



**FACULTAD DE DERECHO Y HUMANIDADES  
ESCUELA PROFESIONAL DE DERECHO**

**TESIS**

**MODIFICACIÓN DE LA LEY 30096 PARA  
INCORPORAR LOS DELITOS DE PHISHING,  
PHARMING Y CARDING COMO DELITOS  
PENALIZABLES CON PRISIÓN, PARA REDUCIR  
LA CIBERDELINCUENCIA, LIMA 2019.**

**PARA OPTAR EL TÍTULO PROFESIONAL DE ABOGADA**

**Autor:**

**Bach. Fuentes Garrido, Karla Vanessa**

**<https://orcid.org/0000-0002-8072-760X>**

**Asesor:**

**Dr. Uchofen Urbina Angela Katherine**

**<https://orcid.org/0000-0002-9705-0615>**

**Línea de Investigación:**

**Ciencias Jurídicas**

**Pimentel – Perú**

**2021**

## Aprobación del Jurado

---

Dr. Jesús Manuel Gonzáles Herrera

**PRESIDENTE**

---

Mg. Daniel Guillermo Cabrera Leonardini

**SECRETARIO**

---

Mg. Carlos Andree Rodas Quintana

**VOCAL**

## **Dedicatoria:**

Dedico el presente trabajo de investigación a Dios, nuestro Padre, quien con su magia que nos transmite día a día puede regalarnos la magia de encontrarnos vivos, y que en estos tiempos difíciles que nos encontramos atravesando me ha enseñado a ser fuerte y enfrentar los desafíos con fortaleza y además, por permitirme el haber llegado hasta este momento tan importante de mi formación académico profesional. A mis padres y hermanos, quienes siempre de alguna u otra manera me demuestran su amor y apoyo incondicional sin importar la circunstancia en la que nos encontremos.

## **Agradecimiento:**

A todas aquellas personas, mis padres, hermanos, compañeros y amigos, quienes en todo momento me han brindado su cariño, apoyo, fortaleza y tiempo para continuar con cada paso de mi carrera profesional y cumplir con ello las metas trazadas, sobre todo en este tiempo muy difícil que nos encontramos atravesando frente a la lucha contra el Covid19, quien su presencia no solo ha dificultado en gran medida nuestro desarrollo personal y familiar sino también académico.

La autora

## Resumen

La presente investigación tiene como objetivo principal justificar por qué los delitos de Phishing, Pharming y Carding deben ser incorporados a la Ley N°30096 como delitos penalizables con penas privativas de la libertad, para ello debe tenerse en consideración que investigar el delito desde cualquier ámbito es hoy en día una actividad muy compleja. Actualmente el auge de la cibercriminalidad va en aumento, generando los llamados delitos informáticos ya que para su consumación se requiere emplear medios electrónicos, ejemplo de estos delitos son: el hacking, propaganda maliciosa de un virus, pornografía infantil y agresión a proveedores de Internet son los delitos informáticos más y más comunes en nuestro país.

Por ello, el Parlamento Peruano promulgó la Ley N°30096, denominada Ley de Delitos Informáticos, modificada posteriormente por la Ley N°30171, la misma que describe que, con tan solo tener acceso a Internet, muchos de los usuarios están expuestos a una cadena de delitos que se cometen incorporando las nuevas tecnologías y avances digitales, según la ley violando la confidencialidad, integridad y la información; asimismo, la citada norma incorporó una serie de delitos informáticos, dentro de los que se encuentran interceptación de información, suplantación de identidad, entre otros, a estos tipos penales se les establecieron sanciones penales con la finalidad de contrarrestar su consumación, razón por la cual es imprescindible que también se incorporen a esta gama de delitos las modalidades delictivas de Phishing, Pharming y Carding como delitos penalizables con prisión, a fin de reducir la ciberdelincuencia en la ley N°30096.

**Palabras clave:** Carding, Ciberdelito, Fraude, Pharming, Phishing, Sistema de Información, Tipificación, Tráfico de datos.

## Abstrac

The main objective of this research is to justify why the crimes of Phishing, Pharming and Carding should be incorporated into Law No. 30096 as crimes punishable by custodial sentences, for this it must be taken into consideration that investigating the crime from any scope It is a very complex activity today. Currently, the rise of cybercrime is on the rise, generating so-called computer crimes since their consummation requires the use of electronic means, examples of these crimes are: hacking, malicious propaganda of a virus, child pornography and aggression against Internet providers are the most common computer crimes in our country.

For this reason, the Peruvian Parliament enacted Law 30096, called the Computer Crimes Law, later modified by Law 30171, which describes that, just by having access to the Internet, many of the users are exposed to a chain of crimes that They are committed incorporating new technologies and digital advances, according to the law, violating confidentiality, integrity and information; Likewise, the aforementioned norm incorporated a series of computer crimes, among which are other interception of information, identity theft, among these criminal types, criminal sanctions were established in order to counteract their consummation, which is why It is essential that the criminal modalities of phishing, pharming and carding are also incorporated into this range of crimes as crimes punishable by imprisonment, in order to reduce cybercrime in Law 30096.

**Keyword:** Carding, Cybercrime, Fraud, Pharming, Phishing, Information System, Typification, Data traffic

## ÍNDICE

I. INTRODUCCIÓN.....	9
1.1. Realidad Problemática .....	10
1.1.1 A nivel internacional .....	10
1.1.2. A nivel nacional.....	11
1.2. Antecedentes de estudio.....	13
1.2.1. A nivel internacional:.....	13
1.2.2. A nivel nacional:.....	15
1.3. Abordaje teórico .....	17
1.3.1 Variable independiente: Modificación de la Ley N°30096 .....	17
1.3.2. Variable dependiente: Incorporar delitos de phishing, pharming y carding .....	24
1.3.3. Derecho Comparado .....	27
1.4. Formulación del Problema. ....	31
1.5. Justificación e importancia del estudio. ....	31
1.6. Hipótesis.....	32
1.7. Objetivos .....	32
1.7.1. Objetivo General.....	32
1.7.2. Objetivos Específicos.....	32
1.8. Limitaciones .....	32
II. MATERIAL Y MÉTODO.....	32
2.1. Tipo de estudio y diseño de la investigación .....	32
2.1.1 Tipo de estudio .....	32
2.1.2 Diseño de investigación .....	33
2.2.1 Población .....	33
2.2.2. Muestra.....	33
2.3. Variables, Operacionalización.....	33

2.4. Técnicas e instrumentos de recolección de datos. ....	33
2.4.1. Técnicas .....	33
2.4.2. Instrumentos .....	34
2.5.    Procedimientos para la recolección de datos. ....	34
2.6.    Aspectos éticos .....	34
2.7.    Criterios de Rigor científico. ....	34
III. REPORTE Y RESULTADOS .....	36
3.1. Tablas y figuras.....	36
3.2. Discusión de resultados .....	45
3.3. Aporte científico .....	49
IV.    CONCLUSIONES Y RECOMENDACIONES .....	50
REFERENCIAS .....	53
ANEXOS .....	58



## I. INTRODUCCIÓN

Actualmente el uso de la tecnología es casi toda actividad que realiza la sociedad, desde los más pequeños hasta los más grandes; no obstante, este medio viene siendo utilizado de manera maliciosa, razón por la cual se busca ejecutar investigaciones al respecto y reglamentar este tipo de conductas que perturban la tranquilidad de cualquier ser humano, ello con la finalidad de resguardar derechos fundamentales. Muestra de este tipo de conductas es lo manifestado por la División de Alta Tecnología de la Policía Nacional del Perú que se encuentra en la ciudad de Lima, quienes en los últimos años registraron un gran aumento de denuncias en lo que respecta a delitos informáticos. Sin embargo, en el Perú la legislación penal general y especial todavía no regula completamente los diversos comportamientos delictivos derivados a través del uso indiscriminado de los denominados campos virtuales como lo son: las páginas web, internet, diversas redes sociales, entre otras.

Es por ello, que el desarrollo del presente trabajo se busca respuesta a la pregunta ¿Permitirá la modificación de la ley 30096 para incorporar los delitos de phishing, pharming y carding como delitos penalizables con prisión reducir la ciberdelincuencia, Lima 2019?, para tal efecto se planteó el siguiente objetivo general justificar por qué los delitos de phishing, pharming y carding deben ser incorporados a la Ley N°30096 como delitos penalizables con penas privativas de la libertad. Asimismo, la presente investigación se desarrollará teniendo en cuenta los trabajos previos relacionados con el tema objeto de estudio, la doctrina, el análisis de documentos y el derecho comparado.

El presente trabajo de investigación fue de suma importancia, ya que abordó un tema que hoy en día está muy presente en nuestras actividades cotidianas, como es el uso del internet y a qué nos podemos estar enfrentando.

En el capítulo I, se describió la realidad problemática con relación a los nuevos eventos delictivos ejecutados mediante medios electrónicos. Por otro lado, se formuló la pregunta de investigación, así como el objetivo general que se busca desarrollar; además, se expuso la importancia y los motivos que justifican la presente investigación; así como limitaciones que se superaron durante el

desarrollo del presente trabajo de investigación. Asimismo, se elaboró el marco teórico, dentro del cual se describe las investigaciones anteriores relacionadas al tema y los fundamentos teóricos que sirve como base fundamental de problema planteado.

En el capítulo II, se explica la parte metodológica tomada en consideración para el desarrollo de la presente investigación, es decir: tipo y diseño, además de establecer las técnicas e instrumentos utilizados en la recolección de datos.

Finalmente, en el capítulo III, se estableció el análisis y la discusión de los resultados obtenidos a través del análisis documental, teniendo presente los objetivos; y posterior a ellos se elaboran consideraciones finales.

## **1.1. Realidad Problemática**

### **1.1.1 A nivel internacional**

A fin de contrarrestar los nuevos eventos delictivos que han visto su mayor auge en el año 2019 y este último año 2020 (respecto de otros años) ya que por la nueva realidad a la que a nivel mundial nos estamos adaptando, los seres humanos realizamos transacciones (compras, ventas, pagos, operaciones en banca, etc.) vía online, la población se ha visto afectada por las nuevas formas de “hechos delictivos” que no se están viendo en la calle como se podría ver anteriormente, sino que estos, se están dando en la red – internet.

En España, según el Informe sobre el estado de internet en materia de seguridad de Akamai, las estafas virtuales ascendieron en un 45% más en comparación al año 2019, produciendo una pérdida de aproximadamente \$/3,400.00 millones de dólares; estas estafas se realizaron bajo diversas modalidades cibernéticas dentro de las que se encuentra el phishing.

En México, la Covid19 incrementó el número de ataques cibernéticos, la mayoría de ellos realizados por correo electrónico y es que diariamente se bloquean 324 mil amenazas de estafa, es decir, se reciben aproximadamente 225 por minuto y 4 por segundo; ello se debe a que

los cibercriminales han implementado nuevas modalidades para delinquir (Forbes, 2021)

#### 1.1.2. A nivel nacional

En el Perú se promulgó una Ley penal especial cuyo propósito fue advertir y condenar las conductas ilícitas que afectan los sistemas y datos informáticos, así como el secreto de las comunicaciones, y otros bienes jurídicos protegidos que resulten dañados con esta modalidad delictiva, como son el patrimonio, la fe pública, orden financiero y monetario, así como la independencia sexual.

Es de esta forma, que el 22 de octubre de 2013 se publicó la Ley N°30096, Ley de delitos informáticos, que posteriormente fue modificada por la Ley N°30171 el 10 de marzo de 2014, esta Ley en lugar de iniciar y abarcar temas no contenidos en el Código Penal actual y la Ley N°30096, presentó también muchas inconsistencias y vacíos en su regulación de delitos informáticos, inclusive en el extremo de sistematizar lo ya determinado en el Código Penal vigente de 1991 presentándose un exceso de regulación normativa, por cuanto si tenemos en cuenta que a medida que la globalización alcanza límites no antes vistos, nuestro ordenamiento jurídico debería ir a la par de ello para así tratar de contrarrestar lo que vulnera hoy en día con gran magnitud lo que son atentados contra el sistema informático como lo son el PHISHING, PHARMING Y CARDING, estableciendo rigurosamente las diferencias y precisiones de cada uno de ellos.

El Código Penal Peruano tipificaba en su CAPÍTULO X “*Delitos Informáticos*” capítulo que habría sido incorporado por el artículo único de la Ley N° 27309 el 17/07/2000, y se habría expresado mediante los artículos 207-A al 207-D los diferentes tipos penales presentados para este tipo de violación al bien jurídico y que por consiguiente fueron derogados por la Única Disposición Complementaria Derogatoria de la Ley N°30096 publicada el 22 de octubre de 2013, la misma que como se mencionó en líneas precedentes fue modificada por la Ley N° 30171, el artículo 207-A que se habría contemplado en el Código Penal el que

finalmente expresaba “*el que utiliza o ingresa indebidamente a una base de datos, sistema de red de computadoras o cualquier parte de la misma, para diseñar, ejecutar o alterar un esquema u otro similar, o para interferir, interceptar, acceder o copiar información en tránsito o contenida en una base de datos, será reprimido con pena privativa de libertad no mayor de dos años o con prestación de servicios comunitarios de cincuenta y dos a ciento cuatro jornadas.*”

Actualmente los conjuntos informáticos no solo son usados como herramientas auxiliares frente a las múltiples ocupaciones que se ejercen diariamente, sino que además se hallan en un grado que posibilita obtener y lograr información, por lo cual son consideradas como medios de comunicación, debido a ello la informática está vigente en casi todas las ocupaciones de los individuos y son usadas en labores que anticipadamente sólo se realizaban de modo manual, esto conlleva a que se digitalice la información siendo almacenada en computadoras, servidores y/o medios virtuales, dejándola propensa a ser suscitada sin permisión.

