UNIVERSIDAD CATÓLICA SANTO TORIBIO DE MOGROVEJO

FACULTAD DE DERECHO

ESCUELA DE DERECHO

Incorporación de la modalidad del Phishing en la Ley de Delitos Informáticos

TESIS PARA OPTAR EL TÍTULO DE

ABOGADO

AUTOR

Jhunior Stalyn Carrero Perez

ASESOR

Jose Leoncio Ivan Constantino Espino

https://orcid.org/0000-0003-0120-7444

Chiclayo, 2024

Incorporación de la modalidad del Phishing en la Ley de Delitos Informáticos

PRESENTADA POR

Jhunior Stalyn Carrero Perez

A la Facultad de Derecho de la
Universidad Católica Santo Toribio de Mogrovejo
para optar el título de

ABOGADO

APROBADA POR

Gladys Yolanda Patricia Ramos Soto Caceres
PRESIDENTE

Fatima del Carmen Perez Burga
SECRETARIO

Jose Leoncio Ivan Constantino Espino
VOCAL

Dedicatoria

Dedico el presente trabajo a mis padres, Jorge y Olga, porque han sido el sustento y el motor más importante de mi vida hasta la fecha. A mis hermanos, Leo, Luis y Dayron, porque han sido mis fieles compañeros y mi motor de superación. Y a mis amigos y compañeros, que han sabido diluir mis tristezas y preocupaciones.

Agradecimientos

El agradecimiento de este trabajo de investigación es para mis padres, por el esfuerzo constante y el sacrificio hecho para mi desarrollo profesional y personal; para mi asesor Dr. Jose Leoncio Ivan Constantino Espino y a todos los profesores que fueron parte de mi etapa universitaria, por su tiempo y sus sabias enseñanzas.

TRABAJO FINAL DE TITULACIÓN

INFORME DE ORIGINALIDAD

23%	22%	9%	16%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	repositorio.uns.edu.pe Fuente de Internet	2%
2	ri.ues.edu.sv Fuente de Internet	2%
3	Submitted to Universidad Americana Trabajo del estudiante	2%
4	Submitted to Universidad Católica Santo Toribio de Mogrovejo Trabajo del estudiante	2%
5	hdl.handle.net Fuente de Internet	2%
6	www.bcn.cl Fuente de Internet	2%
7	Submitted to Corporación Universitaria del Caribe Trabajo del estudiante	1%
8	Submitted to Universidad Internacional de la Rioja Trabajo del estudiante	1%

Índice

Resumen

La tipificación del phishing en la ley de delitos informáticos es de suma urgencia. Porque el nivel de incidencia de este delito a nivel nacional viene aumentando año con año. Sin embargo, la realidad nacional, el desconocimiento y el aumento de la tecnología vienen siendo los factores sociales que más afectan al aumento de esta clase de delitos. Ahora bien, la realidad social no puede ser ajena, debido al avance tecnológico que se está viviendo. En ese sentido, la presente investigación tiene como objetivo Proponer la tipificación de la modalidad del phishing en el artículo 8 de la ley de Delitos Informáticos. Se utilizó la metodología analítica, ya que esta ayudó a dar una solución a cada variable de nuestra problémica, sumado a ello se empleó legislación nacional y extranjera, y datos estadísticos. Como resultado de la investigación, divisamos que proponer la incorporación del phishing en la ley de delitos informáticos es viable y necesario.

Palabras clave: Delitos informáticos, el fraude informático y el phishing.

Abstract

The criminalization of phishing in the law of computer crimes is of utmost urgency. Because the level of incidence of this crime at the national level has been increasing year by year. However, the national reality, the lack of knowledge and the increase of technology are the social factors that most affect the increase of this kind of crime. However, the social reality cannot be ignored, due to the technological progress that is being experienced. In this sense, the objective of this research is to propose the typification of the phishing modality in article 8 of the Computer Crimes Law. The analytical methodology was used, since it helped to give a solution to each variable of our problem, in addition to this, national and foreign legislation and statistical data were used. As a result of the research, we concluded that proposing the incorporation of phishing in the computer crime law is feasible and necessary.

Keywords: cibercryme, computer fraud y phishing

Introducción

De manera general, el phishing es un acto ilícito y una modalidad de los delitos informáticos, cuyos delitos son cometidos a través de medios tecnológicos buscando robar información personal o patrimonial de los internautas; sin embargo, es una modalidad que no está regulada en la legislación nacional. Por lo tanto, esta investigación intenta desarrollar la incorporación de la modalidad del phishing en la ley de Delito Informáticos, Ley 30096. Respecto al phishing, aunque se han pronunciado muchos juristas y existe un nivel de incidencia muy alto en el país, todavía no existe una legislación que sancione estos delitos. Cabe resaltar, Perú tiene la Ley 30096 que incorpora los delitos informáticos, pero tiene muchas inconsistencias por el contexto sociohistórico en que se promulgó la misma

A nivel global, los delitos informáticos han ido aumentando paulatinamente, esto se debe porque hay un avance desmesurado de la tecnología en el ámbito social y personal del ser humano y a la globalización que se vive día con día. Risk-Based Security, una empresa influyente en el ámbito de la ciberseguridad en el mundo, esclarece que solamente para el 2020 hubo un aumento de 36 millones de registros en comparación con años anteriores sobre la violación a los datos personales de los usuarios de computadoras, Tablet u cualquier otro medio tecnológico. Además, resalta que de la totalidad de los delitos informáticos, el 34% corresponde a un ilícito en modalidad del phishing, buscando un beneficio patrimonial.

Asimismo, en Latinoamérica, la incidencia del delito del phishing creció exponencialmente con la pandemia del COVID -19, ya que existió una cuarentena a nivel mundial en la que los medios tecnológicos se convirtieron en una extensión humana más que una herramienta. En el 2021, Kasperski, un antivirus de renombre, reveló mediante un informe anual ejecutado por el equipo de investigación y análisis de la compañía que los ciberataques a los usuarios aumentaron a un 24% en comparación con el año 2019. Inclusive, en el mismo informe, se enlistaron a los países latinos que tienen más afluencia en este tipo de delitos informáticos, este listado está liderado por Ecuador, seguido por Perú, panamá, Guatemala y Venezuela. En el mismo informe se estipuló que se registraron más de 173 mil intentos de infección móvil (phishing), buscando robar datos personales o estados de cuentas de mencionados usuarios.

Ahora bien, en nuestro país se debe tener en cuenta que la mayoría de la población cuenta con acceso a algún medio tecnológico. La INEI menciona que el 90% de los peruanos cuentan con al menos un celular (2017). Es decir, el 90% de la población es probable que se enfrente a un delito informático o intento del mismo.

Durante el mes de noviembre del 2019, según el Ministerio Publico, se registró un total de 6,906 delitos informáticos, cifra ascendente al 79.33% a los delitos registrados en el mismo

período del año 2018 que fueron de 3,851 delitos; esto quiere decir que se duplicó el número de incidencias. Además, los delitos informáticos contra el patrimonio tienen una mayor incidencia se presenta con un 38.24%. (2019, p. 59).

Posteriormente, en el año 2020, se registró un total de 8,674 delitos informáticos (Ley N°30096), donde el mayor porcentaje se agrupa en delitos informáticos contra el patrimonio con 54.65% (4,741 delitos). (2020, p. 50). De esta manera se afecta directa e indirecta los datos personales y patrimoniales de los diversos usuarios que utilizan algún medio tecnológico.

La causa principal del aumento del phishing se debe al libre acceso a los medios tecnológicos, porque al no tener los alcances que posee la tecnología, facilita que sea empleada como móvil para la comisión de un delito informático. Asimismo, La facilidad de emplear los medios tecnológicos como un medio o el fin de la comisión del delito, tiene como causa principal la inexistencia legislativa penal que sancione la utilización de medios informáticos y tecnológicos.

Al considerar el análisis descrito, surge la siguiente problemática: ¿Cómo se deberá incorporar PHISHING como modalidad en el artículo 8 de la ley de delitos informáticos? Asimismo, como objetivos específicos se ha considerado: a) analizar el phishing como tipo penal en el derecho peruano y extranjero; y, b) fundamentar en la doctrina las razones por las cuales el phishing deben ser considerados como tipos penales.

En razón a la cuestión antes planteada que se formuló la siguiente hipótesis: Si los delitos informáticos tienen una evolución constante, se emplean diversos equipos informáticos para obtener datos informáticos y patrimoniales de diversos usuarios, entonces la necesidad de la regulación de la figura jurídica en la ley de delitos informáticos como:

a) El phishing; como aquella alternativa de los delincuentes para expropiarse de información personal o bienes patrimoniales a través de estrategias que incluyen aparatos tecnológicos y principalmente el internet, perjudicando de esta manera a los muchos usuarios que emplean un aparato tecnológico con servicio a una red de internet. Además, es calificado por el Ministerio Publico como el delito con mayor incidencia en el periodo 2019 – 2020.

El trabajo se ha estructurado en tres capítulos. En el primer capítulo se evidenciará los limites del presente trabajo de investigación. Ahora bien, en el segundo capítulo contendrá varios conceptos y definiciones. Finalmente, en el último capítulo, se evidenciará el análisis y el escrutinio del porqué se debe incorporar a la Ley de Delitos Informáticos.

