Red 24/7

Artículo 35 – Red 24/7

1. Cada Parte designará un punto de contacto localizable las 24 horas del día, siete días a la semana, con el fin de garantizar una asistencia inmediata para investigaciones relativas a delitos vinculados a sistemas y datos informáticos, o para obtener las pruebas en formato electrónico de un delito. Esta asistencia comprenderá toda acción que facilite las medidas que figuran a continuación,

o su aplicación directa si lo permite el derecho y la práctica internos:

a. asesoramiento técnico;
b. conservación de datos, de conformidad con los artículos 29 y 30; y
c. obtención de pruebas, suministro de información de carácter jurídico y localización de sospechosos.

2. a. El punto de contacto de una Parte dispondrá de los medios para comunicarse con el punto de contacto de otra Parte siguiendo un procedimiento acelerado.
b. Si el punto de contacto designado por una Parte no depende de la autoridad o autoridades de dicha Parte responsables de la asistencia mutua internacional o de la extradición, dicho punto de contacto se asegurará de poder actuar coordinadamente con esta o estas autoridades por medio de un procedimiento acelerado.

3. Cada Parte garantizará la disponibilidad de personal formado y equipado con objeto de facilitar el funcionamiento de la red.

Capítulo IV – Cláusulas finales

Artículo 36 – Firma y entrada en vigor

1. El presente Convenio está abierto a la firma de los Estados miembros del Consejo de Europa y de los Estados no miembros que hayan partícipado en su elaboración.
2. El presente Convenio estará sujeto a ratificación, aceptación o aprobación. Los instrumentos de ratificación, aceptación o aprobación se depositarán en poder del Secretario General del Consejo de Europa.
3. El presente Convenio entrará en vigor el primer día del mes siguiente a la expiración de un plazo de tres meses desde la fecha en que cinco Estados, de los cuales al menos tres deberán ser miembros del Consejo de Europa, hayan expresado su consentimiento para quedar vinculados por el Convenio, de conformidad con lo dispuesto en los párrafos 1 y 2.
4. Para todo Estado signatario que exprese ulteriormente su consentimiento para quedar vinculado por el Convenio, éste entrará en vigor el primer día del mes siguiente a la expiración de un plazo de tres meses desde la fecha en que haya expresado dicho consentimiento, de conformidad con lo dispuesto en los párrafos 1 y 2.

Artículo 37 – Adhesión al Convenio

1. A partir de la entrada en vigor del presente Convenio, el Comité de Ministros del Consejo de Europa podrá, previa consulta con los Estados contratantes del Convenio y habiendo obtenido su consentimiento unánime, invitar a adherirse al presente Convenio a cualquier Estado que no sea miembro del Consejo de Europa y que no haya participado en su elaboración. La decisión se adoptará respetando la mayoría establecida en el artículo 20.d del Estatuto del Consejo de Europa y con el voto unánime de los representantes de los Estados contratantes con derecho a formar parte del Comité de Ministros.
2. Para todo Estado que se adhiera al Convenio de conformidad con el párrafo 1 precedente, el Convenio entrará en vigor el primer día del mes siguiente a la expiración de un plazo de tres meses desde la fecha del depósito del instrumento de adhesión en poder del Secretario General del Consejo de Europa.

Artículo 38 – Aplicación territorial

1. En el momento de la firma o del depósito del instrumento de ratificación, aceptación, aprobación o adhesión, todo Estado podrá designar el territorio o los territorios a los que se aplicará el presente Convenio.
2. Posteriormente, todo Estado podrá, en cualquier momento y por medio de una declaración dirigida al Secretario General del Consejo de Europa, hacer extensiva la aplicación del presente Convenio a cualquier otro territorio especificado en la declaración. El Convenio entrará en vigor respecto de dicho territorio el primer día del mes siguiente a la expiración de un plazo de tres meses desde la fecha en que el Secretario General haya recibido la declaración.
3. Toda declaración formulada en virtud de los dos párrafos precedentes podrá ser retirada, respecto de cualquier territorio especificado en la misma, mediante notificación dirigida al Secretario General del Consejo de Europa. La retirada surtirá efecto el primer día del mes siguiente a la expiración de un plazo de tres meses desde la fecha en que el Secretario General haya recibido la notificación.

Artículo 39 – Efectos del Convenio

1. El objeto del presente Convenio es completar los tratados o acuerdos multilaterales o bilaterales aplicables entre las Partes, incluidas las disposiciones:

– del Convenio Europeo de Extradición, abierto a la firma el 13 de diciembre de 1957 en París (STE nº 24)
– del Convenio Europeo de Asistencia Judicial en Materia Penal, abierto a la firma el 20 de abril de 1959 en Estrasburgo (STE nº 30),
– del Protocolo adicional al Convenio Europeo de Asistencia Judicial en Materia Penal, abierto a la firma el 17 de marzo de 1978 en Estrasburgo (STE nº 99).