El adelanto en el ejercicio, potencia y variabilidad del software-equipos informáticos fue tan inmediata que precedentemente se podía poseer la completa convicción que nadie era competente para sustraer información específica, sin embargo, gracias a la expansión de la globalización y de los procesos de la expansión de las industrias computacionales e informáticas, ha permitido la edificación de un sistema, que puede almacenar gigantes porciones de información y transmitirla en instantes, cada vez más personas acceden a estos contenidos, sin que las legislaciones sean capaces de regularlos.

Los avances tecnológicos en todo el mundo, así como el desarrollo de la función de almacenamiento que poseen los conjuntos electrónicos en este momento, realizan más difíciles las labores de vigilancia, por lo que resulta complejo legislar tal proporción de dispositivos a la par con el comportamiento de sus usuarios que también permanecen influenciados por las presiones sociales que incitan a las masas a buscar novedosas maneras de obtener dinero. Por ello, resulta

fundamental inspeccionar de modo paralelo a los adelantos tecnológicos y la predominación que se ha ejercido en el ambiente de cada uno de los individuos; los delitos informáticos descritos anteriormente se han venido desarrollado paralelamente a las tecnologías de la información, por lo que la sociedad en su conjunto se ha visto sumergida en un progreso y perfeccionamiento en todas sus zonas, donde la delincuencia ha sido beneficiada, hoy poseen la función de realizar un hecho ilícito a partir de cualquier área del mundo, con un gigantesco ingreso informático, a través del anonimato. Las causas recientemente mencionadas en líneas precedentes son las que demuestran el valor e importancia del “problema” de la averiguación sobre las novedosas maneras jurídicas y forma en cómo se estarían regulando, siendo de esta forma que la investigación presentada mediante este trabajo ha fijado la labor de puntualizar la importancia de la categorización de los delitos de Phishing, Pharming y Carding dentro de la Ley N°30096 y así contrarrestar estos delitos informáticos, sus propiedades y asimismo explicar que la legislación vigente presenta vacíos con respecto a las medidas consideradas hasta ahora en las normativas nacionales.

## **1.2. Antecedentes de estudio.**

### 1.2.1. A nivel internacional:

Alkhalil y et al. (2021) en su artículo *“Phishing Attacks: A Recent Comprehensive Study and a New Anatomy”* exponen que el avance de las nuevas tecnologías trajo consigo nuevas modalidades de acciones delictivas, como es el caso del phishing, el mismo que es un delito cibernético que le permite a los ciberdelincuentes recopilar información importante de los usuarios para finalmente robarles o estafarlos. El primer ciberataque bajo la modalidad de phishing se reportó en 1990, siendo catalogado como uno de los ataques más sofisticados. Actualmente se han implementado estrategias para detectar el phishing, sin embargo, debido al avance constante de la tecnología este delito sigue siendo uno de los más usados por los delincuentes,

los mismos que emplean entre sus métodos tradicionales los correos electrónicos y las páginas web.

Herrera (2016) en su tesis *“El Phishing como delito informático y su falta de tipificación en el Código orgánico Integral Penal”* mencionó que el phishing es una modalidad de delito informático que se ha incrementado significativamente en los últimos años, teniendo como objetivo general determinar que la falta de tipificación de dicho delito genera impunidad, puesto que ello generará seguridad en los usuarios al ser víctimas de algún tipo de delito informático y denunciar tal hecho, no obstante como no se encuentra regulado en el ordenamiento jurídico es imposible su desarrollo en el proceso penal. El autor arribó a las siguientes conclusiones: el delito de Phishing al no encontrarse tipificado promueve la desprotección jurídica y consecuente la tutela de derechos, las autoridades desconocen de la consumación de conductas informáticas que perjudican enormemente a las personas como el caso del phishing, es necesario su adhesión al Convenio de Cibercriminalidad de Budapest ya que es el único referente a la ciberdelincuencia y el delito de Phishing es un delito informático sumamente peligroso que vulnera no sólo la propiedad sino también la intimidad de la sociedad, razón por la cual debe reglarse en el Código Orgánico Integral Penal.

López (2019) en su tesis *“Métodos y técnicas de detección temprana en casos de phishing”* sostiene que el phishing es uno de los fraudes que más dinero les cuesta a las compañías ya que se estima que anualmente pierden 1,6 millones de euros. Por ello, para lograr contrarrestar este tipo de delito se requiere una detección temprana de los sitios web falsos a fin de evitar que las personas sufran estafas o robos. Dentro de las técnicas de detección temprana se encuentran los certificados de transparencia, Referers, los typo-squatting, OSINT, los sistemas de análisis basados en IOCs y la identificación de correos electrónicos a través del SPF, DKIM, DMARC. Finalmente, el autor concluye que no sólo deben establecer técnicas de detección temprana

sino también un sistema de monitoreo que permita seguir las páginas falsas en el momento determinado.

#### 1.2.2. A nivel nacional:

Moncada (2020) en su tesis *“Comparación de técnicas de machine learning para detección de sitios web de phishing”* menciona que el phishing consiste en el robo de datos a través de la creación de páginas falsas, la víctima de este delito es redirigida a una website que él considera segura pero que realmente es falsa, en este tipo de páginas se le solicita a los usuarios ingresar sus datos a fin de validar su identidad, es en ese momento donde el hacker aprovecha para realizar compras a nombre del usuario, generando estafas o robos. Por ello, la presente investigación tenía como finalidad establecer diversas formas de detección a fin de determinar qué páginas web son falsas, empleando para ello la técnica de machine learning, obteniendo como resultados que los clasificadores de bosque aleatorio y árbol de decisión han obtenido un nivel de eficacia ente 97% y 99% en la detención de las páginas phishing.

Zorrilla (2018) en su tesis *“Inconsistencias y ambigüedades en la Ley de delitos informáticos Ley N°30096 y su modificatoria Ley N°30171, que imposibilitan su eficaz cumplimiento”* tiene como objetivo general determinar de qué manera se exponen las inconsistencias y ambigüedades en la ley N°30096. El diseño de la investigación fue no experimental ya que no se manipularon las variables de estudio, para recoger información relevante se utilizaron las técnicas de análisis de documentos y la encuesta, la cual fue aplicada a 30 profesionales del derecho. Finalmente, se concluye delimitando que la Ley N°30096 posee diversos artículos incoherentes que genera confusión al momento de su aplicación, la norma legisla el medio a través del cual se comete el ilícito más no regula conducta y busca regular aquellas que ya se encuentran establecidas en la norma penal adjetiva. En el Perú no existe un texto normativo que determine de manera específica

los tipos penales que definan los delitos que se cometen con mayor frecuencia en redes sociales, por tanto, es necesario sancionar correctamente y la falta de cultura informática es un factor determinante en la comisión de delitos informáticos, es por ello que es necesario contar con profesionales especialista en la materia.

Sequeiros (2016) en su tesis *“Vacíos legales que imposibilitan la sanción de los delitos informáticos en el Nuevo Código Penal Peruano - 2015”* sostiene que si bien la emisión de la Ley N°30096 tiene como finalidad sancionar y prevenir la comisión de ilícitos informáticos. Por último, el autor concluye mencionando que la falta de información respecto a los límites de los delitos informáticos ocasiona impacto en los delitos informáticos ya que impiden conocer de manera íntegra el manejo de determinadas situaciones, a su vez existe la necesidad de fortalecer el uso de tecnología con la finalidad de que el usuario sienta seguridad al realizar actos tecnológicos, más no la privación de estos. Por ello, recomienda que es necesario generar espacios de comunicación con las autoridades competentes a fin de enfrentar esta nueva forma de delinquir, es decir definir la normativa desde la realidad de nuestro país.

Herrera (2018) en su tesis *“Eficacia de la ley de delitos informáticos en el distrito judicial de Huánuco 2017”* señala que uno de los problemas que aqueja a la sociedad es la nueva forma de criminalidad a través de las plataformas tecnológicas, es por ello que planteó como objetivo general demostrar el nivel de eficacia que ofrece la ley de delitos informáticos. Para llevar a cabo dicha investigación se empleó un enfoque mixto, diseño descriptivo y tipo básico. Asimismo, la técnica utilizada fue la encuesta de la cual se obtuvieron datos exactos y fidedignos respecto a la ley N°30096, ley de delitos informáticos. Las conclusiones determinan que la eficacia de los delitos informáticos es baja toda vez que posee deficiencias en cuanto a su aplicación, a su vez no existen juzgados especializados en estos delitos y la falta de profesionales capacitados en delitos de esta materia, lo cual dificulta su desarrollo en la práctica jurídica.



Alvarado (2017) en su tesis *“Análisis de las vulnerabilidades mediante el uso de phishing para mejorar la seguridad informática de los equipos de cómputo y redes de la Municipalidad distrital de Independencia”* señala tiene por finalidad analizar el uso del phishing a fin de mejorar la seguridad informática, para desarrollar la investigación empleó una investigación exploratoria, descriptivo y no experimental; además se aplicó un cuestionario a una muestra conformada por 20 personas que laboraban en la Subgerencia de tecnología de información y Comunicaciones de la Municipalidad y personal Administrativo, Auxiliar de distintas áreas. Sus conclusiones están orientadas a determinar que la municipalidad puede contar con mejores equipos y mejor software, no obstante, es fundamental promover la conciencia de los delitos informáticos, el compromiso de los trabajadores y la capacitación de los mismos para un mejor desempeño laboral.

### **1.3. Abordaje teórico**

#### **1.3.1 Variable independiente: Modificación de la Ley N°30096**

##### **1.3.1.1 Antecedentes generales sobre la regulación de delitos informáticos**

La globalización trae consigo diversos cambios, uno de ellos son los avances tecnológicos a través de la tecnología informática y comunicación empleada por la sociedad. Sin embargo, de acuerdo con el Informe doceavo Congreso de los países Unidos sobre Prevención del Delito y Justicia Penal los avances tecnológicos no solo generan ventajas en el mundo social, sino que también es una nueva modalidad de cometer hechos ilícitos, como el fraude y pornografía infantil, que si bien no son delitos nuevos, la tecnología se ha convertido en una nueva modalidad de llevar a cabo dichos ilícitos. Los delitos más consumados a través de la tecnología se basan en extraer información importante de los usuarios a través de redes informáticas, el envío de correspondencia masiva e ilícita para la obtención de datos personales, el phishing, difusión de virus y otras conductas.

En esta línea el Convenio de Budapest el cual se refiere a la ciberdelincuencia, tiene como finalidad determinar aquellas conductas que vulneran especialmente los datos personales y financieros de las personas, el cual fue incorporado especialmente como un llamado a los países europeos puesto que son aquellos que contaban con una tecnología privilegiada y actualizada, advirtiendo que diversos hechos con el empleo de la tecnología vulneraban datos personales a través del ingreso a computadoras, tablets, celulares, entre otros.

Es por ello que en 1995 se invitó a algunos expertos en informática a fin de desarrollar el sistema informático, los cuales plasmaron dicho convenio y fue aprobado en el año 2001. Mientras que en el Perú aprobó el convenio el 12 de febrero de 2019 mediante la Resolución Legislativa N°30913, que tuvo como resultado la habituación de la propia legislación a este convenio.

De la misma forma, en el Perú se promulgó la Ley N°30096, Ley de delitos informáticos, publicada en el año 2013, la cual regula hechos delictivos a través del uso de sistemas digitales de información, a su vez es importante mencionar que los delitos informáticos han sido regulados también en el Código Penal Peruano, en el Título V, Capítulo X, incorporados en el año 2000 a través de la Ley N°37309 y posteriormente derogados por la Ley N°30096.

En esta línea, los delitos informáticos actualmente se encuentran regulados mediante la Ley N°30096, no obstante, persisten diversos vacíos legales, toda vez que no todos los delitos se han abordado en dicha normativa, teniendo en cuenta que existen nuevas formas de delinquir a través del sistema informático.

En nuestro país, los delitos informáticos más frecuentes a través de las denuncias realizadas al Ministerio Público o Policía Nacional son el fraude, propaganda maliciosa de virus a fin de obtener datos de información personal y financiera, hacking, terrorismo, pornografía infantil, envío de correos electrónicos para conseguir datos conocidos como phishing (información privada como claves de cuentas bancarias, y acceso a correos electrónico), carding (datos de tarjetas de crédito

y/o débito, clonación de tarjetas, obtención de información personal y empresarial, ataques a los proveedores de Internet), y el pharming que mediante el uso de mecanismos para dirigir a los usuarios a sitios web falsos, entre otros novedosos actos criminales valiéndose de tecnologías empresariales para cometer estos actos criminales como los antes descritos y que no se encuentran regulados en nuestra legislación peruana. En este sentido, se puede inferir que si bien la tecnología nos ofrece una diversidad de beneficios y a su vez evoluciona constantemente, como por ejemplo la rapidez para realizar determinados actos, accesibilidad al realizarlos desde el lugar que nos encontremos, fluidez para navegar por la red, poder comunicarnos con otras personas sin importar el lugar en el que se encuentren, mejorar los estudios y trabajo, entre otros; no obstante su desarrollo ha traído consigo una ola de criminalidad, denominada como cibercriminalidad, la cual ha sido empleada por personas inescrupulosas que se valen de estos medios para delinquir con el objeto de obtener datos personales y financieros y así beneficiarse. Por tanto, el Estado se ha visto en la necesidad buscar mecanismos que brinden seguridad a los ciudadanos, uno de ellos la regulación de la Ley N°30096. (Hugo, 2014)

#### 1.3.1.2. Delitos informáticos

De acuerdo con Espinoza (2017) el delito informático se empleó por primera vez en el año 1990, a partir de ese momento los avances tecnológicos fueron desarrollándose significativamente y por tanto delinquir a través del sistema informático con mayor amplitud. La criminalidad informática incluye delitos como el fraude, chantaje, falsificación, robo y además redes que fueron utilizados para la consecución de estos hechos delictivos.

Según Sánchez (2016) el delito informático es un delito que merece ser sancionado penalmente, ello quiere decir que debe encontrarse regulado en la norma penal, por tanto, al ser tipificado y declarado como una conducta antijurídica merece una sanción penal. Por tanto, se entiende como delito informático como aquella conducta ilegal que es

contraria a la norma y que es llevada a cabo a través del uso del sistema informático.