La importancia de este trabajo de investigación es la incorporación en el artículo 8 el tipo penal del phishing, porque se ha visto un incremento notable de estos tipos de modalidades

ara el robo de bienes patrimoniales a nivel global Es por ello que el Perú necesita una incorporación de este tipo penal, para que, al momento de establecerse el procedimiento penal, los fiscales y jueces tengan normas que sustente su postura e incriminen a estos delincuentes.

I. Revisión de literatura

Según el Instituto Universitario del Centro de México se entiende por revisión de la literatura como aquella que "Consiste en destacar, obtener y consultar la bibliografía y otros materiales que pueden ser útiles para los propósitos de estudio, de donde se debe extraer y recopilar la información relevante y necesaria que atañe a nuestro problema de investigación." (p.7)

1.1. Antecedentes

La revista "IT DIGITAL SEGURITY" indica que varios usuarios reportaron más de nueve millones de correos electrónicos sospechosos, existe un aumento del 67% más con respecto a 2018 en todo el mundo. Durante el 2019 hubo reportes de al menos un 55% de las organizaciones de todo el mundo se enfrentaron a ataques de Pishing, un 88% informó de ataques de suplantación de identidad, un 86% informó de ataques de redes sociales, el 84% informó de smishing (SMS/texto), un 83% informó de vishing (voz) y el 81% informó de USB malicioso. Los profesionales de ciberseguridad aseguran que durante el 2020 que existe un aumento del 75% con el secuestro de datos informáticos en varias partes del mundo, pero solamente el 33% de estas personas optaron por recuperar sus datos personales, de las cuales solamente el 22% pagaron, mas no pudieron recuperar su acceso de datos. El grupo APWG (Anti-pishing working group-Europe), una organización internacional, esta indica que durante el 2020 los delitos informáticos se duplicaron. Además, revela que durante el 2021 existió un alza con 245 771 ataques cibernéticos sólo en un mes. Luego, la cantidad de ataques disminuyó en febrero y marzo, aun así, durante marzo sufrió más de 200 000 ataques y fue el cuarto peor mes en la historia de informes del APWG.

En América latina, según la revista "STATISTA", durante setiembre del 2020, casi el 56% de los ciberataques se dirigieron en contra usuarios o infraestructuras ubicadas en Brasil, mientras que aproximadamente el 28% se dirigieron a usuarios en México, Colombia ocupa el tercer lugar con más del 10% de los ataques cibernéticos. Perú ocupa el cuarto lugar con la tasa del 6% en ataques cibernéticos. Durante los primeros meses, en América Latina, los ciberataques crecen un 24% durante los primeros ocho meses de 2021; según esta misma revista, las principales amenazas asechan a la región un promedio de 35 ataques por segundo. Kaspersky, a través su página, anunció en un informe anual que toma en cuenta 20 programas maliciosos. Se concluyó que la seguridad informática debe ser una prioridad.

Además, la tasa de crecimiento a comparación con el 2020 es abismal. La lista de países la lidera Ecuador (+75%), seguido por Perú (+71%), Panamá (+60%), Guatemala (+43%) y Venezuela (+29%). En total, solo el Top20 de malware en la región genera un promedio de 35 ataques por segundo. En este contexto, Brasil lidera la región con más de 1,390 intentos de infección por minuto, seguido de México (299 por minuto); Perú (96 por minuto), Ecuador (89 por minuto) y Colombia (87 por minuto).

En Perú, existe un aumento de delitos informáticos sobre todo en el periodo 2019 – 2020. Según el Ministerio Publico, al mes de noviembre del año 2019, se registró un total de 6,906 delitos informáticos, cifra mayor en un 79.33% a los delitos registrados en el mismo período del año 2018 que fueron de 3,851 delitos; asimismo, al mes de noviembre del 2019 se puede observar que el tipo de delito con mayor incidencia se presenta en los delitos informáticos contra el patrimonio con un 38.24%. Durante el año 2020, se registraron un total de 8,674 delitos informáticos – Ley N°30096, donde el mayor porcentaje se concentra en delitos informáticos contra el patrimonio con 54.65% (4,741 delitos).

El objetivo de esta investigación está orientado a evidenciar lo importante que es el incorporar y evaluar las nuevas modalidades existentes para cometer delitos informáticos, siendo los principales el de sabotaje, pishing, vishing y smishing en el ordenamiento jurídico peruano. Con esto, buscaríamos la incorporación de tipos penales dentro de la Ley N° 30096, ya que esta no cuenta con una actualización adecuada desde que en febrero del 2014 se promulgó la Ley N° 30171 que modifica la ley N° 30096. Todo esto indica que nuestros legisladores pecan de holganza frente a los muchos delitos informáticos suscitados en los últimos años, existiendo una limitación taxativa en nuestro ordenamiento. Frente a todo esto, la descripción del problema sería: ¿Cómo se deberían incorporar el Pishing como modalidad en el artículo 8 de la Ley N° 30096?

Los medios tecnológicos actualmente son utilizados por la mayoría de peruanos, la INEI (Instituto Nacional de Estadísticas e Informática), solamente hasta el 2018 corroboró qué la utilización de las TIC es casi universal, siendo su cifra:

“En los hogares cuyo jefe cuentan con educación universitaria el acceso es casi total (99,7%); los hogares con jefe que tiene educación superior no universitaria el 99,2% tienen acceso a alguna TIC, en los hogares con jefes que tienen educación

secundaria el 96,6% y entre aquellos con educación primaria o menor nivel el 83,5%." (Informe técnico, junio 2018; p. 2)

El diario GESTIÓN nos muestra la realidad sobre el internet y el acceso que posee la población peruana a un medio que se a convertido en necesario a nuestra nueva realidad, constatando que al tercer trimestre del 2020, el 70.3% de la población de Perú, a partir de los seis años, contaba con acceso a internet, según la Encuesta Nacional de Hogares (Enaho). Asimismo, se pudo conocer que la mayor penetración se encuentra en la capital del país. La población de Lima Metropolitana con acceso a internet alcanzaba el 83.4% a setiembre del 2020, superando las áreas resto urbano y rural, en donde el indicador llega al 73.8% y 41.7%, respectivamente.

Al analizar ambos criterios, debemos concluir que la gran mayoría de peruanos cuenta al menos con un dispositivo tecnológico y con acceso a internet, siendo vulnerables para que sea este el objeto o el medio de la comisión de un delito. Además, al contar con la Ley N° 30096 y su modificatoria, la ley N° 30171 del 2014 podemos inquirir la existencia de ciertas deficiencias taxativas en la norma, y por supuesto, su antigüedad da por sentado la precariedad de tipos penales dentro de la misma, siendo inservible para una sociedad que ha ido desarrollándose a un ritmo abrumador, siendo un problema actualmente los delitos como el pishing, vishing, el sabotaje y el smishing. Pero que no están estipulados en la norma de manera clara y precisa, dejando desprotegido a una sociedad que actualmente utiliza las TIC como una extensión del ser humano.

Por ello, hemos llegado a la hipótesis de plantear la incorporación dentro de la Ley N° 30096 y su modificatoria, el reconocimiento de los tipos penales, como el sabotaje, el pishing, vishing y smishing dentro del ordenamiento jurídico, ya que es necesario para la sociedad actual a la que nos enfrentamos, siendo las TIC y el acceso al internet un objeto o medio de comisión de delito.

1.2. Bases teóricas científicas

1.2.1. Los Delitos Informáticos

Para el Derecho comparado, no existe una definición propia del delito informático. Por defecto, no existe una definición universal sobre este tema, aunque varios expertos ya han brindado una definición propia partiendo de las realidades propias de cada país.

Por tanto, para Delgado, M., los delitos informáticos también se le llama delitos cibernéticos o computer related crimes; porque están relacionados con el ordenador u otro medio tecnológico. Garzón y Vizuete en su Tesis de Grado, agregan que los delitos

informáticos: “se consideran como una conducta condenada por la legislación que implica la utilización de tecnologías digitales en la comisión del delito; dirigiéndose a las propias tecnologías de la computación y las comunicaciones; al incluir la utilización incidental de computadoras en su comisión” (2009; p. 1).

Para Vinelli, R. (2021); en la legislación nacional peruana, la acepción que adquirió sobre los delitos informáticos es la restringida, mediante la cual se establece que la comisión de un delito se da por un medio tecnológico, sea este hardwere o softwere no es considerado como delito; es por esto que se necesita establecer características para que se configure el delito de manera eficaz y adecuada. Por ello, el día 22 de octubre del 2012 se promulgó la ley N° 30096; y posteriormente su modificatoria la Ley N°30171, dentro de estas leyes se establecen los parámetros de delitos informáticos en Perú.

En suma, Los delitos informáticos están íntimamente vinculados con la idea de la comisión del delito mediante una computadora, internet, celular, Tablet, etc. Sin embargo, tienen la capacidad de ser el medio por el cual se cometan los ilícitos o como el fin de esta actividad ilegal (Villavicencio; p. 49; 2014). Es decir, los delitos informáticos son actividades antijurídicas que utilizan un equipo tecnológico para conseguir diversos fines; en todos los casos se busca afectar algún bien jurídico. Se debe resaltar que esta actividad ilícita se realiza en el ciberespacio (campo cibernético creado por la red o el internet mediante un equipo tecnológico).