2. Si dos o más Partes han celebrado ya un acuerdo o un tratado relativo a las cuestiones contempladas en el presente Convenio, o han regulado de otro modo sus relaciones al respecto, o si lo hacen en el futuro, podrán asimismo aplicar el citado acuerdo o tratado, o regular sus relaciones de conformidad con el mismo, en lugar del presente Convenio. No obstante, cuando las Partes regulen sus relaciones respecto de las cuestiones objeto del presente Convenio de forma distinta a la prevista en el mismo, lo harán de modo que no sea incompatible con los objetivos y principios del Convenio.
3. Nada de lo dispuesto en el presente Convenio afectará a otros derechos, restricciones, obligaciones y responsabilidades de cada Parte.

Artículo 40 – Declaraciones

Mediante declaración por escrito dirigida al Secretario General del Consejo de Europa, cualquier Estado podrá declarar, en el momento de la firma o del depósito de su instrumento de ratificación, aceptación, aprobación o adhesión, que se acoge a la facultad de exigir, llegado el caso, uno o varios elementos complementarios previstos en los artículos 2, 3, 6.1.b), 7, 9.3 y 27.9.e).

Artículo 41 – Cláusula federal

1. Un Estado federal podrá reservarse el derecho a cumplir las obligaciones especificadas en el Capítulo II del presente Convenio en la medida en que éstas sean compatibles con los principios fundamentales por los que se rijan las relaciones entre su gobierno central y los estados que lo constituyen u otras entidades territoriales análogas, a condición de que pueda garantizar la cooperación según lo previsto en el Capítulo III.
2. Cuando formule una reserva en virtud del párrafo 1, un Estado federal no podrá hacer uso de los términos de dicha reserva para excluir o reducir de manera sustancial sus obligaciones en virtud del Capítulo II. En todo caso, se dotará de medios amplios y efectivos para aplicar las medidas previstas en el citado Capítulo.
3. En lo relativo a las disposiciones del presente Convenio cuya aplicación sea competencia legislativa de cada uno de los estados constituyentes u otras entidades territoriales análogas, que no estén obligados por el sistema constitucional de la federación a adoptar medidas legislativas, el gobierno federal pondrá dichas disposiciones en conocimiento de las autoridades competentes de los estados constituyentes junto con su opinión favorable, alentándolas a adoptar las medidas adecuadas para su aplicación.

Artículo 42 – Reservas

Mediante notificación por escrito dirigida al Secretario del Consejo de Europa, cualquier Estado podrá declarar, en el momento de la firma o del depósito de su instrumento

de ratificación, aceptación, aprobación o adhesión, que se acoge a una o varias de las reservas previstas en el párrafo 2 del artículo 4, el párrafo 3 del artículo 6, el párrafo 4 del artículo 9, el párrafo 3 del artículo 10, el párrafo 3 del artículo 11, el párrafo 3 del artículo 14, el párrafo 2 del artículo 22, el párrafo 4 del artículo 29 y el párrafo 1 del artículo 41. No podrá formularse ninguna otra reserva.

Artículo 43 – Mantenimiento y retirada de las reservas

1. Una Parte que haya formulado una reserva de conformidad con el artículo 42 podrá retirarla total o parcialmente mediante notificación por escrito dirigida al Secretario General del Consejo de Europa. Dicha retirada surtirá efecto en la fecha en que el Secretario General reciba la notificación. Si en la notificación se indica una fecha a partir de la cual ha de hacerse efectiva la retirada de una reserva y esta fecha es posterior a la fecha en la que el Secretario General ha recibido la notificación, la retirada se hará efectiva en dicha fecha posterior.
2. Una Parte que haya formulado una reserva de las mencionadas en el artículo 42 retirará dicha reserva, total o parcialmente, tan pronto como lo permitan las circunstancias.
3. El Secretario General del Consejo de Europa podrá solicitar periódicamente a las Partes que hayan formulado una o varias reservas conforme a lo dispuesto en el artículo 42, información sobre las perspectivas de su retirada.

Artículo 44 – Enmiendas

1. Cada Parte podrá proponer enmiendas al presente Convenio, que el Secretario General del Consejo de Europa comunicará a los Estados miembros del Consejo de Europa, a los Estados no miembros que hayan participado en la elaboración del presente Convenio y a cualquier Estado que se haya adherido o que haya sido invitado a adherirse de conformidad con lo dispuesto en el artículo 37.
2. Toda enmienda propuesta por cualquiera de las Partes será comunicada al Comité Europeo para Problemas Criminales (CDPC), quien someterá al Comité de Ministros su opinión sobre la enmienda propuesta.
3. El Comité de Ministros examinará la enmienda propuesta y la opinión presentada por el CDPC y, previa consulta con los Estados no miembros Partes en el presente Convenio, podrá adoptar la enmienda.
4. El texto de cualquier enmienda adoptada por el Comité de Ministros de conformidad con lo dispuesto en el párrafo 3 del presente artículo será remitido a las Partes para su aceptación.
5. Toda enmienda adoptada de conformidad con el párrafo 3 del presente artículo entrará en vigor treinta días después de que todas las Partes hayan informado al Secretario General de su aceptación.