De la misma forma, Herrera (2016) menciona que, si bien el avance tecnológico constituye una herramienta imprescindible hoy en día, ha venido también acompañado de diversos hechos delictivos, motivo por el cual es necesario estudiar su accionar para así poder tomar las medidas necesarias y enfrentar la cibercriminalidad que se viene dando en la actualidad. Es por ello que al realizar alguna acción que requiera el uso de redes a través de la web, debe tener en cuenta las garantías que generan seguridad en la navegación de los sitios web, y permitan a los usuarios realizar actividades sin temer que sus datos y base financiera se encuentra en peligro.

Levin y Ilkina (2013) señala que los delitos informáticos se constituyen porque para su consumación se requiere del empleo de herramientas electrónicas como computadoras, laptops, tablets, entre otras.

Villavicencio (2014) por su lado sostiene que estos delitos se constituyen por aquellas acciones dirigidas a burlar diversos sistemas de seguridad, a fin de obtener información de las víctimas y así poder estafarlas o robarles.

En esta línea de ideas se puede inferir que para la configuración de dicho tipo penal es necesario que el sujeto activo emplee un medio informático.

#### 1.3.1.3. Seguridad informática

Las políticas de estabilidad informática se han convertido en una forma de comunicarse con las personas, toda vez que a través de ellas se determinan canales de comunicación a fin de interactuar los recursos y servicios informáticos. En este sentido, las políticas de estabilidad o seguridad tienen una postura preventiva respecto al uso y los peligros que trae consigo las redes del sistema informático, para así enfrentar los ataques cibernéticos de los cuales se puede ser víctima en la actualidad. Por tanto, constituye un mecanismo de suma importancia al

momento de realizar determinadas acciones como por ejemplo transacciones, educación a distancia, pagos, teletrabajo, compras por internet, otros, toda vez que frente a la realidad que suscita en la actualidad, en donde el internet se ha convertido en un arma de doble filo, es necesario contar con una herramienta que brinde seguridad a las personas, frente a los distintos delitos informáticos que se vienen desarrollando. (Romero et al., 2018)

#### 1.3.1.4. Regulación de los delitos informáticos en la legislación peruana

El delito informático es uno de los tipos penales que más modificaciones ha sufrido, primigeniamente este tipo penal se encontraba estipulado en el Código Penal de 1991, precisamente en el inciso 3 segundo párrafo del artículo 186. Sin embargo, dicha tipificación no era autónoma, sino que se encontraba establecida como una agravante del delito de hurto.

Posteriormente, estos delitos fueron establecidos en el Capítulo X de la norma adjetiva penal, en los artículos 207-A titulado como delito informático, uso e ingreso indebido de datos, sistema o red; así mismo en el artículo 207-B se establecía la alteración, daño o destrucción de base de datos); en el artículo 207-C se señalaron las circunstancias cualificantes agravantes y finalmente en el artículo 207-D se estableció el tráfico ilegal de datos.

Sin embargo, en el año 2013 dichos artículos fueron derogados debido a la entrada en vigencia de la ley N°30096. Esta ley está constituida por siete capítulos, el primero de ellos establece las: finalidades y objeto de la ley; el segundo de ellos señala los delitos contra datos; el tercero de ellos prescribe los delitos informáticos contra la indemnidad y libertad sexual; el cuarto de ellos señala los delitos informáticos contra la intimidad y el secreto de las comunicaciones; el quinto de ellos estipula los delitos informáticos contra el patrimonio; en el sexto de ellos señala los delitos informáticos contra la fe pública y finalmente en el séptimo capítulo se establecen las disposiciones comunes.

Tiempo después, se promulgó la Ley N°30171 modificando así los artículos 2, 3, 4, 7, 8 y 10 de la Ley N°30096 ya que se buscaba que la mencionada norma cumpla con los estándares establecidos por el Convenio de Budapest (Villavicencio, 2014). Consecuentemente las normas que rigen la delincuencia cibernética en el Perú son las mencionadas.

#### 1.3.1.5. Tipos de Delitos informáticos

Según Pardo (2018) los delitos informáticos se dividen en las siguientes categorías:

- El ingreso no autorizado: este se refiere al ingreso sin derecho o permiso a un sistema o red, por tanto, se contraviene con los lineamientos establecidos, más conocido como hacking.
- Deterioro de datos, información o programas informáticos: se basa en la exclusión de datos relevantes sin que el titular haya realizado dicha acción.
- El sabotaje informático: versa en la alteración de sistemas que interfiere en los sistemas informáticos mediante la red, impidiendo el normal funcionamiento de las redes.
- La interceptación no autorizada: esta se basa en la captación sin permiso por medio de los medios tecnológicos.
- Espionaje informático: uno de los métodos más empleados mediante el cual se compra o transfiere información de carácter confidencial sin autorización alguna, con el objeto de generar pérdidas económicas u otros beneficios.

#### 1.3.1.6. La tipicidad en los Delitos Informáticos

La tipificación de un delito se relaciona directamente con la descripción del acto delictivo, el mismo que puede estar compuesto por una omisión o por unas acciones consideradas como delitos en el ordenamiento normativo.

Doctrinariamente se afirma que un accionar es típico cuando se encuentre dentro del marco normativo establecido por cada Estado,

teniendo como base el principio de legalidad ya que como señala Grisanti (1989) la tipificación se refleja cuando el hecho encaja directamente con el tipo penal.

En los delitos informáticos la tipificación resulta ser un elemento imprescindible debido a que si los actos lesivos no se encuentran estipulados dentro de leyes especiales o de la norma adjetiva penal, las conductas no podrán ser sancionadas.

Dentro de la ley de Delitos Informáticos se tipificó que la acción típica se realizaba cuando el sujeto activo ingresaba de manera deliberada a un sistema, vulnerado el sistema de seguridad impuesto. Este tipo de criminalidad en la actualidad se encuentra en aumento, generando una serie de pérdidas financieras debido a los fraudes cometidos por una o un grupo de personas.

Por otro lado, cabe mencionar que este tipo penal puede ser realizado por cualquier persona que cuente con conocimientos informáticos y de sistemas que le permita acceder sin conflicto a sistemas públicos o privados a fin de obtener información. Y al ser un tipo penal que no conoce fronteras se permite que exista participación de diversos países.

De esta manera, la clasificación de delitos como Phishing, Pharming y Carding son cruciales en las leyes especiales que regulan los delitos informáticos, porque permite a los legisladores clasificar estas acciones como delitos, analizando los bienes jurídicos protegidos en los delitos informáticos.

#### 1.3.1.7. Bienes Jurídicos protegidos en los delitos informáticos

Los bienes jurídicos protegidos en los distintos delitos informáticos regulados a través de la Ley N°30096, la cual fue modificada posteriormente por la Ley N°30171, se estima de manera conjunta puesto que no solo vulnera un determinado bien jurídico, sino que puede vulnerar más de un bien jurídico a la vez, entre ellos: sistemas informáticos, contra la indemnidad y libertad sexual, secreto de comunicaciones, fe pública, contra el patrimonio, etc.

En relación al sistema de información, este debe ser entendido como el conjunto de las bases o banco de datos del proceso informático automatizado, por ende, se configura en un bien independiente de costo económico. (Mayer, 2017)

#### 1.3.1.8. Características que presentan los delitos informáticos contemplados en la Ley N°30096

De acuerdo con la Ley N°30096, las características que presentan los delitos informáticos son las siguientes:

- Conductas ilícitas realizadas por personas con conocimiento en sistemas de información.
- Generan menoscabo al patrimonio económico.
- Avanzan con mayor rapidez por lo que se realizan a través de redes de información con acceso a internet.
- Son delitos genéricos.
- La proliferación masiva perjudica la persecución de los mismos.
- El sujeto activo puede ser cualquier persona.
- Utilización de información con acceso o sin acceso a sistemas digitales.
- Delitos interpersonales y digitales.
- Alteración de información y sistemas de identidad.
- Alto índice de impunidad.
- En el centro de cálculo hay un personal muy inteligente
- Son difíciles de equiparar por cuanto no existen áreas especializadas en todo nuestro territorio. (Hanco, 2018)

#### 1.3.2. Variable dependiente: Incorporar delitos de phishing, pharming y carding

##### 1.3.2.1 Delitos no regulados en la Ley N°30096

##### 1.3.2.2. El phishing

- Definición



Según Herrera (2016) el phishing o suplantación de identidad es un concepto informático que versa en el abuso de un modelo informático y que se realiza a través del uso de un tipo de ingeniería social, el cual se caracteriza por intentar obtener información o datos confidenciales de manera fraudulenta, especialmente a través de la obtención de contraseña de una tarjeta de crédito, información bancaria u otras. El phisher se hace pasar por una persona o empresa a través de una supuesta comunicación electrónica, usualmente se materializa mediante correo electrónico u otra plataforma tecnológica de mensajería. Es decir, este delito tiene la modalidad de estafa puesto que se busca obtener información con fines fraudulentos.

De la misma forma, de acuerdo con Oxman (2013) el phishing busca apoderarse de información personal mediante el internet con la finalidad de ingresar a sus cuentas e incrementar los datos de la persona en cuestión, para así poder comercializarlos de manera ilícita. Esta conducta es considerada como una modalidad de estafa informática, la cual se consuma mediante el envío de enlaces web en donde se imita el contenido de una entidad financiera para engañar al usuario, logrando sustraer información personal y consecuentemente poder ingresar a sus cuentas de crédito.

Mientras que para Valle (2013) el phishing es una técnica empleada por delincuentes con la finalidad de obtener información privada, a través de una comunicación confiable. El escenario en el que se desarrolla este delito usualmente es mediante la duplicidad de una página web en donde se hace creer al usuario que se encuentra en el sitio web correcto, cuando realmente es todo lo contrario. Luego de haber accedido al sitio web erróneo, los usuarios permiten indirectamente el acceso a sus datos confidenciales,

obteniendo los delincuentes un sinnúmero de estafas y fraudes con los datos recabados.

- Características

Según Valle (2013) las características más comunes que presenta este delito son:

- El uso de nombres de compañías conocidas, toda vez que los ciberdelincuentes optan por actuar mediante una imagen corporativa conocida en el mercado y crear confianza en el usuario.
- Utilizar el nombre de un empleado real de la empresa como remitente del correo enviado, puesto que si el usuario se comunica con la empresa para determinar si realmente el correo es verídico y por tanto señala el nombre de la persona que envió el correo, entonces le confirmarán aludiendo que dicha persona labora en la empresa.
- Direcciones web con apariencia correcta, es decir el correo fraudulento suele conllevar al usuario a sitios web de la empresa que está funcionando de pantalla para robar información. Los contenidos y la dirección web enviada son falsos.
- Factor miedo, la oportunidad que tienen los delincuentes es muy corta ya que desde el momento que la empresa comunica a sus clientes que están siendo objeto de fraude y actos delictivos, los usuarios se ponen atentos y evitan recurrir a determinados sitios web. Por tanto, frente a esta circunstancia, el defraudador amenaza a los clientes con una posible pérdida que puede ser orientada a la cuenta del cliente o de índole económico.

#### 1.3.2.3. Pharming

- Definición

El pharming consiste en la manipulación de las direcciones web empleadas por el consumidor, esta figura puede operar como modalidad de estafa informática ya que se puede obtener

datos personales financieros o bancarios de la víctima con la finalidad de consumar el ilícito del apoderamiento ilegal de su patrimonio. (Oxman, 2013)

Asimismo, según Paredes (2013) a través de esta modalidad los ciberdelincuentes se encargan de enviar correos electrónicos en donde señalan mensajes que busca comunicar con el usuario señalando que tiene una alta suma por consumo telefónico y de existir algún reclamo se pueden comunicar con el número proporcionado. El usuario se comunica con el número y le contesta al parecer una trabajadora que orienta a la víctima a proceder con su reclamo, solicitando su número de cuenta bancaria y su contraseña, con estos datos los delincuentes ingresan a su cuenta y consuman el delito.

#### 1.3.2.4. Carding

Según Sarzana (2010) el delito de Carding se consuma cuando el sujeto activo emplea de manera ilegal el número de tarjeta o las tarjetas de terceras personas, además se encuentra íntimamente relacionado con el hacking debido a que para este es empleado para conseguir los números de tarjeta.

Castillo (2005) manifiestan que el carding es la acción de ejecutar compras con la tarjeta de una tercera persona sin su consentimiento. Para ejecutar dicha acción el sujeto activo llena el formulario con datos falsos, consignando una dirección e identificación diferente a la del sujeto.

#### 1.3.3. Derecho Comparado

##### 1.3.3.1. Estados Unidos

De acuerdo con Vega (2010) en el año de 1958 en Estado Unidos se produjo el primer abuso de los sistemas informáticos, sin embargo, no fue hasta 1966 que se produjo la alteración informática de un banco en Mineapolis. Posteriormente, en la década de los 70 se empezó a discutir la importancia de dicho ataque, mientras eso ocurría los ataques cibernéticos se hicieron más frecuentes, hecho que generó que en 1976 el FBI dictará

cursos sobre los delitos informáticos y que el Comité de Asuntos del gobierno expusiera dos informes que dieron pie a la creación de la Ley Federal de Protección de Sistemas en 1985.

Esta Ley fue base para que diversos estados de Estados Unidos como Colorado y Michigan constituyan legislaciones específicas respecto a delitos cibernéticos, anticipándose al Abuse Act y al Computer Fraud, el primero de ellos sancionaba los registros médicos falsos, los fraudes respecto a inmuebles, la irrupción en computadoras del Estado, así como también emplear contraseñas de manera ilegal; sin embargo que estas sanciones sólo eran aplicables a aquellos casos que sobrepasan los mil dólares.