1.2.1.1.Antecedentes

Para Gustavo Sain, los primeros delitos informáticos aparecen en los años 60, porque durante este periodo se había infundido cierto temor a la recolección y almacenamiento de los datos personales en las computadoras propias de la época, debido a la literatura propia de la época. Incluso, es Gustavo Sanin quien cita la obra “1984” de George Orwell, donde se narra la vida un Gran Hermano omnipresente que vigilaba y controlaba la vida de las personas a través del uso de tecnologías.

Además, durante estos años diferentes especialistas en informáticas intentaban arruinar la economía mediante el uso gratuito del servicio móvil, buscando perjudicar a los países involucrados en la guerra de Vietnam. También es Gustavo Sain quien afirma que durante el activismo político hippie de la época hubo un lado informático, porque durante este periodo se utilizaron las llamadas “blue box” o “cajas azules” donde participaban las Bell Corporation y la ATT, aquí se simulaba ser estas empresas para conseguir una comunicación de larga distancia. Estas técnicas fueron un precedente muy importante para desarrollar el hacking a un grado de sofisticación muy alto.

Durante 1990 que el internet sufre una expansión a nivel de todo el mundo, y con este crecimiento surge diversos métodos para recibir y enviar datos ilegales. Asimismo, en este periodo a nivel internacional, los gobiernos y estados comienzan a depender en gran medida a estos medios tecnológicos, utilizándola para guardar documentación secreta, documentos con información importante. Consecuentemente, todos estos gobiernos y estados se encontrarán susceptibles a la comisión de varios delitos informáticos, ya que la despreocupación por proteger estos datos era escasos y muy deficientes. igualmente, en este periodo la discusión respecto a la protección de la intimidad y la privacidad se comienza a hace más sonora a nivel global.

En el gobierno nacional, Villavicencio, comenta que la primera vez que se tipificó el Delito Informático en la legislación peruana estuvo plasmada en el artículo 186, inciso 3, segundo párrafo del código Penal de 1991. Sin embargo, afirma que esta no era parte de un delito autónomo, sino más bien como parte de un agravante del delito de hurto. Actualmente los delitos informáticos están previstos en el Capítulo X del Código Penal: los artículos 207-A (interferencia, acceso o copia ilícita contenida en base de datos), 207-B (alteración, daño o destrucción de base de datos), 207-C (circunstancias cualificantes agravantes), 207-D (tráfico ilegal de datos), y en las leyes penales especiales. Actualmente se cuenta con la Ley N° 30171, modificatoria de la Ley N° 30096, Ley de Delitos Informáticos.

1.2.1.2.Sujetos intervinientes

En toda ejecución punible del derecho penal siempre habrá un sujeto activo y otro pasivo, aunque dentro de estos sujetos pueden caber más de un agente pasivo o activo. Incluso, se habla de que pueden ser personas naturales o jurídicas. Para Acuario (2016), el elemento localizador que define la posición de los sujetos se elige entorno al bien jurídico vulnerado. Es decir, a quien se le vulnere el bien jurídico, será considerado como el sujeto pasivo; mientras que, el sujeto que afectó o lesionó el bien jurídico de la otra persona, esto a través de un tipo penal, será el sujeto activo.

1.2.1.2.1. Sujeto activo

Gonzales en su libro “Teoría del Delito” (2008); dice que al nombrar al sujeto activo del delito, se tiene en consideración que el hecho al ser una obra humana, siempre tiene un autor que ha realizado una acción prohibida y que se encuentra tipificada en el ordenamiento penal. Es decir, el sujeto activo es la persona natural o jurídica que tiene la capacidad y conoce que lo que está haciendo es una conducta antijurídica.

En el caso de los delitos informáticos, el sujeto activo no excluye lo anteriormente dicho, sino que agrega ciertas características que son importantes para la comisión del delito en el ciberespacio. Entre las características más importantes tenemos el de conocer el funcionamiento de las TIC, conocer del lenguaje informático y conocer el lugar estratégico donde recabar información.

1.2.1.2.2. Sujeto pasivo

En términos genéricos, este es el propietario o el titular del bien jurídico vulnerado o puesto en peligro. Para Acuario (p. 18; 2016), en los delitos informáticos propiamente dichos, la definición de sujeto pasivo puede recaer en un numero considerables de ciudadanos, además que pueden ser individuos, instituciones crediticias, gobiernos, instituciones públicas y/o privadas, etc.

1.2.1.3.Bienes jurídicos protegidos

Laura Mayer en la Revista Chilena de Derecho, dice que en el derecho penal es de gran relevancia el bien jurídico, pudiéndose afectar incluso los individuales (personas naturales) o colectivos (personas jurídicas). Asimismo, la misma afectación de un bien jurídico funciona como un fundamento más que adecuado para sancionar la conducta penal; además, determina penas proporcionales y el injusto específico de cada delito (2017; pp 2 -3).

Los bienes jurídicos protegidos por las leyes dependerán al modo operandi del ciberdelincuente, porque su afectación a los bienes jurídicos en los delitos informáticos tiene diversos de modos. Por un lado, cuando se habla de espionaje, podrá afectar derechos como la intimidad de los particulares, los secretos militares o nacionales, etc. Por otro lado, mediante el sabotaje el bien jurídico que se afecta recae sobre la condicional: “si lo que se destruye lo elimina tiene un valor económico”, ya que de este modo se estaría afectado la propiedad de la persona. Y, por último, el fraude informático tiene una afectación al bien patrimonial y a la modificación o secuestro de datos personales a través de programas autómatas que se encargan de recabar información y alterar datos en plataformas virtuales.

Entonces, los bienes jurídicos que se vulneran por medio de los delitos informáticos son muy abundantes y en algunos casos son hasta constitucionales. Pero, la afectación no solo puede recaer sobre las personas naturales, sino que estos delitos también pueden afectar a organizaciones internaciones, estados, naciones, organizaciones militares, entre otros. Es decir, los bienes jurídicos de los delitos informáticos tienen una influencia

bastante extensa, pudiendo vulnerar a civiles, estados completos y hasta organizaciones mundiales

1.2.1.4.Tipos de delitos informáticos

Hay una gran variedad de tipos de delitos informáticos, siendo una de sus características la complejidad con la que se puede detectar y corregir estos errores cibernéticos. Lourdes, M. incluso dice que es muy importante el implementar medidas de seguridad en los sistemas tecnológicos; además de una vigilancia continua a los servidores tecnológicos con los que contemos. Debido a la falta de esta última es que el derecho comparado ha clasificado los delitos a: las copias ilegales de los programas de cómputo, copia ilegal de topografía, las manipulaciones, el espionaje, el sabotaje y el hurto de tiempo. (s/n; pp 8 – 9).

Asimismo, Gonzales J.; Bermeo, J.; Villacreses, E; Guerrero, J. quienes citan a Lara, Martínez & Viollir, quienes categorizan los delitos informáticos en 5 puntos importantes: 1. El acceso no autorizado, 2. El daño a los datos o programas no autorizado, 3. El sabotaje informático, 4. La interceptación no autorizada, y 5. El espionaje informático. (2018; pp 182 -183). Sin embargo, los ilícitos señaladas por las Naciones Unidas son reducidos tres: fraude informático; Sabotaje informático y El espionaje informático; siendo la misma que en la mayoría de países latinoamericanos siguen y se estipulan en su norma penal.

1.2.2. El fraude informático

La RAE dice que el fraude informático es aquella acción contraria a la verdad y a la rectitud, perjudica a la persona a quien se le comete; afecta a muchas personas naturales y jurídicas a nivel mundial. Este delito tiene un antecedente de lo más conocido en el Código de Hammurabi; donde se sancionaba la venta de objetos robados y alteración de pesas y medidas. En la actualidad, la legislación comparada, no tiene una definición exacta de este tipo penal, la más certera es la que le da la doctrina española, definiéndola como un delito con modalidad de estafa, que recae en el engaño o estafa en un tercero, ocasionado un beneficio propio (s/n; s/n; p.4).

Josefina Garcia comenta que, es una de las tipologías del cibercrimen más comunes donde se busca transferir los activos patrimoniales a favor del autor del delito (2008; p. 292). Asimismo, Lourdes Delgado (2016; p. 9), dice que este delito consiste en manipular la informática, aprovechándose de las repeticiones automáticas propias de la tecnología. En algunos países como México, también se le llamada “técnica del salchichón”. Así se le llamó porque cuando existen bienes patrimoniales guardados en el internet, los criminales

proceden a robar estos bienes en cantidades apenas perceptibles para los titulares de estos, ocasionando que levante sospecha alguna del ilícito cometido y que el delincuente cumpla con su objetivo.

Entonces, el fraude informático cuenta con una conducta engañosa para con terceros, ocasionando que estos caigan en error, y obtengan una riqueza patrimonial a costas de los terceros.

1.2.2.1.Sujeto activo

Para Víctor Espinoza en su libro Delitos informáticos y nuevas modalidades delictivas, el sujeto activo puede ser cualquier persona natural con conocimientos básicos en informática, es decir, los posibles sujetos que este autor menciona son: gamers, trabajadores de entidades bancarias, operadores telefónicos, etc. (2022, p. 27). Esta definición no se aleja mucho a la de Josefina Garcia, quien agrega, estos sujetos también pueden ser aquellos legitimados para acceder a estos sistemas, siempre y cuando se manipule el medio tecnológico para un beneficio propio.