Artículo 45 – Solución de controversias

1. Se mantendrá informado al Comité Europeo para Problemas Criminales (CDPC) del Consejo de Europa acerca de la interpretación y la aplicación del presente Convenio.
2. En caso de controversia entre las Partes sobre la interpretación o la aplicación del presente Convenio, las Partes intentarán llegar a un acuerdo mediante negociación o por cualquier otro medio pacífico de su elección, incluida la sumisión de la controversia al CDPC, a un tribunal arbitral cuyas decisiones serán vinculantes para las Partes en litigio, o a la Corte Internacional de Justicia, según acuerden dichas Partes.

Artículo 46 – Consultas entre las Partes

1. Las Partes se consultarán periódicamente, según sea necesario, con el fin de facilitar:

a. la utilización y la aplicación efectivas del presente Convenio, incluida la identificación de cualquier problema al respecto, así como las repercusiones de toda declaración o reserva formulada de conformidad con el presente Convenio;

b. el intercambio de información sobre novedades jurídicas, políticas o técnicas importantes observadas en el ámbito de la delincuencia informática y la obtención de pruebas en formato electrónico;

c. el estudio de la posibilidad de ampliar o enmendar el Convenio.

2. Se informará periódicamente al Comité Europeo para Problemas Criminales (CDPC) del resultado de las consultas mencionadas en el párrafo 1.
3. En caso necesario, el Comité Europeo para Problemas Criminales (CDPC) facilitará las consultas mencionadas en el párrafo 1 y adoptará las medidas necesarias para ayudar a las Partes en sus esfuerzos por ampliar o enmendar el Convenio. Expirado un plazo de tres años como máximo desde la entrada en vigor del presente Convenio, el CDPC procederá, en cooperación con las Partes, a una revisión de todas las disposiciones de la Convención y propondrá, si procede, las enmiendas pertinentes.
4. Salvo cuando el Consejo de Europa los asuma, los gastos que ocasione la aplicación de las disposiciones del párrafo 1 serán sufragados por las Partes, en la forma que ellas mismas determinen.
5. Las Partes recibirán asistencia del Secretario del Consejo de Europa en el ejercicio de las funciones que dimanan del presente artículo.

Artículo 47 – Denuncia

1. Las Partes podrán denunciar en cualquier momento el presente Convenio mediante notificación dirigida al Secretario General del Consejo de Europa.
2. Dicha denuncia surtirá efecto el primer día del mes siguiente a la expiración de un plazo de tres meses desde la fecha en que el Secretario General haya recibido la notificación.

Artículo 48 – Notificación

El Secretario General del Consejo de Europa notificará a los Estados miembros del Consejo de Europa, a los Estados no miembros que hayan participado en la elaboración del presente Convenio, así como a cualquier Estado que se haya adherido o que haya sido invitado a adherirse al mismo:

a. cualquier firma;
b. el depósito de cualquier instrumento de ratificación, aceptación, aprobación o adhesión;
c. cualquier fecha de entrada en vigor del presente Convenio de conformidad con los artículos 36 y 37;
d. cualquier declaración presentada de conformidad con el artículo 40 o cualquier reserva formulada en virtud del artículo 42;
e. cualquier otro acto, notificación o comunicación relativos al presente Convenio.

En fe de lo cual, los infrascritos, debidamente autorizados a tal efecto, firman el presente Convenio.

Hecho en Budapest, el 23 de noviembre de 2001, en versión francesa e inglesa, ambos textos igualmente auténticos, y en un ejemplar único que se depositará en los archivos del Consejo de Europa. El Secretario General del Consejo de Europa remitirá copia certificada a cada uno de los Estados miembros del Consejo de Europa, a los Estados no miembros que hayan participado en la elaboración del Convenio y a cualquier Estado invitado a adherirse al mismo.

Declaraciones y Reservas del Perú al Convenio de Budapest

I. DECLARACIONES CONFORME AL ARTÍCULO 40 DEL CONVENIO:

Art. 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 la totalidad o a una parte de un sistema informático. Cualquier Parte podrá exigir que el delito se cometa infringiendo medidas de seguridad, con la intención de obtener datos informáticos o con otra intención delictiva, o en relación con un sistema informático que esté conectado a otro sistema informático".