Posteriormente, ambas actas fueron reemplazadas por el Acta Federal de Abuso Computacional donde establecieron diversos comandos capaces de dañar las computadoras, marcado un hito ya que se dirigía principalmente a sancionar aquellas acciones que generen daño a las computadoras a través de un virus o grupos de programas capaces de causar el mismo efecto nocivo. En el 2000 los representantes de la Cámara y el Senado establecieron el “Acta de Firmas Electrónicas en el Comercio Global y Nacional” con el objetivo de revestir a los contratos realizados entre empresas y consumidores de validez.

Dentro de las normativas principales que buscan contrarrestar los delitos cibernéticos se encuentran el 18 USC de 1994, relacionado con el fraude y los dispositivos de acceso, principalmente los jueces norteamericanos emplean la sección 1029 y 1030, esta última modificó el pronunciamiento emitido sobre fraude y abuso informático de 1986 y complementa a la Ley de Privacidad de las Comunicaciones Electrónicas de 1986.

#### 1.3.3.2. Chile

Dentro de Latinoamérica Chile fue el primer país en tipificar conductas relacionadas a los delitos informáticos a través de la Ley 19.223 en 1993 cuya finalidad era proteger los datos informáticos y se constituía de cuatro artículos, dentro de los que

se encuentran los siguientes tipos penales: a) Destrucción e inutilización de un sistema de información o sus partes, b) Apoderamiento, uso y conocimiento indebido de información, c) Alteración, daños o destrucción de datos contenidos en un sistema, d) Revelación o difusión de datos. Sin embargo, doctrinariamente se sostiene que dicha normativa debido a su antigüedad requiere una modificación implementando las nuevas formas de criminalidad.

#### 1.3.3.3 Argentina

En el año 2008 se modificó el Código Penal argentino a través de la Ley N°26388, la misma que modificó diversos tipos penales relacionados con los delitos informáticos, tales como: a) Se incorporó en la parte final del artículo 77 el término documento, firma, suscripción así como los términos instrumento privado y certificado; b) Se reemplazó el artículo 128 por una sanción fluctuante entre seis meses a cuatro años al que por cualquier medio electrónico ofrezca, comercio, publicite contenido sexual de menores de 18 años o de sus genitales, así como aquel que realice conexiones en vivo mostrando representaciones sexuales, además aquel que posea contenido sexual será sancionado de entre cuatro a dos años y finalmente aquel que facilite el acceso a pornografía infantil (menores de catorce) será sancionado de un mes a tres años; c) Se reemplazó el título del Capítulo III por "*Violación de Secretos y de la Privacidad*"; d) Se sustituyó el artículo 153 de la norma adjetiva penal, estableciéndose una sanción de entre quince a seis meses para aquella persona que acceda de manera ilegal a una comunicación telefónica, cartas, sobre cerrado, o de otra naturaleza que no le corresponda. La misma sanción obtendrá aquel que interfiera las comunicaciones de manera ilegal, finalmente la sanción será de un mes a un año si el sujeto activo le comunica a una tercera persona el contenido de la carta, pliego o comunicación; e) Se incorporó el artículo 153 bis, donde se estableció una sanción entre quince días a seis

meses para aquella persona que acceda a un sistema o información de un órgano estatal sin la autorización correspondiente, la sanción se incrementa de un mes a un año cuando el sujeto activo accedió a la data sólo para perjudicar la información; f) Se sustituyó el artículo 155, estableciendo una sanción penal de 1.500 a 100 mil pesos para aquella persona que sea encontrada con información perteneciente a terceros; g) Se sustituyó el artículo 157 bis, donde se estableció una sanción penal de un mes a dos años para aquella persona que teniendo conocimiento vulnere un sistema de seguridad confidencial de datos o de igual manera ocurre para aquel que proporcione información privada y para aquella persona que ingrese datos en un archivo; h) Se incorporó el inciso 16 al artículo 173, señalando la figura de fraude a través de medios electrónicos; i) Se incorporó al artículo 183 el siguiente párrafo *“Aquel que inutilice, destruya, introduzca datos será sancionado con la misma pena del párrafo anterior”*; j) Se sustituyó el artículo 197 señalando que aquella persona que entorpece o interrumpe la comunicación será sancionado de seis a dos años; k) Se sustituyó el artículo 255 estipulando que aquella persona que altere, oculte, destruya, sustraiga o inutilice los archivos u objetos cuya finalidad es probar hechos será sancionado de un mes a cuatro años.

#### 1.3.3.4. México

En el año 2000 se realizaron diversas reformas al Código Penal mexicano, estableciendo diversos artículos cuya finalidad era sancionar aquellas conductas que atenten contra los sistemas informáticos, dentro de los cuales se encuentran: a) Artículo 211 bis 1, el cual sanciona a aquel que modifique o destruya información de sistemas informáticos; b) Artículo 211 bis 2, el cual sanciona a aquel que modifique o destruya información de sistemas informáticos pertenecientes al Estado; c) Artículo 211 bis 3, el mismo que sanciona a aquella persona que pese a estar autorizada acceda a los sistemas informáticos con la finalidad de

alterarlos, modificarlos o destruirlo, provocando su pérdida; d) Artículo 211 bis 4, el mismo que sanciona a aquella persona que no cuenta con autorización acceda a los sistemas informáticos relacionados con el sistema financiero con la finalidad de alterarlos, modificarlos o destruirlo, provocando su pérdida; e) Artículo 211 bis 5, el mismo que sanciona a aquella persona que pese a estar autorizada acceda a los sistemas informáticos relacionados con el sistema financiero con la finalidad de alterarlos, modificarlos o destruirlo, provocando su pérdida.

#### **1.4. Formulación del Problema.**

¿Permitirá la modificación de la ley 30096 para incorporar los delitos de Phishing, Pharming y Carding como delitos penalizables con prisión reducir la ciberdelincuencia, Lima 2019?

#### **1.5. Justificación e importancia del estudio.**

La presente investigación se justifica en la necesidad de incorporar los delitos de Phishing, Pharming y Carding a la actual Ley N°30096, ley de delitos informáticos, la cual regula estrictamente aquellos hechos ilícitos que se realizan a través del sistema informático los cuales vulneran una serie de bienes jurídicos. Dicha necesidad subyace de la realidad que suscita en los últimos años en el país, pues si bien la tecnología es una herramienta que facilita diversas actividades, ha sido empleada también de manera maliciosa por sujetos que buscan sacar provecho económico mediante el sistema informático lo cual se refleja en el gran número de denuncias informáticas, razón por la cual se reguló la Ley N°30096, no obstante esta posee diversos vacíos legales, lo cual imposibilita el desarrollo de determinados actos en la vía penal al no encontrarse regulados en la norma jurídica, por tanto constituye la impunidad, perjudicando gravemente a los usuarios víctimas de este tipo de actividades ilícitas.

La presente investigación busca penalizar con pena privativa determinados delitos como Phishing, Pharming y Carding, con la finalidad de otorgar seguridad jurídica e informática a los usuarios que utilizan de manera constante la tecnología, ello quiere decir que dicha regulación beneficiará a todos los ciudadanos ya que no serán víctimas de delitos informáticos.

## **1.6. Hipótesis**

La modificación de la Ley N°30096 incorporando los delitos de Phishing, Pharming y Carding reducirán el índice de ciberdelincuencia en el Perú.

## **1.7. Objetivos**

### **1.7.1. Objetivo General**

Justificar por qué los delitos de Phishing, Pharming y Carding deben ser incorporados a la Ley N°30096 como delitos penalizables con penas privativas de la libertad.

### **1.7.2. Objetivos Específicos**

- a) Establecer la incidencia de no encontrarse reguladas las actividades conocidas como Phishing, Pharming y Carding como delitos informáticos inciden en los derechos de los usuarios.
- b) Analizar la ley N°30096 – Ley de delitos informáticos, a fin de evaluar si se considera los delitos de Phishing, Pharming y Carding como delitos penalizables.
- c) Examinar las deficiencias legislativas en relación a la tipificación de los delitos informáticos que atentan a la totalidad de sistemas informáticos en legislación extranjera.

## **1.8. Limitaciones**

La investigación se limitará a examinar la ciberdelincuencia realizada a través de sistemas informáticos actuales y las carencias legislativas existentes en relación al tema por no encontrarse tipificados dentro de la Ley N°30096 las actividades de Phishing, Pharming y Carding como delitos penalizables de atentado a los sistemas informáticos.

Asimismo, cabe mencionar que el presente estudio se efectuó en el periodo 2019

## **II. MATERIAL Y MÉTODO**

### **2.1. Tipo de estudio y diseño de la investigación**

#### **2.1.1 Tipo de estudio**



El tipo de estudio empleado en la presente investigación es básico con un enfoque cualitativa, toda vez que se parte de un marco teórico y se tiene como finalidad explicar y entender la importancia de incorporar a la Ley N°30096 las actividades conocidas como phishing, carding y pharming.

### **2.1.2 Diseño de investigación**

Por otro lado, el diseño de investigado empleado fue No Experimental, por cuanto se inspira prácticamente en la observación de los fenómenos tal y como se proporcionan en su entorno natural para luego ser analizarlos.

### **2.2.1 Población**

El escenario de estudio de la investigación fue la Ley N°30096 debido a que se busca analizar sus deficiencias a fin de determinar la importancia de incorporar las modalidades de phishing, pharming y carding. De igual manera se analizaron las leyes sobre delitos informáticos de Estados Unidos, México, Argentina y Chile.

### **2.2.2. Muestra**

Los sujetos participantes serán sólo aquellas normas jurídicas que versan sobre delitos informáticos tanto a nivel nacional como internacional.

## **2.3. Variables, Operacionalización**

Variable independiente: Modificación de la Ley N°30096

Variable dependiente: Incorporar delitos de phishing, pharming y carding

## **2.4. Técnicas e instrumentos de recolección de datos.**

### **2.4.1. Técnicas**

- **Análisis documental:** Es una técnica para recopilar información cuya finalidad es describir y presentar documentos de forma sistemática y unificada para facilitar su recuperación. Comprende además el procesamiento

integral del análisis, que a su vez incluye bibliografía y descripción general.

#### 2.4.2. Instrumentos

- Ficha de análisis documental: A fin de registrar información relevante relacionada con el tema de estudio.

#### 2.4.3 Instrumento de recolección de datos

La aplicación del instrumento de recolección de datos permitió obtener información relevante y oportuna en relación al problema, objetivo general y objetivos específicos del estudio.

### 2.5. Procedimientos para la recolección de datos.

**Paso 1:** Se analizó la realidad a fin de determinar si el problema de investigación era relevante para ser estudiado, continuamente se estableció la realidad problemática, se formuló el problema y los objetivos específicos.

**Paso 2:** Se estableció el escenario donde se desarrolló la investigación.

**Paso 3:** Se seleccionó y ejecuto la técnica de análisis documental, así como su instrumento, ambos relacionados con la investigación.

**Paso 4:** Se analizó la información recopilada y se estructuraron los resultados.

**Paso 5:** Se interpretaron y discutieron los resultados obtenidos, a través de los cuales se pudieron establecer las consideraciones finales.

### 2.6. Aspectos éticos

Dentro de la investigación se respetaron las fuentes de la información, las mismas que han sido citadas de acuerdo al formato APA; de igual manera la información recopilada provino de fuentes fidedignas sin que exista de por medio alguna alteración.

### 2.7. Criterios de Rigor científico.

Hay ciertos criterios que permiten evaluar el rigor y la calidad científica de los estudios cualitativos y sobre los cuales hay consenso parcial.

- **Credibilidad o valor de la verdad:** Respeto por los hechos y situaciones causados en el entorno temporal y espacial de la presente investigación (2019) teniendo en cuenta la estimación valorativa de los datos obtenidos a través de la información derivada de la aplicación del instrumento de investigación.
- **Dependencia:** involucra el grado de consistencia o seguridad de los resultados y hallazgos del análisis luego del procesamiento de la información obtenida a través del instrumento.
- **Confirmabilidad:** El nivel de implicación en la exploración, no se ha eludido, en todo caso se alarga la garantía suficiente sobre el proceso a lo que se refiere la presente investigación, resultando como producto de la información arrojada por el instrumento aplicado, donde los datos no permanecen sesgados, ni responden a ningún tipo de manipulación de naturaleza personal.

### III. REPORTE Y RESULTADOS

#### 3.1. Tablas y figuras

Tabla 1:

*Establecer la incidencia de no encontrarse reguladas las actividades conocidas como Phishing, Pharming y Carding como delitos informáticos inciden en los derechos de los usuarios.*

---

#### INCIDENCIA DE LA FALTA DE REGULACIÓN DE LOS DELITOS DE PHISHING, PHARMING Y CARDING

---

	<p>De acuerdo con Zorrilla (2018) en el Perú existen diversas actividades que atentan contra el sistema informático y violenta las garantías o seguridad que otorga el internet, las principales conductas ilícitas que se realizan a través del sistema informático son las siguientes: phishing, carding y pharming; las cuales se consuman mediante el uso de la tecnología, los mismos que no se encuentran regulados en la legislación nacional.</p>
Vacíos Normativos	<p>En este sentido, la regulación de las actividades mencionadas líneas arriba, resultan necesarias ya que son las acciones más frecuentes en el ámbito informático, teniendo en cuenta que el uso del internet es una herramienta indispensable para la realización de distintas actividades desde lo más cotidiano hasta de uso laboral, por lo que se debería penalizar dichas conductas con pena privativa de libertad con el objeto de reducir el índice de ciberdelincuencia. No obstante, hasta la fecha el legislador no ha establecido un criterio de valoración económica del ilícito generado al sistema informático con la finalidad de determinar si la conducta realizada configura una infracción administrativa o comportamiento penal, de la misma forma no ha establecido criterios respecto a la valoración de la gravedad que ocasionan los delitos informáticos, existiendo vacíos legales que dificultan el desarrollo de la presente ley en la realidad jurídica.</p>

---

*Nota.* Esta tabla muestra la incidencia de la falta regulación de los delitos de phishing, pharming y carding – elaboración propia.