1.2.2.2.Sujeto pasivo

Víctor Espinoza (2022), menciona que toda persona natural o jurídica puede ser blanco de esta modalidad delictiva, más aún si cuenta con escasos conocimientos en informática, mayormente ancianos y niños (p. 97). Es decir, este sujeto es el propietario o titular del bien afectado.

1.2.2.3.En el derecho comparado

1.2.2.3.1. Alemania

Acuario, S. (2016) afirma que en Alemania la ley que sanciona hechos ilícitos relacionados con la informática comenzó desde el primero de agosto de 1986. Pero no fue hasta el 15 de mayo de 1986 en la que se promulgó la ley contra la Criminalidad Económica, los delitos que se estipulados fueron: el espionaje de datos; la estafa informática, la falsificación de datos probatorios y otros documentos que ayuden con el engaño en el tráfico jurídico, alteración de datos, sabotaje informático y la utilización abusiva de cheques o tarjetas de crédito.

Además, cuando se trata de introducir nuevos tipos penales dentro de su normativa penal, toma como base científica la reflexión y el análisis sobre aquellos delitos a los que la aplicación del delito penal tradicional no llegara fácilmente.

Para Gustavo Valmaceda (2011), la doctrina en este país utiliza como criterio restrictivo para que encaje en el tipo penal de fraude el de corresponder a un “engaño”

hacia otra persona, asemejándose a una estafa. Es decir, que el ilícito se llamaría como tal si existe un perjuicio directo con el patrimonio de la persona (p. 113).

1.2.2.3.2. Austria

La ley de reforma penal del veintidós de diciembre de 1987 contempla dos delitos como el de la destrucción de datos, delimitando los datos personales y el de los programas informáticos. Además, el de la Estafa informática.

1.2.2.3.3. Francia

Aquí se promulgó la Ley número 88-19 del cinco de enero de 1988 en la que habla sobre el Fraude Informático. En esta ley se establece los delitos como: el acceso Fraudulento a un sistema de elaboración de datos; el sabotaje informático; la destrucción de datos; la falsificación de documentos informatizados falsos (Acuario; 2016; p. 36).

1.2.2.3.4. Estados unidos

En este país se adoptó una postura más activa de los delitos informáticos con el Acta de Fraude y Abuso Computacional de 1986, la que se modificó con el acta Federal de Abuso computacional de 1994 (18 U.S.C. Sec. 1030). Fue en esta ley que se estableció como delitos: todos lo que utilizan virus y a raíz de esto ocasionan pérdidas materiales del tercero. Asimismo, la preocupación de este país por tratar de controlar los delitos que se relacionan a estos tipos de malware que dañan el equipo tecnológico ha sido primordial y su foco de actuación frente a los delitos informáticos. (Acuario, 2016, pp. 37 – 38)

1.2.2.3.5. Chile

En 1993, se promulgó la ley N° 19 223, la que establece los parámetros taxativos que se deben tener en cuenta al momento de indicar que una actividad debe ser considerada como una conducta típica. En esta legislación, los principales delitos que se toma en consideración son: el sabotaje informático, el espionaje informático y el daño de hardware. Sin embargo, estos delitos son previstos de una manera general y limitada. (Acuario; 2016; pp. 39 – 38)

1.2.3. Phishing

Mayra Mariana cita a Jerry Félix y Chris Hauck, quienes durante una conferencia de 1987 se hizo referencia al termino en un documento “Sistema de seguridad: La perspectiva de un Hacker”. Sin embargo, no fue hasta que la compañía AOL utilizó este término como tal. Incluso, fue antes de 1995 que varios “hackers” comenzaron a utilizar números de tarjetas falsas, duplicados de las mismas y a piratear software, esto significó una gran pérdida para la empresa AOL. Por esta razón, fue la misma empresa que creó la AOHell que se encarga de hacer frente a estas estafas (2021, p. 9).

El Phishing es utilizado para indicar un engaño hecho a un usuario para obtener algún tipo de beneficio personal o financiero; también es utilizado para suplantar la identidad digital de otra persona y así obtener algún beneficio. Siendo este uno de los más sencillos y comunes ciberataques cometidos por los ciberdelincuentes (Jefatura de Gabinete de ministros Argentina, 2021, p. 1)

Existen muchas formas de phishing que son utilizada en el Internet, sus modalidades son muy variadas y el modo operandi es muy abundante. Según Mayra Mariana, actualmente la forma más utilizada del Phishing es de mediante el envío masivo de correos electrónicos, esto con la finalidad de apropiarse de los datos personales y patrimoniales de internautas incautos (2021, p. 10).

El phishing como bien se ha mencionado, busca vulnerar la privacidad, busca expropiarse de bienes patrimoniales ajenos y suplantar a terceros utilizando un medio tecnológico, buscando siempre un beneficio propio, incluso si eso significa perjudicar a terceros.

1.2.3.1.Fases del phishing

Al existir una constante evolución del phishing, son varios los estudios que demuestran la existencia de múltiples etapas en la comisión del delito del phishing. Pero debemos considerar que las mismas pueden variar dependiendo de la modalidad, la dificultad, la complejidad, el nivel de conocimiento del "phisher" y la participación de la víctima. Es por ello que Mayra Mariana distingue seis fases:

1.2.3.1.1. Planificación

Esta etapa se caracteriza principalmente por la preparación del ataque por parte del ciberdelincuente, es durante esta etapa que se decidirá por: quien será la víctima, la modalidad, el tipo de phishing que irá a realizar, el número de víctimas y el de ciberdelincuentes, si se va realizar a una persona natural o a una persona jurídica, etc. (Mariana, 2021, pp. 15 – 16). Es decir, esta etapa está comprendida Fase interna del Inter Crimines, es aquí donde el criminal delibera si va a cometer el delito y la estrategia que trazará para cometer su maquiavélico plan.

1.2.3.1.2. Preparación

Mariana comenta que dentro de esta etapa la existencia de la participación es insignificante. Porque en esta etapa el ciberdelincuente se preocupa por la finalidad por el que comete el ilícito, los medios que va a emplear y los mecanismos que serán útiles. Un ejemplo de esto es la diferentes en la forma que pueden existir dentro de un correo que es particular o colectivo. Explicado de una mejor manera, si se trata de un correo para

engañar a alguien particular, este será muy personal, más preparado y personalizado. Si, por lo contrario, es colectivo, este tendrá que ser más común y genérico (2021, p. 16). Esta fase forma parte de los Actos Preparatorios; porque lo actos son anteriores a la ejecución del delito. Durante este proceso existe un insuficiente contenido delictivo

1.2.3.1.3. Ataque

En esta etapa, los ciberdelincuentes se encargan de enviar todo tipo de phishing mediante los medios tecnológicos pertinente a su plan. Aquí juega un importante papel la influencia de la víctima con su participación, sea esta baja, media o alta. Y cada una tendrá un nivel distinto de complejidad. Inclusive, Mariana (2021) dice que durante esta etapa se conoce con bastante énfasis la "anatomía del phishing"; aquí podemos discernir siete elementos esenciales: el malware en sí, la infección, la ejecución, la entrada de datos, el atacante y el servidor legítimo. Asimismo, se debe tener en cuenta la existencia dos fases de infección transcendentales: cuando el equipo tecnológico se infecta y cuando el código tecnológico malicioso es ejecutado (p. 17). Esta etapa ya es considerada como tentativa, ya que el agente ya inició con la ejecución del delito.

1.2.3.1.4. Recogida de datos

Durante esta etapa el delincuente espera que el programa malicioso comience a recolectar datos personas e información relevante para hacer de los bienes patrimoniales de las víctimas. El tiempo va a depender muchas veces del nivel de participación de las victimas; es decir, si el nivel de participación baja el tiempo que se requerirá será más corto; si el nivel es medio el tiempo que se emplee será más extenso, y si el nivel es alto, el tiempo que se necesite será aún más amplio. Este periodo es considerado como la consumación, ya que es durante este periodo que el agente alcanza el objetivo que estuvo planeando

1.2.3.1.5. Ejecución

Etapa en la que el pisher ya tiene los datos de las víctimas, durante esta etapa el delincuente decide si toda la información que posee es utilizada en beneficio propio o es vendida a otras personas para que sean estas las cometan los ilícitos penales. En esta fase, el agente obtiene compensar el propósito que perseguía.

1.2.3.1.6. Post-ataque

Cuando se ha logrado el objetivo primordial del phisher, sigue el borrado de todo rastro que sea utilizado para inculpar al delincuente.

1.2.4. Clasificación

1.2.4.1.Vishing

Este término proviene del “voice phishing”; esta modalidad intenta convencer a su víctima por medio de llamada telefónica, esta puede ser mediante celular o el teléfono, en esta se busca la recolección de datos por medio del habla y de la oralización. Según la “Dirección Nacional de Ciberseguridad”, en este tipo de phishing, el phisher afirma formar parte de la alguna empresa pública o privada, con esta supuesta suplantación se busca conseguir datos de los terceros (2021, p. 2).