Texto de declaración:

"De conformidad con lo dispuesto en el artículo 2 del Convenio sobre la Ciberdelincuencia, la República del Perú declara que su legislación exige que el delito de acceso ilícito se cometa infringiendo medidas de seguridad".

Art. 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 comunicados en transmisiones no públicas efectuadas a un sistema informático, desde un sistema informático o dentro del mismo, incluidas las emisiones electromagnéticas procedentes de un sistema informático que contenga dichos datos informáticos. Cualquier Parte podrá exigir que el delito se haya cometido con intención delictiva o en relación con un sistema informático conectado a otro sistema informático".

Texto de declaración:

"De conformidad con lo dispuesto en el artículo 3 del Convenio sobre la Ciberdelincuencia, la República del Perú declara que su legislación exige que el delito de interceptación ilícita se cometa con intención delictiva y que dicho delito puede cometerse en relación con un sistema informático conectado a otro sistema informático".

Art. 7, Falsificación informática

"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 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".

Texto de declaración:

"De conformidad con lo dispuesto en el artículo 7 del Convenio sobre la Ciberdelincuencia, la República del Perú declara que podrá exigir que exista una intención fraudulenta o delictiva similar, conforme a lo establecido en su derecho interno, para que las conductas descritas en dicho artículo generen responsabilidad penal".

Art. 27, Procedimientos relativos a las solicitudes de asistencia mutua en ausencia de acuerdos internacionales aplicables

"9. e) En el momento de la firma o el depósito de su instrumento de ratificación, aceptación, aprobación o adhesión, cada Parte podrá informar al Secretario General del Consejo de Europa de que, por razones de eficacia, las solicitudes formuladas en virtud del presente apartado deberán dirigirse a su autoridad central".

Texto de declaración:

"De conformidad con lo establecido en el artículo 27, numeral 9, literal e) del Convenio sobre la Ciberdelincuencia, la República del Perú declara que, en aras de la eficacia, las solicitudes efectuadas en virtud de lo dispuesto en el numeral 9 del Convenio deberán dirigirse a su autoridad central".

II. RESERVAS CONFORME AL ARTÍCULO 42 DEL CONVENIO:

Art. 6, Abuso de los dispositivos

"3. Cualquier Parte podrá reservarse el derecho a no aplicar lo dispuesto en el apartado 1 del presente artículo, siempre que la reserva no afecte a la venta, la distribución o cualquier otra puesta a disposición de los elementos indicados en el apartado 1.a.ii) del presente artículo".

Texto de reserva:

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

Art. 9, Delitos relacionados con la pornografía infantil

"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".

Texto de reserva:

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

Art. 29, Conservación rápida de datos informáticos almacenados

"4. Cuando una Parte exija la doble tipificación penal como condición para atender una solicitud de asistencia mutua para el registro o el acceso de forma similar, la confiscación o la obtención de forma similar o la revelación de datos almacenados, dicha Parte podrá reservarse, en relación con delitos distintos de los previstos con arreglo a los artículos 2 a 11 del presente Convenio, el derecho a denegar la solicitud de conservación en virtud del presente artículo en los casos en que tenga motivos para creer que la condición de la doble tipificación penal no podrá cumplirse en el momento de la revelación".

Texto de reserva:

"Conforme al numeral 4 del artículo 29 del Convenio sobre la Ciberdelincuencia, la República del Perú se reserva el derecho a denegar la solicitud de conservación en virtud de dicho artículo en el caso que tenga motivos para creer que, en el momento de la revelación de los datos, no se cumplirá con la condición de la doble tipificación penal".

1809507-1

ENTRADA EN VIGENCIA

Entrada en vigencia "Convenio sobre la Ciberdelincuencia" (en adelante, el Convenio), adoptado el 23 de noviembre de 2001 en la ciudad de Budapest, Hungría; aprobado mediante Resolución Legislativa N° 30913, del 12 de febrero de 2019; y, ratificado a través del Decreto Supremo N° 010-2019-RE, del 9 de marzo de 2019. **Entrará en vigor el 1 de diciembre de 2019**.

1809511-1

Ley N°30096, “Ley de Delitos Informáticos”

LEY DE DELITOS INFORMÁTICOS

LEY Nº 30096

EL PRESIDENTE DE LA REPÚBLICA

POR CUANTO:

EL CONGRESO DE LA REPÚBLICA;

Ha dado la Ley siguiente:

CAPÍTULO I

FINALIDAD Y OBJETO DE LA LEY

Artículo 1.- Objeto de la Ley

La presente Ley tiene por objeto prevenir y sancionar las conductas ilícitas que afectan los sistemas y datos informáticos y otros bienes jurídicos de relevancia penal, cometidas mediante la utilización de tecnologías de la información o de la comunicación, con la finalidad de garantizar la lucha eficaz contra la ciberdelincuencia.