## Exceso de casos archivados

### Denuncias por delitos informáticos 2013-2020, según estado procesal

ESTADO	CANTIDAD	%
Archivadas	12608	58%
En proceso	8842	41%
Sobreseimiento	125	1%
Sentencia	108	0%
Terminación anticipada	4	0%
<b>TOTAL</b>	<b>21 687</b>	

*Nota.* Cuadro realizado por el Ministerio Público – Informe de Análisis N° 4

## Análisis y discusión

Respecto al objetivo N° 1 en relación al objetivo Establecer la incidencia de no encontrarse reguladas las actividades conocidas como Phishing, Pharming y Carding como delitos informáticos inciden en los derechos de los usuarios; de los resultados obtenidos en cuanto al análisis de normas jurídicas según Zorrilla (2018) la Ley N°30096 posee diversos artículos incoherentes que genera confusión al momento de su aplicación, la norma legisla el medio a través del cual se comete el ilícito más no regula conducta y busca regular aquellas que ya se encuentran establecidas en la norma penal adjetiva; toda vez que en el Perú no existe un texto normativo que determine de manera específica los tipos penales que definan los delitos que se cometen con mayor frecuencia en redes sociales, por tanto es necesario sancionar correctamente, además la falta de cultura informática es un factor determinante en la comisión de delitos informáticos, es por ello que es necesario contar con profesionales especialista en la materia. De la misma forma, Sequeiros (2016) menciona que la falta de información respecto a los límites de los delitos informáticos impide

conocer de manera íntegra el manejo de determinadas situaciones, a su vez existe la necesidad de fortalecer el uso de tecnología con la finalidad de que el usuario sienta seguridad al realizar actos tecnológicos, más no la privación de estos. Por ello, recomienda que es necesario generar espacios de comunicación con las autoridades competentes a fin de enfrentar esta nueva forma de delinquir, es decir definir la normativa desde la realidad de nuestro país.

**Tabla 2:**

*Analizar la ley N°30096 – Ley de delitos informáticos, a fin de evaluar si se considera los delitos de Phishing, Pharming y Carding como delitos penalizables.*

<b>LEY DE DELITOS INFORMÁTICOS</b>					
<b>Capítulo II</b>	<b>Capítulo III</b>	<b>Capítulo IV</b>		<b>Capítulo V</b>	<b>Capítulo VI</b>
<b>Delitos contra datos y sistemas informáticos</b>	<b>Delitos informáticos contra indemnidad libertad sexuales</b>	<b>la</b>	<b>Delitos informáticos contra la intimidad y el secreto de las comunicaciones</b>	<b>Delitos informáticos contra el patrimonio</b>	<b>Delitos informáticos contra la fe pública</b>
<ul style="list-style-type: none"> <li>• Acceso ilícito</li> </ul> <p>Este tipo penal sanciona la vulneración de la confidencialidad mediante medios electrónicos sin contar con el acceso permitido,</p>	<ul style="list-style-type: none"> <li>• Proposición a niños, niñas y adolescentes con fines sexuales por</li> </ul>	<ul style="list-style-type: none"> <li>a</li> </ul>	<ul style="list-style-type: none"> <li>Este tipo penal sanciona la interrupción de las emisiones electromagnéticas así como los datos</li> </ul>	<ul style="list-style-type: none"> <li>• Fraude informático</li> </ul> <p>Este tipo penal sanciona la acción de introducir, borrar, diseñar,</p>	<ul style="list-style-type: none"> <li>• Suplantación de identidad</li> </ul> <p>Este tipo penal sanciona la acción de suplantar la identidad</p>

<p>hecho que vulnera las medidas de seguridad establecidas implementadas con la finalidad de evitar transgresiones al sistema informático. Asimismo, este tipo penal se considera como un delito de mera actividad, ya que para su configuración se requiere que el sujeto activo acceda al sistema teniendo pleno conocimiento que dicho accionar se encuentra prohibido por la norma (Gutiérrez, 1991)</p>	<p>medios tecnológicos Este tipo penal sanciona las propuestas sexuales realizadas hacia los menores a través de medios tecnológicos, con la finalidad de recabar pornografía infantil o realizar actividades que vulneren la libertad</p>	<p>informáticos privados, así mismo este delito establece diversas agravantes, dentro de las que se encuentran: la primer agravante se da cuando la interceptación de información recae sobre datos establecidos como privados, secretos o confidenciales de acuerdo con la Ley</p>	<p>de una tercera persona ya sea jurídica o natural, a fin de generarle un perjuicio. Asimismo, este delito es un delito de resultado ya que se requiere que el sujeto activo suplante la identidad de una tercera persona mediante la creación de perfiles falsos en</p>
<p>• Atentado contra la integridad de datos informáticos</p> <p>Este tipo penal sanciona principalmente el hecho de dañar, borrar, alterar, deteriorar, introducir, suprimir y hacer inaccesible la información de la</p>	<p>sexual o la indemnidad; asimismo dentro de este tipo penal se infieren dos supuestos, el primero de ellos se basa en el contacto realizado</p>	<p>27806 con una sanción penal de cinco a ocho años; la segunda agravante se da cuando se intercepten datos relacionados con la seguridad, defensa o soberanía nacional con</p>	<p>perjudique a un tercero o genere un beneficio para sí mismo (Villavicencio, 2014) caso contrario quedaría en tentativa.</p>

---

data informática a través de las tecnologías de la información; asimismo este tipo penal requiere para su consumación que el sujeto activo tenga conocimiento de que su accionar está en contra de la Ley, sin importar si el resultado que este logre (Villavicencio, 2013)

contra menores de una sanción penal de catorce años cuya ocho a diez años y sanción penal es de finalmente la tercera cuatro a ocho años y agravante se da cuando el segundo de ellos se el sujeto activo forma parte de un grupo realizado contra un criminal cuya sanción es menor de catorce y incrementada un tercio dieciocho años cuya más del máximo sanción penal fluctúa establecido (Orts, 2001)

- 
- Atentado a la integridad de sistemas informáticos

entre tres a seis años (Villavicencio, 2013)

Este tipo penal sanciona aquel accionar que busca inutilizar de manera total o parcial un sistema informático, entorpeciendo e imposibilitando sus servicios a través de diversas técnicas de la información, sin embargo, a diferencia de los otros tipos



---

penales anteriormente mencionados este tipo penal es un delito resultado ya que para su configuración se requiere que el sujeto cumpla con imposibilitar los sistemas informáticos (Bramont, 2000)

---

*Nota.* Esta tabla muestra la tipificación actual de los delitos informáticos en el Perú – elaboración propia.

### **Análisis y discusión**

Respecto al objetivo específico N° 2, el cual es Analizar la ley N°30096 – Ley de delitos informáticos, a fin de evaluar si se considera los delitos de Phishing, Pharming y Carding como delitos penalizables; se determinó que dentro de la citada norma no se encuentran establecidos de manera expresa los delitos de phishing, pharming y carding, este hecho genera en la práctica jurídica un conflicto ya que al no estar establecidos de acuerdo al principio de legalidad, la conducta realizada por el sujeto no acarrea consigo responsabilidad penal, asimismo cuando se pretende encajar dicha conducta con otros tipos penales ya establecidos, las argumentaciones resultan débiles, ello se corrobora con Herrera (2018) quien en su investigación manifiesta que la eficacia de los delitos informáticos es baja toda vez que posee deficiencias en cuanto a su aplicación, hecho que dificulta su desarrollo en la práctica jurídica. Finalmente, debe decir que en el Perú no existe un texto normativo que establezca de manera explícita las nuevas modalidades de delitos cibernéticos (phishing, pharming y carding) siendo el principal factor para su continua consumación.

**Tabla 3:**

*Examinar las deficiencias legislativas en relación a la tipificación de los delitos informáticos que atentan a la totalidad de sistemas informáticos en legislación extranjera.*

<b>DEFICIENCIAS LEGISLATIVAS EN LEGISLACIONES EXTRANJERAS</b>			
<b>Estados Unidos</b>	<b>Chile</b>	<b>Argentina</b>	<b>México</b>
En 2004 la Comisión Federal de Comercio de los Estados Unidos tuvo el primer proceso contra un fisher, el mismo que era un adolescente residente de California quien supuestamente había creado una página web cuyo diseño era similar al de American Online con la finalidad de robar números de tarjetas de los usuarios. Razón por la cual en el año 2005 el Senador Patrick Leahy promulgará la Ley Antiphishing, cuya	El phishing se vio reflejado por primera vez en el año 2003, donde los ciberdelincuentes crearon diversos correos electrónicos con nombres de compañías reconocidas a nivel internacional y nacional con la finalidad de enviar diversos mensajes llamados "spam" en los cuales se ponía un link de páginas fraudulentas a fin de que los usuarios ingresen sus datos y así poder robar su información. De acuerdo con	En el año 2008 a través de la Ley N° 26388, la misma que modificó el Código Penal argentino con el objetivo de incorporar diversos tipos penales relacionados con los delitos informáticos, sin embargo en ningún aspecto a la citada Ley se establecieron los delitos de phishing, pharming o carding; el primero de ellos en la república argentina sigue siendo tratado dentro del artículo 173 inciso 16 de la norma adjetiva penal,	En el año 2019 la república mexicana aprobó dos dictámenes cuya finalidad era reformular la Ley General del sistema Nacional de Seguridad Pública, específicamente los delitos referidos a la seguridad cibernética. El artículo que se modificó fue: a) Artículo 211 bis 1 según el cual aquella persona que sin contar con autorización destruya, modifique o genere la pérdida de información será

---

finalidad era sancionar las actuaciones criminales configuradas a través de la creación de páginas falsas o el envío de spam a diversos correos electrónicos con el objetivo de estafar a los usuarios, imponiendo una sanción de hasta cinco años y una multa ascendente de 250.000 dólares. Sin embargo, la normativa resulta insuficiente ya que las tasas de phishing durante el año 2020 aumentaron en un 20%. Aunado a ello Estados Unidos no ha regulado el delito de pharming ni carding pese a que en el 2016 se detuvieron a 26 personas supuestamente involucradas en el robo 530

la brigada especializada en estos tipos penales, las denuncias de Phishing en Chile corresponden al 3.61% durante estos últimos cinco años, de igual manera ocurre con el delito de pharming cuya modalidad al igual que el phishing encajan en el delito de estafa sin embargo no existe una adecuada distinción de ambas modalidades, generando confusión en su tipificación y pese a que en el 2018 el ejecutivo envió un mensaje al Congreso solicitando la derogación y el reemplazo de la Ley 19.233 por una nueva normativa actualizada, esto no se ha dado. El intento de

donde se establece el delito de estafa, este hecho genera una sensación de laguna normativa pues en la práctica jurídica aún no logra determinarse qué delitos se encuentran inmersos dentro de la figura fraude informático, ejemplo de ello es que en el año 2016 un grupo de personas logró robar 3,5 millones de pesos de la ciudad Autónoma de Buenos aires a través de una página web falsa muy similar a la que empleaba la municipalidad; esta operación se realizó mediante transferencias falsas a nombre de proveedores de la Municipalidad. De igual

sancionado de 2 a 5 años de prisión y con 365 días multa. Sin embargo, este tipo penal no resulta claro ya que los jueces tienen diversos problemas al momento de identificar la naturaleza delictiva de los delitos informáticos, generando que su tipificación carezca de sustento y al ser el principio de legalidad base para el derecho penal si la conducta no encaja en ningún tipo penal, no puede configurarse un hecho delictivo, tal cual ocurre con la tipificación de los delitos de pharming y carding.

---

---

millones de dólares a través del robo de identidades para usar las tarjetas de débito y crédito.

modificar la normativa anteriormente señalada no es nuevo ya que anteriormente se han realizado dos intentos más, los cuales resultaron fallidos. La incorporación del nuevo proyecto presentado por el ejecutivo permitirá reducir la criminalidad informática ya que dentro de sus tipos penales se encuentra establecido el fraude informático, falsificación informática, la perturbación informática, entre otras como es el caso del carding, modalidad que existe pero que no ha sido desarrollada ni señalada en la Ley 19.233 (Hiplán, 2019)

manera ocurre con los delitos de pharming y la nueva modalidad cibernética llamada carding, las cuales no cuentan con una tipificación idónea dentro del marco normativo penal argentino.

---

*Nota.* Esta tabla muestra las deficiencias legislativas en legislaciones extranjeras – elaboración propia.

## **Análisis y discusión**

Respecto al objetivo específico N° 3, el cual es examinar las deficiencias legislativas en relación a la tipificación de los delitos informáticos que atentan a la totalidad de sistemas informáticos en legislación extranjera; de los resultados obtenidos en Derecho Comparado se pudo comprobar que ningún país cuenta con una legislación idónea para contrarrestar la consumación de estos tipos penales, ya que se busca que estos encajen con tipos penales ya establecidos, generando confusión en los operadores del derecho al momento de establecer la tipificación de la acción, por ello es necesario que exista una tipificación adecuada de cada una de estas modalidades de ciberdelincuencia a fin de que el número de casos perpetrados disminuya, protegiendo los intereses de los usuarios. La necesidad de tipificación se corrobora con lo señalado por Alkhalil y et al. (2021) quienes sostienen que, si bien la tecnología constituye una herramienta importante en la actualidad, este ha traído consigo una serie de modalidades delictivas como por ejemplo el phishing, el cual se caracteriza por la información recabada por ciberdelincuentes a fin de sacar provecho económico, este es una forma de estafa.