Además, Víctor Espinoza (2022) comenta que bajo esta modalidad el derecho penal clásico lo reconoce como un delito de suplantación de identidad y fraude informático (p. 122)

1.2.4.2.Smishing

Para Víctor Espinoza estos delitos consisten en enviar los enlaces maliciosos por medio de mensajes de texto, SMS o cualquier servicio de mensajería (2022; p. 121). La línea que sigue esta modalidad inicia con la victima recibiendo un mensaje con la indicación de abrir cierto enlace o el de descargar cierta aplicación, para, finalmente conseguir el fin ilícito perseguido por el phisher. (Dirección Nacional de Ciberseguridad; 2021, p. 3).

1.2.4.3.Pharming

Regulada en la Ley N° 30096, en su art. 10 y art. 8 respectivamente; delito de abuso de mecanismo y fraude informático. En esta modalidad se busca crear paginas webs de entidades bancarias u otros con el objetivo de hacerse con las cuentas bancarias de las víctimas.

1.2.4.4.Skimming

Esta consiste en duplicar por medios tecnológicos las tarjetas bancarias para apoderarse de los datos necesarios de usuarios para que se pueda cometer el ilícito (Espinoza; 2022; p. 122).

II. Materiales y métodos

El tipo de investigación que se utilizó fue la aplicada, ya que buscó analizar mediante un análisis escrupuloso la realidad que enfrentan los tipos penales del fraude informático en la sociedad. Además, la pobre explicación que existe en la ley de delitos informáticos (Ley N° 30096 y Ley N° 30171), significó un atraso al momento de sancionar la acción ilícita por parte de los ciberdelincuentes.

Asimismo, la investigación trató de brindar una solución al problema que se planteó, se basó siempre en la consolidación y búsqueda del conocimiento y la ciencia para su adecuada

aplicación en el mundo real; siendo la idea de fondo la utilidad con la que se estructuró el conocimiento, logrando así ciertas soluciones al problema.

El otro tipo de investigación que se siguió, fue la documental, porque la investigación se situó en buscar la modificatoria más acertada que se pudo plasmar en las Leyes de Delitos informáticos. Además, se dispuso de varias fuentes bibliográficas para un posterior análisis y reflexión teórica, de esta manera se construyó y se adquirió conocimientos del tema; siendo esta una base fundamental para que parta la investigación.

El método analítico que se empleó fue el analítico, pues, se examinó la teoría más acorde con los fines que se buscó. Incluso, se realizaron dos fichas del estado del arte a fin de organizar las fuentes que se usaron y ayudaron a sistematizar la organización de la bibliografía que se consiguió, la mayoría de estas fuentes fueron actuales y se apoyaron en artículos nacionales e internaciones, libros digitales, jurisprudencia, leyes, artículos científicos, etc.

Cabe resaltar, la búsqueda de fuentes bibliográficas referentes al tema investigado dio como resultado un abundante material electrónico, libros en físico, revistas nacionales, extranjeras y tesis. Inclusive, estas fuentes tuvieron un estrecho vínculo con los delitos informáticos, derecho penal y el fraude informático. Al mismo tiempo, las recomendaciones hechas por la comunidad internacional fueron ser importantes, porque brindaron varias soluciones al problema planteado en la presente investigación.

III. Resultados y discusión

Este apartado se desarrollará en función a los objetivos específicos planteados. De modo que, se harán conocer fuentes bibliográficas como aquellas consignadas en el Marco Teórico, esto con el fin de defender nuestro análisis y aporte obtenido del objetivo general. Buscando las razones para incorporar el Phishing en el artículo 8 de la ley de delitos informáticos.

3.1.Análisis del phishing como tipo penal en el derecho penal peruano y extranjero.

El primer acápite tendrá por finalidad buscar una respuesta ante el planteamiento de nuestro primer objetivo específico, teniendo en consideración al phishing y al fraude informático como figuras protagonistas. Ambos tipos penales serán comparados en un ámbito nacional e internacional, teniendo en cuenta las legislaciones de: Alemania, España y Estados unidos, Chile, Argentina, Ecuador y Brasil.

3.1.1. Tratamiento del Phishing en la legislación comparada

En el desarrollo de este punto, se analizó la legislación internacional y su legislación del fraude y el phishing, entre ellas se consideró las legislaciones de: Alemania, España, Estados Unidas, Chile, Argentina, Brasil y Ecuador; además de algunos tratados internacionales.

Durante 1983, se crea la Organización de Cooperación y Desarrollo Económico (OCDE), y con esta nace el estudio para hacer frente a la mala praxis de las computadoras u otros medios tecnológicos. En pocas palabras, esta fue los primeros reglamentos internacionales que trata de proteger a los usuarios de las computadoras u otros medos tecnológicos de ese entonces. Posteriormente, en 1986, se publicó un informe titulado "delitos informáticos: análisis de la norma jurídica", este describía las normas legislativas vigentes y las propuestas de reformas en varios estados miembros de la OCDE. Además, fue en este informe donde se limitó y enumeró los tipos de delitos que deberían ser sancionados, entre ellos estaba el fraude informático y el phishing. (Acuario, 2016; p. 30).

Luego, el 01 de julio del 2004, se pone en vigor el Convenio de Budapest, con 30 estados miembros. Satzager define al Convenio de Budapest como aquella que lucha contra la cibercriminalidad, misma que al ser un tratado multilateral de derecho público, esta rige en los países miembros (p.13; 2017). Actualmente, este convenio cuenta con 87 países miembros. Asimismo, el Perú se adhirió el 13 de febrero del 2019 a este convenio Internacional mediante Resolución Legislativa N° 30913.

Ahora bien, en diversos países se han promulgado leyes que tipifican el delito como tal, mientras que, en muchas otras a duras penas dan con la definición y embarcan parte del enfoque que se da hoy en día.

3.1.1.1.Europa y Estados Unidos

ALEMANIA	ESPAÑA	ESTADOS UNIDOS
Las políticas contra los delitos informáticos se adoptaron el 15 de mayo de 1986 con la Segunda Ley contra la criminalidad económica. Misma en la que se contempla al artículo 263, donde se suscribe el delito de Estafa por computador, norma penal que se acerca mucho al tipo penal del phishing.	El delito del phishing en España se promulgo el 22 de diciembre en la Ley de Orgánica 14/2022. Anteriormente, no se podía probar el delito y se encuadraba en la estafa general; aunque esto muchas veces resultaba una vulneración al principio de legalidad. En la directiva 2019/713 se planteó castigar los actos preparatorios destinados a la ejecución del delito de estafa informática. Ahora bien, en la legislación española existen abundante jurisprudencia respecto al tema.	Estados Unidos pertenece a la tradición de COMMON LAW; y de esto parte la riqueza argumental, legislativa y jurisprudencial. Es la única legislación que ha sido estudiada y en la que se ha encontrado definiciones explicitas y técnicas de varios tipos penales informáticos, entre ellos el phishing y sus muchas variantes.

263A. ESTAFA POR COMPUTADOR (1) Quien, con el propósito, de procurarse para sí o para un tercero una ventaja patrimonial antijurídica, en la medida en que él perjudique el patrimonio de otro, por una estructuración incorrecta del programa, por la utilización de datos incorrectos o incompletos, por el empleo no autorizado de datos, o de otra manera por medio de la influencia no autorizada en el desarrollo del proceso, será castigado con pena privativa de la libertad hasta cinco años o con multa.	Inciso a) del Art. 249.1. «a) Los que, con ánimo de lucro, obstaculizando o interfiriendo indebidamente en el funcionamiento de un sistema de información o introduciendo, alterando, borrando, transmitiendo o suprimiendo indebidamente datos informáticos o valiéndose de cualquier otra manipulación informática o artificio semejante, consigan una transferencia no consentida de cualquier activo patrimonial en perjuicio de otro».	1030 - FRAUDE Y ACTIVIDAD RELACIONADA EN RELACIÓN CON COMPUTADORAS: 1. Quien habiendo accedido a sabiendas a un computadora sin autorización o exceder el acceso autorizado, y por medio de dicha conducta haber obtenido información que ha sido determinada por United Estados Gobierno de conformidad con una orden o estatuto ejecutivo para exigir protección contra la divulgación no autorizada por razones de defensa nacional o relaciones exteriores, o cualquier dato restringido, como se define en el párrafo y. de la sección 11 de la Ley de Energía Atómica de 1954, con razones para creer que dicha información así obtenida podría usarse para la lesión de United Estates, o en beneficio de cualquier nación extranjera, deliberadamente comunica, entrega, transmite o hace que se comuniquen, entreguen o transmitan, o intente comunicarse, entregar, transmitir o hacer que se comunique, entregue o transmita lo mismo a cualquier persona no tiene derecho a recibirlo, o deliberadamente retiene lo mismo y no lo entrega al funcionario o empleado de United estates con derecho a recibirlo; 2. Accede intencionalmente a computadora sin autorización o excede el acceso autorizado, y, por lo tanto, obtiene: a) Información contenida en un registro financiero de una institución financiera, o de un emisor de tarjeta (…). b) Información de cualquier departamento o agencia de United Estados; o C) Información de cualquier computadora protegida; (…) 4) A sabiendas y con la intención de defraudar, accede a una computadora protegida sin autorización, o excede el acceso autorizado, y por medio de dicha conducta promueve el fraude previsto y obtiene algo de valor, a menos que el objeto del fraude y la cosa obtenida consistan solo en el uso de la computadora y el valor de dicho uso no es superior a $ 5,000 en un período de 1 año; (…)

Respecto al análisis realizado a la legislación española, esta brinda un tratamiento poco específico de los delitos informáticos. Además, es conocido que el principal problema en esta legislación es el desconocimiento de la población respecto a los delitos informáticos, problema que no es ajeno a ningún país, ni sociedad en el mundo; porque las diversas entidades bancarias y empresas en general cuentan con abundantes datos personales de sus usuarios y clientes, esto hace que estos últimos sean los más afectados sean los más afectados, cuando violan las defensas cibernéticas de las empresas en general. Sin embargo, se debe destacar la reforma que España ha ido realizando a lo largo del tiempo, y los avances positivos que se ha logrado conseguir con las mismas. En ese sentido, en el Código Penal español, la figura del fraude informático se subdivide en múltiples conductas típicas, todas estas se abocan a sancionar la conducta que cause un perjuicio económico a un tercero a través de medios informáticos.