CAPÍTULO II

DELITOS CONTRA DATOS Y SISTEMAS INFORMÁTICOS

Artículo 2.- Acceso ilícito

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

Será reprimido con la misma pena el que accede a un sistema informático excediendo lo autorizado. (*)

(*) Artículo modificado por el Artículo 1 de la Ley N° 30171, publicada el 10 marzo 2014, cuyo texto es el siguiente:

“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 contra la integridad de datos informáticos

El que, a través de las tecnologías de la información o de la comunicación, 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 modificado por el Artículo 1 de la Ley N° 30171, publicada el 10 marzo 2014, cuyo texto es el siguiente:

"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 contra la integridad de sistemas informáticos

El que, a través de las tecnologías de la información o de la comunicación, 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. (*)

(*) Artículo modificado por el Artículo 1 de la Ley N° 30171, publicada el 10 marzo 2014, cuyo texto es el siguiente:

"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."

CAPÍTULO III

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 las tecnologías de la información o de la comunicación, 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 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. (*)

(*) Artículo modificado por el Artículo 1 de la Ley N° 30171, publicada el 10 marzo 2014, cuyo texto es el siguiente:

"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."

CAPÍTULO IV

DELITOS INFORMÁTICOS CONTRA LA INTIMIDAD Y EL SECRETO DE LAS COMUNICACIONES

Artículo 6.- Tráfico ilegal de datos

El que crea, ingresa o utiliza indebidamente una base de datos sobre una persona natural o jurídica, identificada o identificable, para comercializar, traficar, vender, promover, favorecer o facilitar información relativa a cualquier ámbito de la esfera personal, familiar, patrimonial, laboral, financiera u otro de naturaleza análoga, creando o no perjuicio, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años. (*)

(*) Artículo derogado por la Única Disposición Complementaria Derogatoria de la Ley N° 30171, publicada el 10 marzo 2014.

Artículo 7.- Interceptación de datos informáticos

El que, a través de las tecnologías de la información o de la comunicación, intercepta 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, será reprimido con 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 las normas de la materia.

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

(*) Artículo modificado por el Artículo 1 de la Ley N° 30171, publicada el 10 marzo 2014, cuyo texto es el siguiente:

"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."

CAPÍTULO V

DELITOS INFORMÁTICOS CONTRA EL PATRIMONIO

Artículo 8. Fraude informático

El que, a través de las tecnologías de la información o de la comunicación, procura para sí o para otro un provecho ilícito en perjuicio de tercero mediante el diseño, introducción, alteración, borrado, supresión, clonación de datos informáticos o cualquier interferencia o manipulación en el funcionamiento de un sistema informático, será reprimido con una pena privativa de libertad no menor de tres ni mayor de ocho años y con sesenta a ciento veinte días multa.

La pena será privativa de libertad no menor de cinco ni mayor de diez años y de ochenta a ciento cuarenta días multa cuando se afecte el patrimonio del Estado destinado a fines asistenciales o a programas de apoyo social. (*)

(*) Artículo modificado por el Artículo 1 de la Ley N° 30171, publicada el 10 marzo 2014, cuyo texto es el siguiente:

"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."

CAPÍTULO VI

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.

CAPÍTULO VII

DISPOSICIONES COMUNES

Artículo 10.- Abuso de mecanismos y dispositivos informáticos

El que 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. (*)

(*) Artículo modificado por el Artículo 1 de la Ley N° 30171, publicada el 10 marzo 2014, cuyo texto es el siguiente:

"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."

Artículo 11.- Agravantes

El juez aumenta la pena privativa de libertad hasta en un tercio por encima del máximo legal fijado para cualquiera de los delitos previstos en la presente Ley cuando:

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.

"Artículo 12.- Exención de responsabilidad penal

Está exento de responsabilidad penal el que realiza las conductas descritas en los artículos 2, 3, 4 y 10 con el propósito de llevar a cabo pruebas autorizadas u otros procedimientos autorizados destinados a proteger sistemas informáticos." (*)

(*) Artículo incorporado por el Artículo 3 de la Ley N° 30171, publicada el 10 marzo 2014.

DISPOSICIONES COMPLEMENTARIAS FINALES

PRIMERA.- Codificación de la pornografía infantil

La Policía Nacional del Perú puede mantener en sus archivos, con la autorización y supervisión respectiva del Ministerio Público, material de pornografía infantil, en medios de almacenamiento de datos informáticos, para fines exclusivos del cumplimiento de su función. Para tal efecto, cuenta con una base de datos debidamente codificada.

La Policía Nacional del Perú y el Ministerio Público establecen protocolos de coordinación en el plazo de treinta días a fin de cumplir con la disposición establecida en el párrafo anterior.