### **3.2. Discusión de resultados**

Con la utilización de la tecnología han surgido nuevas formas de atentado contra la seguridad a través de sistemas digitales de información las que hoy en día no se encuentran reguladas por el ordenamiento jurídico peruano, que si bien es cierto el Perú en el año 2013 promulgó la Ley N°30096 – Ley de Delitos Informáticos, a fin de contrarrestar estas conductas a la fecha no ha existido ninguna modificación, pese a que han pasado siete años aproximadamente, hecho que genera que en la ley actual no se hayan considerado las nuevas formas delictivas que la globalización y el avance de la tecnología ha traído consigo, por lo que, esta ley no regula las actividades que atentan contra nuestra seguridad digital conocidos como PHISHING, PHARMING Y CARDING. Respecto al objetivo N° 1 en relación a Establecer la incidencia de no encontrarse reguladas las actividades conocidas como Phishing, Pharming y Carding como delitos informáticos inciden en los derechos de los usuarios; se determinó que en el Perú no existe un texto

normativo que determine de manera específica los tipos penales que definan los delitos que se cometen con mayor frecuencia en redes sociales, por lo que resulta importante modificar la Ley N°30096 y su modificatoria Ley N°30171 a fin de incorporar estas actividades conocidas como PHISHING, PHARMING Y CARDING como delitos penalizables, ya que como se ha venido explicando el "phishing, carding y pharming" son modalidades de engaño moderno, que nacieron con la globalización, que si desde sus inicios la población hubiese sido debidamente informada a nivel preventivo por las entidades bancarias en el extremo que las mismas nunca solicitan a sus clientes datos de índole personal vía online, quizás estos casos o esta moderna forma de criminalización no hubiera sido tan frecuente como lo es en la actualidad, puesto que según los boletines estadísticos del Ministerio Público en el año 2018 se registraron 3851 delitos informáticos, mientras que en el año 2019 se registró 6906 de delitos informáticos durante los meses de enero a noviembre, lo cual representa el 0.71% del total de casos, registrándose con mayor grado de comisión los delitos informáticos contra el patrimonio, siendo que en el año 2018 fueron 1336 y en el año 2019 se incrementaron a 2641 casos. A pesar que desde el año 2013, existe una ley de delitos informáticos, todo ello nos evidencia, que la Ley no es la forma de solucionar todos los problemas sociales, en especial los ataques a los bienes jurídicos tutelados por el Estado, sino que además tiene que estar amparado por fines preventivos, de concientización de los sujetos pasivos, respecto de los posibles ataques a su patrimonio al contar con tarjetas de crédito y/o débito y si bien en la actualidad existe una unidad especializada en estos delitos a nivel policial, ello no es suficiente, ya que dicha especialización debe desarrollarse en la administración de justicia, es decir en Jueces y Fiscales, es más, por tanto deberían existir fiscalías y juzgado especializados en delitos de ciberdelincuencia.

Respecto al objetivo N° 2 que fue analizar la ley N°30096 – Ley de delitos informáticos, a fin de evaluar si se considera los delitos de Phishing, Pharming y Carding como delitos penalizables; se determinó que dentro de la citada norma no se encuentran establecidos de manera expresa los delitos de phishing, pharming y carding, ya que si bien es cierto los delitos informáticos en la Ley N°30096 y su modificación por la Ley N°30171 contempla los delitos

contra datos y sistemas informáticos (Capítulo II) Este capítulo está conformado por las siguientes figuras penales: el artículo 2 (acceso ilícito), el artículo 3 (atentando a la integridad de datos informáticos) y el artículo 4 (atentando a la integridad de sistemas informáticos). Esta figura penal de acceso ilícito sanciona la violación de la confidencialidad, que se realiza a través del acceso no autorizado al sistema, vulnerando las medidas de seguridad establecida para evitar que ajenos ingresen a un sistema informático; por el verbo rector acceder se entiende el hecho de entrar en un lugar o pasar a él, que en esta figura se entiende el acto de entrar sin autorización del titular a un sistema. El término vulnerar se entiende como “transgredir, quebrantar”, aquel que cometa este acto ilícito será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días-multa, aún no se han incorporado los delitos de phishing, pharming y carding.

La Regulación de los delitos informáticos constituyen un gran avance en nuestro país, sin embargo, ha sido materia de la presente tesis avocarnos, en específico a las nuevas formas de criminalidad en el aspecto económico- es decir en la afectación del patrimonio de la víctima con las denominadas estafas informáticas, cuyo denominador común y forma de comisión es a través de la utilización del soporte operativo es decir el uso del internet, puesto que en la actualidad estos fraudes bancarios son concurrentes, es más año tras años se incrementan de manera significativa, por lo que considero que su nivel de punición debe ser severo, a fin de que la comunidad tenga en cuenta que el Estado asume un verdadero rol punitivo, en la protección de las actividades y datos bancarios, así como en la protección del patrimonio de la víctima, más aún que es común la entrega de tarjetas de crédito, con la finalidad de hacerse un uso responsable, ante necesidades urgentes, sin embargo la víctima se ve perjudicada cuando de pronto la entidad bancaria le cursa cartas de adeudo y requiriendo pagos, por supuestas compras y/o transferencia que ha realizado, lo cual es no reconocido por la víctima, iniciándose así una verdadera odisea, ya que en mucho de los casos, dicha víctima llega a dar a INFOCORP; y lo que es peor aún, la transferencia de dinero efectuado por el ciberdelincuente desde las tarjetas de débito de la víctima hacia personas desconocidas, que en muchos de los casos afectan el derecho alimentario de los dependientes del

sujeto pasivo. Todo ello permite afirmar, que pese a que la regulación de los delitos informáticos ha sido un gran avance en nuestro país, también es cierto que dicha regulación es precaria para una realidad como la nuestra, por lo que se necesita de manera urgente una modificación a la ley de delitos informáticos que dé una verdadera respuesta a las nuevas formas de criminalidad materia de estudio, es decir a estos ataques al patrimonio a través de la utilización ilícita de las claves de acceso a banca online, que afectan la seguridad y confianza en el mercado de las transacciones patrimoniales. Ahora si tenemos en cuenta como ha sido regulada la estafa en nuestro Código Penal, podremos darnos cuenta que el delito de estafa tiene un enfoque antiguo, donde se establecía como requisito y forma de engaño, la existencia de una interrelación entre los sujetos del delito (activo-pasivo), es decir entre quien engaña, maniobra, crea, situaciones fingidas o fraudulentas, atribuye cualidades y/o utiliza nombres falsos, simula, deforma u oculta hechos ciertos, etc., y, por el otro lado se encuentra el engañado, que le atribuye a ello un significado diverso del que en un contexto normal de comunicación le hubiere asignado.

Es así que ante la respuesta penal nula, frente a los fraudes informáticos de apoderamiento patrimonial, por no haberse regulado el phishing, pharming y carding, es que muchas veces los operadores de justicia recurren al concepto general de estafa, es como se ha explicado, la estafa en el Código Penal tiene una concepción antigua donde se requiere el desprendimiento del patrimonio del sujeto pasivo basado en el engaño, astucia, ardid, sin embargo en este tipo penal de los que se desprende son sus claves y/o contraseñas basadas en un error, cuando es voluntario o de manera involuntaria cuando se hace uso de los malware, requiriéndose en tal sentido una regulación.

Finalmente, respecto al objetivo N° 3, el cual fue examinar las deficiencias legislativas en relación a la tipificación de los delitos informáticos que atentan a la totalidad de sistemas informáticos en legislación extranjera, de los resultados se pudo comprobar que ningún país cuenta con una legislación idónea para contrarrestar la consumación de estos tipos penales, ya que se busca que estos encajen con tipos penales ya establecidos, generando confusión en los operadores del derecho al momento de establecer la tipificación de la acción,



por ello es necesario que exista una tipificación adecuada de cada una de estas modalidades de ciberdelincuencia a fin de que el número de casos perpetrados disminuya, protegiendo los intereses de los usuarios.

### **3.3. Aporte científico**

De acuerdo con Bunge (2015) la investigación científica es aquella actividad que busca resolver un problema a través de la reflexión sistemática y metódica y tiene como objetivo aportar nuevos conocimientos en el campo de la investigación, partiendo del estudio del problema que se suscita en la realidad. En la presente tesis el aporte científico radica en el aporte teórico y práctico, en el primero de ellos se describió la realidad donde se suscita el problema, luego de ello se analizó y contrastó con la legislación nacional e internacional, disgregando la Ley N°30096, así como los tipos penales que buscan incorporarse; en el segundo de ellos se estableció una modificatoria legislativa incorporando las nuevas modalidades delictivas, que son phishing, pharming y carding, cuyo texto quedaría redactado de la siguiente manera:

#### **LEY N° 30096**

##### **Artículo 5.- Atentado contra la seguridad jurídica y confianza – Phishing**

El que, mediante medios informáticos suplanta la identidad de una persona o una organización con el objetivo de engañar a terceras personas, valiéndose de la confianza que esta tiene en las organizaciones para revelar información confidencial, será reprimido con una pena privativa de libertad no menor de 4 años ni mayor de 8 años e inhabilitación según corresponda y con 90 a 180 días multa; además del pago de una reparación civil proporcional al daño causado.

##### **Artículo 6.- Atentado contra los sitios web – Pharming**

El que, mediante medios informáticos suplanta o tergiversa la identidad de un sitio web, valiéndose de sus conocimientos para obtener información confidencial de terceros, será reprimido con una pena privativa de libertad no menor de 4 años ni mayor de 8 años e inhabilitación según corresponda y con 90 a 180 días multa; además del pago de una reparación civil proporcional al daño causado.

#### Artículo 7.- Atentado contra los sitios web – Carding

El que, mediante medios informáticos accede ilegalmente a los datos de una tarjeta de crédito o débito con la finalidad de aprovecharse de terceros, será reprimido con una pena privativa de libertad no menor de 4 años ni mayor de 8 años e inhabilitación según corresponda y con 90 a 180 días multa; además del pago de una reparación civil proporcional al daño causado.

### IV. CONCLUSIONES Y RECOMENDACIONES

#### Conclusiones

- La Ley N°30096 posee diversos artículos incoherentes que genera confusión al momento de su aplicación, la norma legisla el medio a través del cual se comete el ilícito más no regula conducta y busca regular aquellas que ya se encuentran establecidas en la norma penal adjetiva.
- La Ley N°30096 posee diversas deficiencias legislativas respecto de la tipificación jurídica de las actividades consideradas como PHISHING, PHARMING Y CARDING.
- El "phishing, carding y pharming" son modalidades de engaño moderno, que nacieron con la globalización, que si desde sus inicios la población hubiese sido debidamente informada a nivel preventivo por las entidades bancarias en el extremo que las mismas nunca solicitan a sus clientes datos de índole personal vía online, quizás estos casos o esta moderna forma de criminalización no hubiera sido tan frecuente como lo es en la actualidad.
- En la modalidad de "phishing", mediante la cual el sujeto activo es quien solicita claves y/o contraseñas por correo electrónico y al ser otorgadas por el sujeto pasivo del delito, se le defrauda en su patrimonio, con ello se puede concluir que no se requiere que la víctima haya incurrido en un error y por ello transfiera su patrimonio, es más en este modalidad de criminalidad, la víctima no tiene en deseo de efectuar transacciones

bancarias, sino que estas son realizadas por un tercero, al haber obtenido datos personales de maneta ilegítimo.

- Actualmente el problema de la ciberdelincuencia, no solo se trata de un robo de información personal del sistema bancario, sino además que estos sujetos compran y venden malware en línea, usualmente en la red oscura, y luego de ello lo comercializan mejorado, tal es así que dichos delincuentes llegan a tener incluso una línea de asistencia para solucionar problemas con su servidor ilegal.
- A nivel internacional respecto de los delitos informáticos, existe el convenio de Budapest que regula la ciberdelincuencia, el cual se suscribió el 23 de noviembre del 2001 en la Ciudad de Budapest- Hungría, y entró en vigencia desde el 01 de Julio del 2004; sin embargo en nuestro país recién nos adherimos al mismo en el año 2019, aprobándose mediante Resolución Legislativa N° 30913 el 12 de febrero de 2019; y ratificándolo a través del Decreto Supremo N° 010-2019-RE, el 9 de marzo de 2019, y entró en vigencia en nuestro país desde el 1 de diciembre de 2019.
- El sujeto activo del delito o también conocido como ciberdelincuente, puede ser cualquier persona, es decir no requiere algún requisito personal o conocimientos técnicos cualificados.

### **Recomendaciones**

- Se recomienda diferenciar a la estafa tradicional con la estafa informática de naturaleza moderna, buscando la inclusión en la ley de delitos información del "phishing, carding y pharming" en los cuales el nivel de interacción del sujeto activo y pasivo del delito es mínimo, ya que la obtención de los datos bancarios de la víctima, son obtenidos a través de desvío a páginas fraudulentas –phishing- que efectúa el ciberdelincuente o con el uso de los malware –pharming-, siendo que en este último, todos los datos que haya utilizado el sujeto pasivo en la banca electrónica son decodificados y así le sustraen las claves personales, para proceder a darles un uso ilegal, advirtiéndose así que no siempre es necesario la interacción /o comunicación personal entre sujetos, por lo que no puede

hablar de engaña, como lo requiere el delito de estafa regulado en nuestro Código Penal.

- Se recomienda estipular una sanción idónea para las nuevas modalidades de estafa phishing, pharming y carding, ya que la aplicación de pena privativa disminuiría la consumación de estas modalidades delictivas, y ello no implica la vulneración del principio de lesividad, sino más bien se protege de una manera efectiva a los ciudadanos, ya que como lo he señalado el dinero de las tarjetas de débito en mucho de los casos cubren las necesidades básicas tales como educación, alimento, vestimenta. O caso contrario se debería especificar como agravante y que la pena sea efectiva, en los casos que la transferencia, y/o manipulación de datos sean de una tarjeta de débito. Siendo claro que para frenar estos delitos, no basta el pago de indemnizaciones a los titulares de las cuentas corrientes y/o tarjetas de crédito y/ débito, sino que se hace necesario crear una cultura bancaria, difundir por todos los medios posibles las formas posibles de ciberdelincuencia y además que la misma se encuentra penalizada de manera severa en nuestro ordenamiento penal; para que de ese manera la población se sienta segura de uso de sistema bancario vía online. Es decir, resulta indispensable, dar seguridad a los datos personales que circulan tanto en redes sociales virtuales como en cuentas de correo electrónico, tarjetas de crédito, compras en línea, en la medida en que pueden otorgar antecedentes a terceros para el acceso no autorizado a cuentas bancarias y comerciales, que se han vuelto especialmente vulnerables debido a la masificación de Internet.
- Se recomienda a los legisladores parametrizar que conductas merecen o no ser concebidas como un delito informático, ya que si por ejemplo una persona usa las redes sociales y difama a una persona, se estaría vulnerando un delito contra el honor, cuyo tratamiento y persecución es por acción privada, más no ante un delito informático; pero si una persona de manera ilegal y/o maliciosa ingresa sin tener la debida autorización a un sistema de datos y sabotea la base, dicha conducta sí se clasifica dentro de los delitos informativos.