En el artículo 248.2 del instrumento normativo español, se ha regulado la figura de la estafa informática o phishing, aquí se establece la denominación “phisher” al sujeto activo que comete fraude mediante un medio tecnológico para sacar provecho de un bien módico u otro bien materializado por la red digital.

Ahora bien, de las legislaciones estudiadas, se inquiere que el bien jurídico protegido es el patrimonio; asimismo, tal y como refiere Santos (2021) el “ánimo de lucro”, debe ocurrir en el momento de la acción, no se prolonga en el tiempo después de consumarse el delito (p. 37). Es decir, el objetivo del sujeto activo es hacerse de los bienes patrimoniales del sujeto pasivo, todo esto en una misma acción. Sin embargo, al cerrase en esta idea, deducimos que el phishing en la doctrina tiende a ser calificado como un delito conclusivo. En cuanto a la estructura típica esta se caracteriza por la disposición patrimonial a través de la manipulación informática, o al hacer que el sujeto pasivo caiga en error al brindar enlaces falsos mediante mensaje de texto, mensaje de voz o llamada telefónica, u otras aplicaciones que facilitan el contacto con otras personas mediante un medio tecnológico.

Para diferenciar la estafa, propiamente dicha, del phishing, se debe tener en cuenta el modo operandi para engañar al sujeto pasivo o a los terceros involucrados, es decir, cuando se habla de una estafa, estamos hablando de un contacto directo con la persona; mientras que, cuando se habla del phishing, el sujeto activo utiliza los medios tecnológicos como un medio para conseguir los bienes patrimoniales. Además, no se puede dejar de lado al avance tecnológico, con esto los múltiples mecanismos que se han ido agregando y evolucionando con la

tecnología a fin de que el phisher logre el objetivo de la manipulación informática para la consumación del delito. En ese sentido, estamos tratando con un delito de resultado.

Además, en la presente norma el legislador español hace mención a "programas informáticos" y hace un hincapié en que el sujeto activo puede ser cualquier persona que haya fabricado un programa informático con el fin de defraudar al sujeto pasivo; o, haya introducido programas informáticos en el mercado negro con el fin de otorgar herramientas al phisher y se le facilite la comisión de una estafa informática. Incluso, se pretende incluir en el delito de phishing, el uso de medios electrónicos de pago, tales como la tarjeta de crédito, débito o cheques de viajes como objeto material para perjudicar el patrimonio del sujeto pasivo, esto es, retirar dinero sin consentimiento.

Con relación al Estado de Alemán, el ámbito teórico tiene una legislación poco escrupulosa en relación con los Delitos Informáticos. Sin embargo, las instituciones gubernamentales están bien informadas respecto a las mismas, es por ello que el Gobierno Federal, como se puede ver en su página web oficial, tiene cuatro áreas de acción: i. Orden conjunta de ciberseguridad del Estado y las Empresas; ii) acción segura y auto determinativa en un entorno digitalizado; iii) posicionamiento activo de Alemania en la política de ciberseguridad en Europa y el mundo; y, iv) potente y sostenible arquitectura de seguridad cibernética en todo el estado.

Asimismo, el estatuto alemán tiene una normativa de los Delitos Informáticos muy actualizada, porque cuenta con la Segunda Ley que establece medidas contra la ciberdelincuencia promulgada el 15 de mayo 1986, y cuya actualización se publicó el 23/12/2022. Así pues, en temas prácticos, Alemania es uno de los primeros países en tratar y capacitar a sus agentes policiales; incluso, su estructura está dirigida a proteger a los ciudadanos de estos tipos de delitos. Está conformada por la Policía de los Estados Federados (LKA), la Policía Criminal de Alemania (BKA)y la Policía Federal, aunque esta última no tiene competencia en toda Alemania.

Para Acuario (2016), los delitos informáticos en Alemania son un problema muy difícil de combatir, porque están en constante desarrollo. Por lo tanto, establecer nuevos conceptos y agregarlos al Derecho Penal Tradicional es complicado, ya que requiere de un arduo análisis para que no se creen normas sin sentido.

Ahora bien, de la inspección a la norma de Estados unidos, se entiende que es el país que está a la vanguardia en tema de delitos informáticos, su legislación abarca la mayoría de problemas relacionados a la ciberdelincuencia y, especialmente, trata de proteger la

privacidad de los individuos y todo tipo de negocios y agencias gubernamentales y privadas. Incluso, su legislación habla de varios supuestos en este tipo de delitos.

Ahora bien, se debe tener en cuenta que la tradición jurídica estadounidense es el common law, lo que quiere decir que aparte de tener las reglas emanadas De las leyes en sentido estricto, también existen normas jurídicas que se emanan del derecho consuetudinario.

En 1992, el estado de California adoptó la Ley de Privacidad, aquí se establecieron los delitos a la intimidad; y, cuyas sanciones son pecuniarias, parten desde $10 000 por cada una de las personas afectadas, hasta $ 50 000 por el acceso imprudencial a una base de datos. Acuario apunta que para esta norma se realizaron enmiendas, teniendo como principal objetivo el de aumentar la protección a las personas naturales y jurídicas (p.37; 2016). Posteriormente, en 1994 se adoptó el Acta Federal del Abuso Computacional, mediante el cual se modifica el Acta de Fraude y Abuso computacional de 1986; con la finalidad de actualizar el concepto de términos técnicos.

Sin embargo, algo que se debe mencionar, es el término que hace referencia su ley penal, el "ordenadores protegidos" (protected computers), término que abarca mucho, desde un ordenador utilizado por una Persona Jurídica pública y privada, así como personas naturales; básicamente, cualquier tipo de ordenador conectado a internet.

3.1.1.2.Sudamérica

CHILE	ARGENTINA	PARAGUAY	BRASIL	COLOMBIA
La reforma de los delitos informáticos en chile se dio con la Ley N° 21 459 promulgada en diciembre del 2022, con esta ley se derogó la Ley N° 19223. Lo importante de este cuerpo normativo es que permite sancionar la tentativa y la frustración de los delitos que se contemplan en esta ley.	La ley N° 26 388 se promulgó durante junio de 2008; la presente ley modifica e incorpora figuras típicas del derecho penal buscando regular la comisión de delitos mediante medios tecnológicos.	en Paraguay existe la Unidad Especializada de Delitos Informáticos, unidad que fue creada para combatir los hechos punibles cometidos mediante la tecnología. Esta unidad actúa mediante Resoluciones N° 4408/11 y 3459/10.	La legislación de delitos informáticos es la Ley N° 12737, esta ley es considerada insuficiente para disuadir a los delincuentes. Cabe indicar, la acción penal es iniciada por la persona natural o jurídica vulnerada. La Oficina para la Represión de la Delincuencia Cibernética de la Policía Federal es la principal entidad encargada de investigar los delitos cibernéticos y cuenta con un laboratorio forense digital.	En el 2009 se promulgó la Ley N° 1273, ley que establece varios delitos informáticos como tipos penales.
LEY NÚMERO 21.459 Artículo 7°. - Fraude informático. El que, causando perjuicio a otro, con la finalidad de obtener un beneficio económico para sí o para un tercero, manipule un sistema informático, mediante la introducción, alteración, daño o supresión de datos informáticos o a través de cualquier interferencia en el	**LEY 26 388** (QUE MODIFICA AL CÓDIGO PENAL ARGENTINO) ARTICULO 9º — Incorporase 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	**CÓDIGO PENAL PARAGUAYO** Artículo N° 188 - Operaciones fraudulentas por computadora 1º El que con la intención de obtener para sí o para otro un beneficio patrimonial indebido, influyera sobre el resultado de un procesamiento de datos mediante: 1. programación falsa;	**CÓDIGO PENAL BRASILEÑO** Arte. 154- INVASIÓN DE DISPOSITIVO INFORMÁTICO: A. Invadir el dispositivo informático de otra persona, conectado o no a los equipos de la red, mediante la violación indebida de un mecanismo de seguridad y con el fin de obtener, manipular o destruir datos o información sin la autorización expresa o	**LEY 1273 DEL 2009, LEGISLACIÓN COLOMBIANA** Artículo 269G. SUPLANTACIÓN DE SITIOS WEB PARA CAPTURAR DATOS PERSONALES. El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas

funcionamiento de un sistema informático, será penado: 1) Con presidio menor en sus grados medio a máximo y multa de once a quince unidades tributarias mensuales, si el valor del perjuicio excediera de cuarenta unidades tributarias mensuales. 2) Con presidio menor en su grado medio y multa de seis a diez unidades tributarias mensuales, si el valor del perjuicio excediere de cuatro unidades tributarias mensuales y no pasare de cuarenta unidades tributarias mensuales. 3) Con presidio menor en su grado mínimo y multa de cinco a diez unidades tributarias mensuales, si el valor del perjuicio no excediere de cuatro unidades tributarias mensuales. Si el valor del perjuicio excediere de cuatrocientas unidades tributarias mensuales, se aplicará la pena de presidio menor en su grado máximo y multa de veintiuna a treinta unidades tributarias mensuales. Para los efectos de este artículo se considerará también autor al que, conociendo o no pudiendo menos que conocer la ilicitud de la conducta descrita en el inciso primero, facilita los medios con que se comete el delito.	altere el normal funcionamiento de un sistema informático o la transmisión de datos.	2. utilización de datos falsos o incompletos; 3. utilización indebida de datos; o 4. otras influencias indebidas sobre el procesamiento, y con ello, perjudicará el patrimonio de otro, será castigado con pena privativa de libertad de hasta cinco años o con multa. 2º En estos casos, se aplicará también lo dispuesto en el artículo 187, incisos 2º al 4º.	tácita del titular del dispositivo o instalar vulnerabilidades para el uso ilícito. ventaja: Pena de prisión preventiva, de 3 (tres) meses a 1 (un) año, y multa. § 1º La misma pena se aplica a quien produzca, ofrezca, distribuya, venda o difunda un dispositivo o programa informático con el fin de permitir la práctica de las conductas definidas en el caput. § 2 La pena se aumenta de un sexto a un tercio si la invasión produce daños económicos. § 3 Si la invasión tiene como resultado la obtención del contenido de las comunicaciones electrónicas, intimidad, secretos comerciales o industriales, información confidencial, en los términos de la ley, o control remoto no autorizado del dispositivo invadido: Pena - reclusión, de 6 (seis) meses a 2 (dos) años, y multa, si la conducta no constituye un delito más grave. § 4º En el caso del § 3, la pena es aumentada de uno a dos tercios si hay divulgación, comercialización o transmisión a tercero, por cualquier motivo, de los datos o informaciones obtenidas. § 5º Se aumenta la pena de un tercio a la mitad si el delito se comete contra: 1-	emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave. En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave. la pena señalada en los dos incisos anteriores se agravará de una tercera parte a la mitad, si para consumarlo el agente ha reclutado víctimas en la cadena del delito.

			presidente de la República, gobernadores y alcaldes: El presidente del Supremo Tribunal Federal, presidente de la Cámara de Diputados, del Senado Federal, de la Asamblea Legislativa del Estado, de la Cámara Legislativa del Distrito Federal o de la Cámara Municipal o	

Entonces, las legislaciones sudamericanas tienden a estar desactualizada, o son limitan a sancionar acciones antijuridicas demasiado genéricas. Sin embargo, de los procesos que se han mencionado anteriormente, la legislación que es más completa es la Ley Penal de Paraguay, porque su legislación brinda las herramientas necesarias para abatir los delitos informáticos en la práctica. Es decir, su legislación no solo se aboca al elemento teórico, sino que también brinda un soporte en el ámbito práctico. Roibon, M. (s.f.), dice que actualmente en los países en vías de desarrollo son el principal objetivo de los delincuentes cibernéticos, porque el avance tecnológico supone un enorme desafío para estos países. (p. 11). Incluso Temperini, M. (2014), publicó un estudio donde resalta el porcentaje de la sanción realizas de ciertos países en temas de delitos informáticos. En el que se concluye que el 81% de países tienen un nivel de regulación muy precario en estos temas (p. 137)

3.1.2. El phishing en la normativa peruana

En el Perú está la Ley N° 30096, ley que incorpora a los Delitos informáticos como acciones punibles del derecho, entró en vigencia el 21 de octubre del 2013. Posteriormente, se promulgó la ley N° 30171, esta modifica la a la Ley N° 300096, y la que modifica varios de artículos en mencionada ley. Ahora bien, el Perú mediante Resolución Legislativa N° 30913, publicada el 13 de febrero del 2019, incorporándose asi en el Tratado de Budapest. Este tratado sanciona y prohíbe acciones ilegales que utilizan algún aparato tecnológico como medio o como la finalidad de la comisión de un delito; es decir, acciones como: el acceso ilícito en todo o parte del sistema informático, el compartir archivos dañados y por consecuencia dañar el equipo del destinatario, y, por último; todas las herramientas digitales o aplicativos que se pueden emplear para el hacking. (Satzger, H; s/n; p.)

Sin embargo, la legislación peruana sigue estando demasiado atrás, y fue promulgada antes que EL Perú firme el tratado de Budapest, mostrando de esta manera lo arcaica de la norma con respecto a nuestro contexto histórico actual. Por ello, Vinelli (2021, p. 97), mediante datos recabados por el Banco Central de Reserva indica que las operaciones interbancarias por una red digital tienen un 18 % más que años anteriores. Es decir, Perú no cuenta actualmente con las condiciones para hacer frente a delitos informáticos, esto debido a la legislación arcaica y poco específica.

Ahora bien, las jurisprudencias de estos casos son pocas, debido a que o no encajan en ningún tipo penal de la Ley de Delitos informáticos y se tiene que utilizar otras normas penales que encajen mejor y ayuden al Fiscal en su teoría del caso, o simplemente sea declarada improcedente porque el delito no se concretó. La sentencia 1100/2020, en la que el TC declara infundada la demanda de habeas corpus, que condena a Marcos Morales Varga,

por cometer delitos como el fraude informático y la falsificación de firmas en documentos privados. Esta sentencia aporta la rapidez con que la Corte Superior de Justicia de Lima aplicó las agravantes. Teniendo en cuenta el periodo de desarrollo del delito con la manipulación de contraseñas sobre las cuentas bancarias de los usuarios. (Castro, R,2022; p. 20).

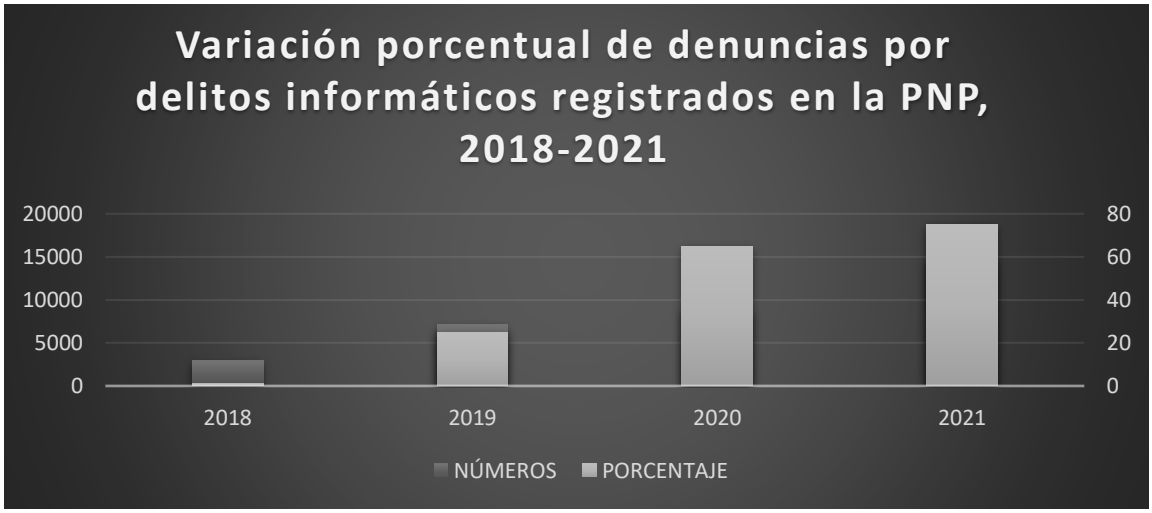
3.2. Cimentar en la doctrina las razones por las cuales el phishing debe ser considerado como tipo penal

El segundo punto tendrá por finalidad brindar una respuesta ante el planteamiento de nuestro segundo objetivo específico, esto es, las causas por las que se debe incluir el phishing tácitamente en la Ley de Delitos Informáticos, Ley 30096.