SEGUNDA.- Agente encubierto en delitos informáticos

El fiscal, atendiendo a la urgencia del caso particular y con la debida diligencia, puede autorizar la actuación de agentes encubiertos a efectos de realizar las investigaciones de los delitos previstos en la presente Ley y de todo delito que se cometa mediante tecnologías de la información o de la comunicación, con prescindencia de si los mismos están vinculados a una organización criminal, de

conformidad con el artículo 341 del Código Procesal Penal, aprobado mediante el Decreto Legislativo 957.

TERCERA.- Coordinación interinstitucional de la Policía Nacional del Perú con el Ministerio Público

La Policía Nacional del Perú fortalece al órgano especializado encargado de coordinar las funciones de investigación con el Ministerio Público. A fin de establecer mecanismos de comunicación con los órganos de gobierno del Ministerio Público, la Policía Nacional del Perú centraliza la información aportando su experiencia en la elaboración de los programas y acciones para la adecuada persecución de los delitos informáticos, y desarrolla programas de protección y seguridad. (*)

(*) Disposición modificada por el Artículo 2 de la Ley N° 30171, publicada el 10 marzo 2014, cuyo texto es el siguiente:

"TERCERA. Coordinación interinstitucional entre la Policía Nacional, el Ministerio Público y otros organismos especializados

La Policía Nacional del Perú fortalece el órgano especializado encargado de coordinar las funciones de investigación con el Ministerio Público. A fin de establecer mecanismos de comunicación con los órganos de gobierno del Ministerio Público, el centro de respuesta temprana del gobierno para ataques cibernéticos (Pe-CERT), la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI) y los Organismos Especializados de las Fuerzas Armadas, la Policía Nacional centraliza la información aportando su experiencia en la elaboración de los programas y acciones para la adecuada persecución de los delitos informáticos, y desarrolla programas de protección y seguridad."

CUARTA.- Cooperación operativa

Con el objeto de garantizar el intercambio de información, los equipos de investigación conjuntos, la transmisión de documentos, la interceptación de comunicaciones y demás actividades correspondientes para dar efectividad a la presente Ley, la Policía Nacional del Perú, el Ministerio Público, el Poder Judicial y los operadores del sector privado involucrados en la lucha contra los delitos informáticos deben establecer protocolos de cooperación operativa reforzada en el plazo de treinta días desde la vigencia de la presente Ley. (*)

(*) Disposición modificada por el Artículo 2 de la Ley N° 30171, publicada el 10 marzo 2014, cuyo texto es el siguiente:

"CUARTA. Cooperación operativa

Con el objeto de garantizar el intercambio de información, los equipos de investigación conjuntos, la transmisión de documentos, la interceptación de

comunicaciones y demás actividades correspondientes para dar efectividad a la presente Ley, la Policía Nacional del Perú, el Ministerio Público, el Poder Judicial, el Pe-CERT (Centro de respuesta temprana del gobierno para ataques cibernéticos), la ONGEI (Oficina Nacional de Gobierno Electrónico e Informática), Organismos Especializados de las Fuerzas Armadas y los operadores del sector privado involucrados en la lucha contra los delitos informáticos deben establecer protocolos de cooperación operativa reformada en el plazo de treinta días desde la vigencia de la presente Ley."

QUINTA.- Capacitación

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

SEXTA.- Medidas de seguridad

La Oficina Nacional de Gobierno Electrónico e Informática (ONGEI) promueve permanentemente, en coordinación con las instituciones del sector público, el fortalecimiento de sus medidas de seguridad para la protección de los datos informáticos sensibles y la integridad de sus sistemas informáticos.

SÉTIMA.- Buenas prácticas

El Estado peruano realiza acciones conjuntas con otros Estados a fin de poner en marcha acciones y medidas concretas destinadas a combatir el fenómeno de los ataques masivos contra las infraestructuras informáticas y establece los mecanismos de prevención necesarios, incluyendo respuestas coordinadas e intercambio de información y buenas prácticas.

OCTAVA.- Convenios multilaterales

El Estado peruano promueve la firma y ratificación de convenios multilaterales que garanticen la cooperación mutua con otros Estados para la persecución de los delitos informáticos.

NOVENA.- Terminología

Para efectos de la presente Ley, se entenderá, de conformidad con el artículo 1 del Convenio sobre la Ciberdelincuencia, Budapest, 23.XI.2001:

a. Por sistema informático: todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, cuya función, o la de alguno de sus

elementos, sea el tratamiento automatizado de datos en ejecución de un programa.

b. Por datos informáticos: toda representación de hechos, información o conceptos expresados de cualquier forma que se preste a tratamiento informático, incluidos los programas diseñados para que un sistema informático ejecute una función.