## REFERENCIAS

- Alkhalil, Z., Hewage, C., Nawafans, L. y Khan, I. (2021) Phishing Attacks: A Recent Comprehensive Study and a New Anatomy. *Frontiers*, 3(1).  
<https://doi.org/10.3389/fcomp.2021.563060>
- Akamai. (2020). Informe sobre el Estado de Internet en materia de seguridad de Akamai. <https://www.akamai.com/es/es/multimedia/documents/state-of-the-internet/soti-security-phishing-for-finance-report-2021.pdf>
- Alvarado, J. D. (2017) *Análisis de las vulnerabilidades mediante el uso de phishing para mejorar la seguridad informática de los equipos de cómputo y redes de la Municipalidad distrital de Independencia* [Tesis de posgrado, Universidad Nacional Santiago Antúnez de Mayolo] Repositorio Institucional UNASAM.  
[http://repositorio.unasam.edu.pe/bitstream/handle/UNASAM/2655/T033\\_4602\\_2813\\_M.pdf?sequence=1&isAllowed=y](http://repositorio.unasam.edu.pe/bitstream/handle/UNASAM/2655/T033_4602_2813_M.pdf?sequence=1&isAllowed=y)
- Bramont, L. (2000). Delitos informáticos. *Revista Peruana de Derecho de la Empresa*, 51(2), 35-46.  
<http://revistas.upagu.edu.pe/index.php/NU/article/view/196>
- Bunge, M. (2015). La investigación científica.  
[https://www.ecured.cu/Investigaci%C3%B3n\\_cient%C3%ADfica](https://www.ecured.cu/Investigaci%C3%B3n_cient%C3%ADfica)
- Castillo, M. (2005). *Estudio Técnico de los Delitos Informáticos*. Editorial Futura
- Espinoza, M. (2017) *Derecho penal informático: deslegitimación del poder punitivo en la sociedad de control* [Tesis de pregrado, Universidad Nacional del Antiplano] Repositorio Institucional UNAP.  
[http://repositorio.unap.edu.pe/bitstream/handle/UNAP/6309/Espinoza\\_Coila\\_Michael.pdf?sequence=1&isAllowed=y](http://repositorio.unap.edu.pe/bitstream/handle/UNAP/6309/Espinoza_Coila_Michael.pdf?sequence=1&isAllowed=y)

Forbes. (2021). Covid-19 detona ciberataques en México: hasta 4 amenazas por segundo vía mail. <https://www.forbes.com.mx/ciberataques-4-por-segundo-mexico-2020/>

Gutiérrez, M. (1991) *Fraude informático y estafa*. Ministerio de Justicia

Hanco, E. (2018). *La Tipificación del Bien Jurídico Protegido en la Estructura del Tipo Penal Informático como causas de su deficiente regulación en la Ley 30096, Perú – 2017* [Tesis de pregrado, Universidad Nacional de San Agustín] Repositorio Institucional UNSA. <http://repositorio.unsa.edu.pe/bitstream/handle/UNSA/6436/DEhazaey.pdf?sequence=1&isAllowed=y>

Herrera, E. A. (2016). *El Phishing como delito informático y su falta de tipificación en el Código Orgánico Integral Penal* [Tesis de pregrado, Universidad Central del Ecuador] Repositorio Institucional UCE. <http://www.dspace.uce.edu.ec/bitstream/25000/8132/1/T-UCE-0013-Ab-399.pdf>

Herrera, L. M. (2018) *Eficacia de la ley de delitos informáticos en el distrito judicial de Huánuco 2017* [Tesis de pregrado, Universidad de Huánuco] Repositorio Institucional UDH. <http://repositorio.udh.edu.pe/bitstream/handle/123456789/1058/HERRERA%20OURSUA%2C%20Lesly%20Monica.pdf?sequence=1&isAllowed=y>

Hiplán, S. (2019) *La Ley 19.223 a 26 Años de su Promulgación* [Tesis de grado, Universidad de Chile] Repositorio Institucional UCHILE. <http://repositorio.uchile.cl/bitstream/handle/2250/173119/La-ley-N%C2%B019223-a-26-a%C3%B1os-de-su-promulgacion.pdf?sequence=1&isAllowed=y>

Hugo, S. (2014). Tipificación de los delitos informáticos patrimoniales en la nueva Ley de delitos informáticos N° 30096. *Alma Máter*, 1(69). <https://revistasinvestigacion.unmsm.edu.pe/index.php/alma/article/view/11870>

Levin, A. y Ilkina, D. (2013). *Comparación internacional del crimen cibernético*. Ryerson University.

López, J. (2019). *Métodos y técnicas de detección temprana de casos de phishing* [Tesis de posgrado, Universidad Oberta de Catalunya] Repositorio Institucional UOC.

<http://openaccess.uoc.edu/webapps/o2/bitstream/10609/89225/6/jlopezsanchez012TFM0119memoria.pdf>

Mayer, L. (2017). El bien jurídico protegido en los delitos informáticos. *Scielo*, 44(1). [https://scielo.conicyt.cl/scielo.php?script=sci\\_arttext&pid=S0718-34372017000100011](https://scielo.conicyt.cl/scielo.php?script=sci_arttext&pid=S0718-34372017000100011)

Moncada, A. (2020). Comparación de técnicas de machine learning para detección de sitios web de phishing. *Revista Universidad de Lima*, 13(01). <https://doi.org/10.26439/interfases2020.n013.4886>

Orts, E. (2001). *Delitos informáticos y delitos comunes cometidos a través de la informática*. Tirant Lo Blanch

Oxman, N. (2013). Estafas informáticas a través de internet acerca de la imputación penal del “phishing” y el “pharming”. *Redalyc*, 2(12). <https://www.redalyc.org/pdf/1736/173629692007.pdf>

Paredes, J. M. (2013). *De los delitos cometidos con el uso de sistemas informáticos en el distrito judicial de Lima, en el periodo 2009-2010* [Tesis de posgrado, Universidad Nacional Mayor de San Marcos] Repositorio Institucional UNMSM. [http://cybertesis.unmsm.edu.pe/bitstream/handle/20.500.12672/10314/Paredes\\_pj.pdf?sequence=3&isAllowed=y](http://cybertesis.unmsm.edu.pe/bitstream/handle/20.500.12672/10314/Paredes_pj.pdf?sequence=3&isAllowed=y)

Pardo, A. (2018). *Tratamiento jurídico penal de los delitos informáticos contra el patrimonio, Distrito Judicial de Lima, 2018* [Tesis de posgrado, Universidad

César Vallejo] Repositorio Institucional UCV.  
[https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/20372/Pardo\\_VA.pdf?sequence=1&isAllowed=y](https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/20372/Pardo_VA.pdf?sequence=1&isAllowed=y)

Romero, M. Figueroa, G., Vera, D., Alava, J. (2018). *Introducción a la seguridad informática y el análisis de vulnerabilidades*. <https://www.3ciencias.com/wp-content/uploads/2018/10/Seguridad-inform%C3%A1tica.pdf>

Sánchez, D. (2020) *Estudio teleológico del carding y bins. Su impunidad e impacto en el sistema mexicano* [Tesis de pregrado, Benemérita Universidad Autónoma de Puebla] Repositorio Institucional BUAP.  
<https://repositorioinstitucional.buap.mx/bitstream/handle/20.500.12371/11702/20210223150451-5912-TL.pdf?sequence=2>

Sánchez, J. (2016). *Delitos informáticos*. Academia de la Magistratura.  
<http://repositorio.amag.edu.pe/bitstream/handle/123456789/623/MANUAL%20CURSO%20DELITOS%20INFORMATICOS.pdf?sequence=4&isAllowed=y>

Sarzana, C. (2010). *El Uso Indebido de Tarjetas de Crédito*. Editorial Temis

Sequeiros, I.C. (2016) *Vacíos legales que imposibilitan la sanción de los delitos informáticos en el Nuevo Código Penal Peruano - 2015* [Tesis de pregrado, Universidad de Huánuco] Repositorio Institucional UDH.  
<http://repositorio.udh.edu.pe/bitstream/handle/123456789/286/IVETT%20CLARITZA%20SEQUEIROS%20CALDERON.pdf?sequence=1&isAllowed=y>

Valle, J.C. (2013). *El delito informático de phishing* [Tesis de pregrado, Universidad Regional Autónoma de Los Andes] Repositorio Institucional UNIANDES.  
<https://dspace.uniandes.edu.ec/bitstream/123456789/2819/1/TUQMDPC005-2013.pdf>

Vega, J. (2010) *Los delitos informáticos en el Código Penal* [Tesis de grado, Universidad Católica de Santa María] Repositorio Institucional UCSM.



<http://tesis.ucsm.edu.pe/repositorio/bitstream/handle/UCSM/6824/88.0774.MG.pdf?sequence=1&isAllowed=y>

Villavicencio, F. (2014). Delitos informáticos. *Ius Et Veritas*, 24(49), 284-304.  
<http://revistas.pucp.edu.pe/index.php/iusetveritas/article/view/13630/14253>

Villavicencio, F. (2013). *Derecho Penal- Parte general*. Grijley

Zorrilla, K. J. (2018). *Inconsistencias y ambigüedades en la Ley de delitos informáticos Ley N° 30096 y su modificatoria Ley N° 30171, que imposibilitan su eficaz cumplimiento* [Tesis de pregrado, Universidad Nacional de Ancash]  
Repositorio Institucional UNASAM.  
[http://repositorio.unasam.edu.pe/bitstream/handle/UNASAM/2332/T033\\_7022\\_1905\\_T.pdf?sequence=1&isAllowed=y](http://repositorio.unasam.edu.pe/bitstream/handle/UNASAM/2332/T033_7022_1905_T.pdf?sequence=1&isAllowed=y)

## ANEXOS

### ANEXO I: Matriz de consistencia

**TÍTULO: MODIFICACIÓN DE LA LEY 30096 PARA INCORPORAR LOS DELITOS DE PHISHING, PHARMING Y CARDING COMO DELITOS PENALIZABLES CON PRISIÓN, PARA REDUCIR LA CIBERDELINCUENCIA, LIMA 2019.**

VARIABLES	PROBLEMA	HIPÓTESIS	OBJETIVOS
<b>INDEPENDIENTE :</b>  Delitos informáticos	¿Permitirá la modificación de la Ley 30096 para incorporar los delitos de Phishing, Pharming y Carding como delitos penalizables con prisión reducir la ciberdelincuencia, Lima 2019?	La modificación de la Ley N° 30096 incorporando los delitos de Phishing, pharming y carding reducirán el índice de ciberdelincuencia en el Perú.	<b>GENERAL:</b>  Justificar por qué los delitos de Phishing, Pharming y Carding deben ser incorporados a la Ley N° 30096 como delitos penalizables con penas privativas de la libertad  <b>ESPECÍFICOS:</b>
<b>DEPENDIENTE:</b>  La modificación de la Ley N° 30096			

			<p><b>1. Establecer la incidencia de no encontrarse reguladas las actividades conocidas como Phishing, Pharming y Carding como delitos informáticos inciden en los derechos de los usuarios.</b></p> <p><b>2. Analizar la ley N° 30096 – Ley de delitos informáticos, a fin de evaluar si se considera los delitos de Phishing, Pharming y Carding como delitos penalizables.</b></p> <p><b>3. Examinar las deficiencias legislativas en relación a la tipificación de los delitos informáticos que atentan a la totalidad de sistemas informáticos en legislación extranjera.</b></p>
--	--	--	--

## ANEXO II: Ficha de Análisis documental

### DATOS GENERALES

TÍTULO DEL PROYECTO:

NOMBRE DE LA UNIVERSIDAD:

FECHA DE REALIZACIÓN

Variable Independiente: Modificación de la Ley N° 30096

INDICADOR	FUENTES DE INFORMACIÓN	APORTE
<b>Base normativa</b>	Constitución Política del Perú	
	Ley N° 30096	
	Análisis jurídico	

Variable Dependiente: Incorporar delitos de phishing, pharming y carding

INDICADOR	FUENTES DE INFORMACIÓN	APORTE
<b>Delitos informáticos</b>	Ley	
	Doctrina	
	Derecho Comparado	

## Anexo III: LEY N° 30096

### LEY DE DELITOS INFORMÁTICOS



#### 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.- Propositiones 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.- Propositiones 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  
Modifícase 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

Modifícase 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

## Anexo IV: Legislación Comparada



### Ley 19.223

#### **TIPIFICA FIGURAS PENALES RELATIVAS A LA INFORMÁTICA**

#### **MINISTERIO DE JUSTICIA**

Teniendo presente que el H. Congreso Nacional ha dado su aprobación al siguiente

Proyecto de Ley:

"Artículo 1°.- El que maliciosamente destruya o inutilice un sistema de tratamiento de información o sus partes o componentes, o impida, obstaculice o modifique su funcionamiento, sufrirá la pena de presidio menor en su grado medio a máximo.

Si como consecuencia de estas conductas se afectaren los datos contenidos en el sistema, se aplicará la pena señalada en el inciso anterior, en su grado máximo.