DÉCIMA.- Regulación e imposición de multas por la Superintendencia de Banca, Seguros y AFP

La Superintendencia de Banca, Seguros y AFP establece la escala de multas atendiendo a las características, complejidad y circunstancias de los casos aplicables a las empresas bajo su supervisión que incumplan con la obligación prevista en el numeral 5 del artículo 235 del Código Procesal Penal, aprobado por el Decreto Legislativo 957.

El juez, en el término de setenta y dos horas, pone en conocimiento del órgano supervisor la omisión incurrida por la empresa, con los recaudos correspondientes sobre las características, complejidad y circunstancias del caso particular, a fin de aplicarse la multa correspondiente.

UNDÉCIMA.- Regulación e imposición de multas por el Organismo Supervisor de Inversión Privada en Telecomunicaciones

El Organismo Supervisor de Inversión Privada en Telecomunicaciones establece la escala de multas atendiendo a las características, complejidad y circunstancias de los casos aplicables a las empresas bajo su supervisión que incumplan con la obligación prevista en el numeral 4 del artículo 230 del Código Procesal Penal, aprobado por el Decreto Legislativo 957.

El juez, en el término de setenta y dos horas, pone en conocimiento del órgano supervisor la omisión incurrida por la empresa, con los recaudos correspondientes sobre las características, complejidad y circunstancias del caso particular, a fin de aplicarse la multa correspondiente. (*)

(*) Disposición modificada por el Artículo 2 de la Ley N° 30171, publicada el 10 marzo 2014, cuyo texto es el siguiente:

"UNDÉCIMA.- Regulación e imposición de multas por el Organismo Supervisor de Inversión Privada en Telecomunicaciones

El Organismo Supervisor de Inversión Privada en Telecomunicaciones establece las multas aplicables a las empresas bajo su supervisión que incumplan con la

obligación prevista en el numeral 4 del artículo 230 del Código Procesal Penal, aprobado por Decreto Legislativo 957.

Las empresas de telecomunicaciones organizan sus recursos humanos y logísticos a fin de cumplir con la debida diligencia y sin dilación la obligación prevista en el numeral 4 del artículo 230 del Código Procesal Penal.

El juez, en el término de setenta y dos horas, pone en conocimiento del órgano supervisor la omisión incurrida por la empresa a fin de que el Organismo Supervisor de Inversión Privada en Telecomunicaciones aplique la multa correspondiente."

DISPOSICIONES COMPLEMENTARIAS MODIFICATORIAS

PRIMERA. Modificación de la Ley 27697, Ley que otorga facultad al fiscal para la intervención y control de comunicaciones y documentos privados en caso excepcional

Modificase el artículo 1 de la Ley 27697, Ley que otorga facultad al fiscal para la intervención y control de comunicaciones y documentos privados en caso excepcional, modificado por el Decreto Legislativo 991 y por Ley 30077, en los siguientes términos: (*) RECTIFICADO POR FE DE ERRATAS

"Artículo 1. Marco y finalidad

La presente Ley tiene por finalidad desarrollar legislativamente la facultad constitucional otorgada a los jueces para conocer y controlar las comunicaciones de las personas que son materia de investigación preliminar o jurisdiccional.

Solo podrá hacerse uso de la facultad prevista en la presente Ley en los siguientes delitos:

1. Secuestro.
2. Trata de personas.
3. Pornografía infantil.
4. Robo agravado.
5. Extorsión.
6. Tráfico ilícito de drogas.

7. Tráfico ilícito de migrantes.

8. Delitos contra la humanidad.

9. Atentados contra la seguridad nacional y traición a la patria.

10. Peculado.

11. Corrupción de funcionarios.

12. Terrorismo.

13. Delitos tributarios y aduaneros.

14. Lavado de activos.

15. Delitos informáticos."

SEGUNDA. Modificación de la Ley 30077, Ley contra el crimen organizado

Modificase el numeral 9 del artículo 3 de la Ley 30077, Ley contra el crimen organizado, en los siguientes términos:

"**Artículo 3.- Delitos comprendidos**

La presente Ley es aplicable a los siguientes delitos:

(...)

9. Delitos informáticos previstos en la ley penal."

TERCERA. -Modificación del Código Procesal Penal

Modificase el numeral 4 del artículo 230, el numeral 5 del artículo 235 y el literal a) del numeral 1 del artículo 473 del Código Procesal Penal, aprobado por Decreto Legislativo 957 y modificado por Ley 30077, en los siguientes términos: (*) RECTIFICADO POR FE DE ERRATAS

"Artículo 230.- Intervención o grabación o registro de comunicaciones telefónicas o de otras formas de comunicación

(...)

4. Los concesionarios de servicios públicos de telecomunicaciones deberán facilitar, en el plazo máximo de treinta días hábiles, la geolocalización de teléfonos móviles y la diligencia de intervención, grabación o registro de las

comunicaciones, así como la información sobre la identidad de los titulares del servicio, los números de registro del cliente, de la línea telefónica y del equipo, del tráfico de llamadas y los números de protocolo de internet, que haya sido dispuesta mediante resolución judicial, en tiempo real y en forma ininterrumpida, las veinticuatro horas de los trescientos sesenta y cinco días del año, bajo apercibimiento de ser pasible de las responsabilidades de ley en caso de incumplimiento. Los servidores de las indicadas empresas deberán guardar secreto acerca de las mismas, salvo que se les citare como testigos al procedimiento. El juez fija el plazo en atención a las características, complejidad y circunstancias del caso en particular.

Dichos concesionarios otorgarán el acceso, la compatibilidad y conexión de su tecnología con el Sistema de Intervención y Control de las Comunicaciones de la Policía Nacional del Perú. Asimismo, cuando por razones de innovación tecnológica los concesionarios renueven sus equipos o software, se encontrarán obligados a mantener la compatibilidad con el Sistema de Intervención y Control de las Comunicaciones de la Policía Nacional del Perú. (*)

(*) Confrontar con el Artículo 6 de la Ley N° 30171, publicada el 10 marzo 2014.

Artículo 235. Levantamiento del secreto bancario

(...)

5. Las empresas o entidades requeridas con la orden judicial deberán proporcionar, en el plazo máximo de treinta días hábiles, la información correspondiente o las actas y documentos, incluso su original, si así se ordena, y todo otro vínculo al proceso que determine por razón de su actividad, bajo apercibimiento de las responsabilidades establecidas en la ley. El juez fija el plazo en atención a las características, complejidad y circunstancias del caso en particular.

Artículo 473.- Ámbito del proceso y competencia

1. Los delitos que pueden ser objeto de acuerdo, sin perjuicio de los que establezca la Ley, son los siguientes:

   a) Asociación ilícita, terrorismo, lavado de activos, delitos informáticos, contra la humanidad;"

CUARTA.- Modificación de los artículos 162, 183-A y 323 del Código Penal

Modificase los artículos 162, 183-A y 323 del Código Penal, aprobado por el Decreto Legislativo 635, en los siguientes términos:

"Artículo 162.- Interferencia telefónica

El que, indebidamente, interfiere o escucha una conversación telefónica o similar será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años.

Si el agente es funcionario público, la pena privativa de libertad será no menor de cuatro ni mayor de ocho años e inhabilitación conforme al artículo 36, incisos 1, 2 y 4.

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 las normas de la materia.

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

(*) Confrontar con el Artículo 4 de la Ley N° 30171, publicada el 10 marzo 2014.

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 323.- Discriminación

El que, por sí o mediante terceros, discrimina a una o más personas o grupo de personas, o incita o promueve en forma pública actos discriminatorios, por motivo racial, religioso, sexual, de factor genético, filiación, edad, discapacidad, idioma, identidad étnica y cultural, indumentaria, opinión política o de cualquier índole, o condición económica, con el objeto de anular o menoscabar el reconocimiento, goce o ejercicio de los derechos de la persona, será reprimido con pena privativa de libertad no menor de dos años ni mayor de tres o con prestación de servicios a la comunidad de sesenta a ciento veinte jornadas.

Si el agente es funcionario o servidor público, la pena será no menor de dos ni mayor de cuatro años e inhabilitación conforme al numeral 2 del artículo 36.

La misma pena privativa de libertad señalada en el párrafo anterior se impondrá si la discriminación se ha materializado mediante actos de violencia física o mental, o si se realiza a través de las tecnologías de la información o de la comunicación." (*)

(*) Confrontar con el Artículo 4 de la Ley N° 30171, publicada el 10 marzo 2014.

DISPOSICIÓN COMPLEMENTARIA DEROGATORIA

ÚNICA. Derogatoria

Deróguese el numeral 4 del segundo párrafo del artículo 186 y los artículos 207-A, 207-B, 207-C y 207-D del Código Penal. (*) RECTIFICADO POR FE DE ERRATAS

Comuníquese al señor Presidente Constitucional de la República para su promulgación.

En Lima, a los veintisiete días del mes de setiembre de dos mil trece.

FREDY OTÁROLA PEÑARANDA

Presidente del Congreso de la República

MARÍA DEL CARMEN OMONTE DURAND

Primera Vicepresidenta del Congreso de la República

AL SEÑOR PRESIDENTE CONSTITUCIONAL DE LA REPÚBLICA

POR TANTO:

Mando se publique y cumpla.

Dado en la Casa de Gobierno, en Lima, a los veintiún días del mes de octubre del año dos mil trece.

OLLANTA HUMALA TASSO

Presidente Constitucional de la República

JUAN F. JIMÉNEZ MAYOR

Presidente del Consejo de Ministros