Artículo 2°.- El que con el ánimo de apoderarse, usar o conocer indebidamente de la información contenida en un sistema de tratamiento de la misma, lo intercepte, interfiera o acceda a él, será castigado con presidio menor en su grado mínimo a medio.

Artículo 3°.- El que maliciosamente altere, dañe o destruya los datos

contenidos en un sistema de tratamiento de información, será castigado con presidio menor en su grado medio.

Artículo 4°.- El que maliciosamente revele o difunda los datos contenidos en un sistema de información, sufrirá la pena de presidio menor en su grado medio. Si quien incurre en estas conductas es el responsable del sistema de información, la pena se aumentará en un grado."

Y por cuanto he tenido a bien aprobarlo y sancionarlo; por tanto promúlguese y llévase a efecto como Ley de la República.

Santiago, 28 de Mayo de 1993.-  
ENRIQUE KRAUSS RUSQUE,  
Vicepresidente de la

República.- Francisco Cumplido  
Cereceda, Ministro de Justicia.

Lo que transcribo a Ud. para su conocimiento.- Saluda atentamente a Ud., Martita

Worner Tapia, Subsecretario de  
Justicia.





### **Ley 26.388**

El Senado y Cámara de Diputados de la Nación Argentina reunidos en Congreso, etc. sancionan con fuerza de Ley:

ARTÍCULO 1º — Incorporáanse como últimos párrafos del artículo 77 del Código Penal, los siguientes:

El término "documento" comprende toda representación de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento, archivo o transmisión.

Los términos "firma" y "suscripción" comprenden la firma digital, la creación de una firma digital o firmar digitalmente.

Los términos "instrumento privado" y "certificado" comprenden el documento digital firmado digitalmente.

ARTICULO 2º — Sustitúyese el artículo 128 del Código Penal, por el siguiente:

Artículo 128: Será reprimido con prisión de seis (6) meses a cuatro (4) años el que produjere, financiare, ofreciere, comerciare, publicare, facilitare, divulgare o distribuyere, por cualquier medio, toda representación de un menor de dieciocho (18) años dedicado a actividades sexuales

explícitas o toda representación de sus partes genitales con fines predominantemente sexuales, al igual que el que organizare espectáculos en vivo de representaciones sexuales explícitas en que participaren dichos menores.

Será reprimido con prisión de cuatro (4) meses a dos (2) años el que tuviere en su poder representaciones de las descritas en el párrafo anterior con fines inequívocos de distribución o comercialización.

Será reprimido con prisión de un (1) mes a tres (3) años el que facilitare el acceso a espectáculos pornográficos o suministrare material pornográfico a menores de catorce (14) años.

ARTICULO 3º — Sustitúyese el epígrafe del Capítulo III, del Título V, del Libro II del Código Penal, por el siguiente:

*"Violación de Secretos y de la Privacidad"*

ARTICULO 4º — Sustitúyese el artículo 153 del Código Penal, por el siguiente:

Artículo 153: Será reprimido con prisión de quince (15) días a seis (6) meses el que abriere o accediere indebidamente a una comunicación electrónica, una carta, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, que no le esté dirigido; o se apoderare indebidamente de una comunicación electrónica, una carta, un pliego, un despacho u otro papel privado, aunque no esté cerrado; o indebidamente suprimiere o desviare

de su destino una correspondencia o una comunicación electrónica que no le esté dirigida.

En la misma pena incurrirá el que indebidamente interceptare o capture comunicaciones electrónicas o telecomunicaciones provenientes de cualquier sistema de carácter privado o de acceso restringido.

La pena será de prisión de un (1) mes a un (1) año, si el autor además comunicare a otro o publicare el contenido de la carta, escrito, despacho o comunicación electrónica.

Si el hecho lo cometiere un funcionario público que abusare de sus funciones, sufrirá además, inhabilitación especial por el doble del tiempo de la condena.

ARTICULO 5º — Incorpórase como artículo 153 bis del Código Penal, el siguiente:

Artículo 153 bis: Será reprimido con prisión de quince (15) días a seis (6) meses, si no resultare un delito más severamente penado, el que a sabiendas accediere por cualquier medio, sin la debida autorización o excediendo la que posea, a un sistema o dato informático de acceso restringido.

La pena será de un (1) mes a un (1) año de prisión cuando el acceso fuese en perjuicio de un sistema o dato informático de un organismo público estatal o de un proveedor de servicios públicos o de servicios financieros.

ARTICULO 6º — Sustitúyese el artículo 155 del Código Penal, por el siguiente:

Artículo 155: Será reprimido con multa de pesos un mil quinientos (\$ 1.500) a pesos cien mil (\$ 100.000), el que hallándose en posesión de una correspondencia, una comunicación electrónica, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, no destinados a la publicidad, los hiciere publicar indebidamente, si el hecho causare o pudiere causar perjuicios a terceros.

Está exento de responsabilidad penal el que hubiere obrado con el propósito inequívoco de proteger un interés público.

ARTICULO 7º — Sustitúyese el artículo 157 del Código Penal, por el siguiente:

Artículo 157: Será reprimido con prisión de un (1) mes a dos (2) años e inhabilitación especial de un (1) a cuatro (4) años, el funcionario público que revelare hechos, actuaciones, documentos o datos, que por ley deben ser secretos.

ARTICULO 8º — Sustitúyese el artículo 157 bis del Código Penal, por el siguiente:

Artículo 157 bis: Será reprimido con la pena de prisión de un (1) mes a dos (2) años el que:

1. A sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales;
2. Ilegítimamente proporcionare o revelare a otra información registrada en un archivo o en un banco de datos

personales cuyo secreto estuviere obligado a preservar por disposición de la ley.

3. Ilegítimamente insertare o hiciere insertar datos en un archivo de datos personales.

Cuando el autor sea funcionario público sufrirá, además, pena de inhabilitación especial de un (1) a cuatro (4) años.

ARTICULO 9º — Incorpórase como inciso 16 del artículo 173 del Código Penal, el siguiente:

Inciso 16. El que defraudare a otro mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos.

ARTICULO 10. — Incorpórase como segundo párrafo del artículo 183 del Código Penal, el siguiente:

En la misma pena incurrirá el que alterare, destruyere o inutilizare datos, documentos, programas o sistemas informáticos; o vendiere, distribuyere, hiciere circular o introdujere en un sistema informático, cualquier programa destinado a causar daños.

ARTICULO 11. — Sustitúyese el artículo 184 del Código Penal, por el siguiente:

Artículo 184: La pena será de tres (3) meses a cuatro (4) años de prisión, si mediare cualquiera de las circunstancias siguientes:

1. Ejecutar el hecho con el fin de impedir el libre ejercicio de la

autoridad o en venganza de sus determinaciones;

2. Producir infección o contagio en aves u otros animales domésticos;

3. Emplear sustancias venenosas o corrosivas;

4. Cometer el delito en despoblado y en banda;

5. Ejecutarlo en archivos, registros, bibliotecas, museos o en puentes, caminos, paseos u otros bienes de uso público; o en tumbas, signos conmemorativos, monumentos, estatuas, cuadros u otros objetos de arte colocados en edificios o lugares públicos; o en datos, documentos, programas o sistemas informáticos públicos;

6. Ejecutarlo en sistemas informáticos destinados a la prestación de servicios de salud, de comunicaciones, de provisión o transporte de energía, de medios de transporte u otro servicio público.

ARTICULO 12. — Sustitúyese el artículo 197 del Código Penal, por el siguiente:

Artículo 197: Será reprimido con prisión de seis (6) meses a dos (2) años, el que interrumpiere o entorpeciere la comunicación telegráfica, telefónica o de otra naturaleza o resistiere violentamente el restablecimiento de la comunicación interrumpida.

ARTICULO 13. — Sustitúyese el artículo 255 del Código Penal, por el siguiente:

Artículo 255: Será reprimido con prisión de un (1) mes a cuatro (4) años, el que sustrajere, alterare, ocultare, destruyere o inutilizare en todo o en parte objetos destinados a servir de prueba ante la autoridad competente, registros o documentos confiados a la custodia de un funcionario público o de otra persona en el interés del servicio público. Si el autor fuere el mismo depositario, sufrirá además inhabilitación especial por doble tiempo.

Si el hecho se cometiere por imprudencia o negligencia del depositario, éste será reprimido con multa de pesos setecientos cincuenta (\$ 750) a pesos doce mil quinientos (\$ 12.500).

ARTICULO 14. — Deróganse el artículo 78 bis y el inciso 1º del artículo 117 bis del Código Penal.

ARTICULO 15. — Comuníquese al Poder Ejecutivo.

DADA EN LA SALA DE SESIONES DEL CONGRESO ARGENTINO, EN BUENOS AIRES, A LOS CUATRO DIAS DEL MES DE JUNIO DEL AÑO DOS MIL OCHO.



**Código Penal Federal**  
**Capítulo II - Acceso ilícito a**  
**Sistemas y Equipos de Informática**

**Artículo 211 bis 1**

Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa.

**Artículo 211 bis 2**

Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de uno a cuatro años de prisión y de doscientos a seiscientos días multa.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le

impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.

A quien sin autorización conozca, obtenga, copie o utilice información contenida en cualquier sistema, equipo o medio de almacenamiento informáticos de seguridad pública, protegido por algún medio de seguridad, se le impondrá pena de cuatro a diez años de prisión y multa de quinientos a mil días de salario mínimo general vigente en el Distrito Federal. Si el responsable es o hubiera sido servidor público en una institución de seguridad pública, se impondrá además, destitución e inhabilitación de cuatro a diez años para desempeñarse en otro empleo, puesto, cargo o comisión pública.

Las sanciones anteriores se duplicarán cuando la conducta obstruya, entorpezca, obstaculice, limite o imposibilite la procuración o impartición de justicia, o recaiga sobre los registros relacionados con un procedimiento penal resguardados por las autoridades competentes.

**Artículo 211 bis 3**

Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de dos a ocho años de prisión y de trescientos a novecientos días multa.

Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente

copie información que contengan, se le impondrán de uno a cuatro años de prisión y de ciento cincuenta a cuatrocientos cincuenta días multa.

A quien estando autorizado para acceder a sistemas, equipos o medios de almacenamiento informáticos en materia de seguridad pública, indebidamente obtenga, copie o utilice información que contengan, se le impondrá pena de cuatro a diez años de prisión y multa de quinientos a mil días de salario mínimo general vigente en el Distrito Federal. Si el responsable es o hubiera sido servidor público en una institución de seguridad pública, se impondrá además, hasta una mitad más de la pena impuesta, destitución e inhabilitación por un plazo igual al de la pena resultante para desempeñarse en otro empleo, puesto, cargo o comisión pública.

#### Artículo 211 bis 4

Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a dos años

de prisión y de cincuenta a trescientos días multa.

#### Artículo 211 bis 5

Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa.

Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente copie información que contengan, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa.

Las penas previstas en este artículo se incrementarán en una mitad cuando las conductas sean cometidas por funcionarios o empleados de las instituciones que integran el sistema financiero.

#### Artículo 211 bis 6

Para los efectos de los artículos 211 Bis 4 y 211 Bis 5 anteriores, se entiende por instituciones que integran el sistema financiero, las señaladas en el artículo 400 Bis de este Código.

#### Artículo 211 bis 7

Las penas previstas en este capítulo se aumentarán hasta en una mitad cuando la información obtenida se utilice en provecho propio o ajeno.

## **Propuesta**

Ley N° 30096 con la incorporación de los artículos

### **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 deliberada e ilegítimamente accede a todo o en parte de un sistema informático, siempre que se realice con vulneración de medidas de seguridad establecidas para impedirlo, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días-multa. Será reprimido con la misma pena, el que accede a un sistema informático excediendo lo autorizado.

#### **Artículo 3. Atentado a la integridad de datos informáticos**

El que deliberada e ilegítimamente daña, introduce, borra, deteriora, altera, suprime o hace inaccesibles datos informáticos, será reprimido con

pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días-multa.

#### **Artículo 4. Atentado contra 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.

#### **Artículo 5. Atentado contra la seguridad jurídica y confianza – Phishing**

El que, mediante medios informáticos suplanta la identidad de una persona o una organización con el objetivo de engañar a terceras personas, valiéndose de la confianza que esta tiene en las organizaciones para revelar información confidencial, será reprimido con una pena privativa de libertad no menor de 4 ni mayor de 8 años.

#### **Artículo 6. Atentado contra los sitios web – Pharming**

El que, mediante medios informáticos suplanta o tergiversa la identidad de un sitio web, valiéndose de sus conocimientos para obtener información confidencial de terceros, será reprimido con una pena privativa de libertad no menor de 4 ni mayor de 8 años.

### **Artículo 7. Atentado contra los sitios web – Carding**

El que, mediante medios informáticos accede ilegalmente a los datos de una tarjeta de crédito o débito con la finalidad de aprovecharse de terceros, será reprimido con una pena privativa de libertad no menor de 4 ni mayor de 8 años.

## **CAPÍTULO III DELITOS INFORMÁTICOS CONTRA LA INDEMNIDAD Y LIBERTAD SEXUALES**

### **Artículo 6. Propositiones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos**

El que a través de internet u otro medio análogo contacta con un menor de catorce años para solicitar u obtener de él material pornográfico, o para proponerle llevar a cabo cualquier acto de connotación sexual con él o con tercero, será reprimido con una pena privativa de libertad no menor de cuatro ni mayor de ocho años e inhabilitación conforme a los numerales 1, 2, 4 y 9 del artículo 36 del **Código Penal**.

Cuando la víctima tiene entre catorce y menos de dieciocho años de edad y medie engaño, la pena será no menor de tres ni mayor de seis años e inhabilitación conforme a los numerales 1, 2, 4 y 9 del artículo 36 del **Código Penal**.

## **CAPÍTULO IV DELITOS INFORMÁTICOS CONTRA LA INTIMIDAD Y EL SECRETO DE**

## **LAS COMUNICACIONES**

### **Artículo 7. Tráfico ilegal de datos**

**\*Derogado**

### **Artículo 8. 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 9. 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.