3.2.1. Aumento de los delitos informáticos durante las últimas décadas

El aumento de los delitos informáticos es muy creciente, como lo indican los boletines del Ministerio Público, solamente el 2018 se registraron 3851 delitos informáticos, en el 2019, dio un salto adicionándose 2641 casos a la cifra registrada en el 2018 (Garrido, K., 2021; p. 46). Ahora bien, Quijano, A. (2020) confirma que entre los periodos correspondientes al 2018 y 2020, tiempo en que el Perú se adhirió al Convenio de Budapest, el nivel de incidencias de los delitos informáticos aumentó drásticamente (p. 34). Asimismo, el Ministerio de Justicia y Derechos Públicos en el libro titulado “ciberdelincuencia reporte de información estadística y recomendaciones para la prevención”, muestra una base estadística apoyada en las denuncias hechas en el Ministerio Publico y los registros de la Policía Nacional del Perú, con el siguiente gráfico:

Tabla 1



Nota. 1 "Ciberdelincuencia, reporte de información estadística y recomendación para la prevención", Flores, C.; Rodríguez, T; et all. (2022). Observatorio Nacional de Política Criminal. p. 10. Recuperado de https://cdn.www.gob.pe/uploads/document/file/3562747/Rep

Además, el Diario “El Peruano”, en una publicación del 04 de setiembre del 2022, dio a conocer datos estadísticos con el título de “Denuncias por delitos informáticos se incrementaron en más del 90% en el Perú”, aquí se estableció que, durante el 2021, el Ministerio Publico recibió 18mil 596 denuncias de casos de cibercrimen, esto equivale a un aumento de porcentual del 92 % en comparación al año 2020. Por otra parte, la PNP registró 14 mil 671 denuncias por delitos informáticos durante el año 2021. Lo que significa que hubo un aumento del 65% en comparación del año 2020 y años anteriores a este.

Sin embargo, Quijano, A. (2020), cita a la Rodríguez, quien en el 2020 señaló que existen capacitaciones que son completas, pero estas no llegan a todos los agentes de justicia. Indicando; además, que existe una necesidad de publicidad para con estos temas. Asu vez, la necesidad de que se cuente con un presupuesto para la compra de instrumentos tecnológicos para hacer frente a la ciberdelincuencia (p. 51).

Entonces, los delitos informáticos tienen un mayor número de incidencias por cada año transcurrido, significando que el grado de evolución es progresivo, pero el nivel de las denuncias indica que los pobladores se informan más, contribuyendo a que estos tipos de delitos son más conocidos.

3.2.2. Vulneración al principio de legalidad:

Ahora bien, En el derecho penal, uno de los principios fundamentales es el principio de legalidad, este principio consiste en dar la primacía de la ley sobre cualquier actividad o función del poder público. Cristobal, T. menciona que el principio de legalidad escoge a la ley como configuradora del derecho penal, pues esta tiene como objeto la creación de delitos y penas (p. 264). Este principio condiciona al legislador a crear leyes entendibles y con una redacción precisa; mismas condiciones que la Ley 30096 y su modificatoria (Ley 30171) no cuentan. Cabe mencionar que en la legislación del artículo que cree conveniente incorporar el tipo penal del phishing, cuenta con 8 verbos rectores (mismos que se muestran más adelante).

Respecto a esto, Terreros, M. en la tesis de Hidalgo, C. y Solano, S.; dice que el artículo 8 de la Ley antes mencionada, se presenta al fraude como delito de resultado; es decir, no basta con cumplir con el tipo penal para que se consuma el delito, más bien, necesita que se perciba resultados (que cause perjuicio a un tercero) (pp. 62-63). En pocas palabras, la ley al tener muchos verbos rectores, hace que la ley no cumpla con su función rectora. Es por ello que, en muchas ocasiones, se deba recurrir a otras normas penales para poder sancionar a estos cibercriminales.

3.3. Incorporación del phishing como modalidad en el artículo 8 de la ley de delitos informáticos

En este capítulo, el objetivo que se busca es el de dar una respuesta al planteamiento de nuestro objetivo general. Asimismo, se intenta explicar las razones por las que se debe incorporar el PHISHING en la Ley de Delitos informáticos.

Como bien se ha establecido en puntos anteriores, los delitos informáticos previstos en el cuerpo normativo peruano se encuentran desactualizado, y esto permite que los delincuentes cibernéticos tengan un gran campo de acción ilícita.

La propuesta sugerida es la siguiente:

LEY 30096	LEY 30171	MODIFICATORIA SUGERIDA
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 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."	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. 8.1. **El que** mediante la **remisión o el envío** de uno o más correos electrónicos, mensajes de texto, mensajes de voz, o utilice cualquier otro medio tecnológico buscando defraudar patrimonialmente y/o sustraer información privada de una persona natural o jurídica. Será

		sancionado con pena privativa de libertad no menor de cuatro años y no mayor de seis. 8.2. La pena no será menor de 7 años ni mayor de 10 años: a. Cuando el monto robado supere el 30% de una UIT. b. Cuando el robo sea perpetrado a los bonos de ayuda social otorgados por el estado o cualquier órgano perteneciente a este. c. Cuando el agente actúe en calidad de miembro de una organizan criminal.

Conclusiones

1. El phishing tiene un nivel de incidencia muy alto en la legislación nacional e internacional debido al avance tecnológico. Ahora bien, a nivel internacional, en países como España, Chile, Argentina, Paraguay, Alemania, Brasil y Colombia se advierte que existe cierta conciencia digital, pero la falta sustantiva de la norma complica salvaguardar el bien jurídico patrimonial del sujeto pasivo ocasionando impunidad. La ley penal de delitos informáticos en Estados Unidos es la más completa, pues llega considerar al phishing como un tipo penal. Por el contrario, nuestra normativa nacional se encuentra desfasada, pues no se ha hecho una actualización a la misma desde el 2014 que entró en vigencia la última modificatoria, incluso la jurisprudencia en torno a este tipo penal es escasa, lo cual dificulta aún más su correcta aplicación y punición en la realidad.
2. En la doctrina se ha encontrado escasa bibliografía documental y virtual. Sin embargo, de lo estudiado, la doctrina califica el delito del Phishing como uno de los delitos informáticos que ha tenido un auge significativo durante los últimos años. Las razones por las cuales el phishing debe ser considerado como tipo penal son: En nuestra normativa, este delito al ser clasificado como ley penal en blanco dificulta la correcta aplicación al jurista; asimismo, el nivel de incidencia a nivel global ha ido en aumento vulnerando la esfera patrimonial e incluso la privacidad de las personas. A pesar de las

razones advertidas, el phishing no cuenta con una regularización exacta en nuestra normativa, ocasionando la impunidad de este delito.

3. En virtud de que la ley de delitos informáticos no cumplió aún con la función para la que fue legislada toda vez que, se encuentra desfasada a la realidad sociocultural en la que vivimos dejando de lado delitos con mayor incidencia como es el phishing. En ese sentido, se ha propuesto la incorporación del phishing como agravante del artículo 8 de la ley de delitos informáticos cuyo contenido tipifica el delito de fraude informático.

Recomendaciones

1. Se recomienda que las entidades públicas, privadas y población general reciban capacitación de lo susceptible que puede ser su información en un medio digital y el alcance que tienen los delincuentes para hacerse con esta información.
2. Se recomienda que se actualice urgentemente la Ley N° 30096 para que los delitos informáticos estén a la par con el contexto social e histórico actual.

Referencias

TESIS

Ventura, A. (2021). La tipificación del phishing, smishing y vishing en nuestro sistema penal peruano, para la lucha contra la ciberdelincuencia en lima, 2020. (Tesis de pre grado, Universidad Privada del Norte). Recuperado de https://repositorio.upn.edu.pe/bitstream/handle/11537/28942/Ventura%20Quijano%2c%20Mishell%20Alisson.pdf?sequence=11&isAllowed=y

Hidalgo, C. y Solano, G. (2021). El phishing como conducta delictiva no regulada en el ordenamiento juridico peruano. Propuesta de incorporación del artículo 7-a en la ley de delitos informáticos 30096. (Tesis de pre grado, Universidad Nacional Del Santa). http://repositorio.uns.edu.pe/bitstream/handle/UNS/3849/52376.pdf?sequence=1&isAllowed=y.

Zorrilla, K. (2018). Inconsistencias y ambigüedades en la ley de delitos informáticos ley nº 30096 y su modificatoria ley nº 30171, que imposibilitan su eficaz cumplimiento. (Tesis de pre grado, Universidad Nacional De Ancash "Santiago Antunez De Mayolo). Recuperado de http://repositorio.unasam.edu.pe/bitstream/handle/UNASAM/2332/T033_70221905_T.pdf?sequence=1&isAllowed=y.

Cangalaya, J. (2020). Fraude Informático en los Bonos de Subsidio Social en Épocas de pandemia, en la Provincia de Chanchamayo, 2020. (Tesis de pre grado, Universidad de Huánuco). Recuperado de http://repositorio.udh.edu.pe/bitstream/handle/123456789/2662/Cangalaya%20Hilario%2c%20Jhon%20Marathon.pdf?sequence=1&isAllowed=y

Huaman, C. (2020). "Los delitos informáticos en Perú y la suscripción del convenio de Budapest". (Tesis para optar el titulo profesional de Abogada. Universidad Andina de Cuzco). (pp. 95 – 98). Recuperado de https://repositorio.uandina.edu.pe/bitstream/handle/20.500.12557/4116/Marleny_Tesis_bachiller_2020.pdf?sequence=1&isAllowed=y

Acuario, S. (2016). "Delitos Informáticos: Generalidades". Recuperado de https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

Cavada, J. (22/12/2015). "delitos Informáticos. Chile Y Legislación extranjera". Recuperado https://www.camara.cl/verDoc.aspx?prmTIPO=DOCUMENTOCOMUNICACIONCUENTA&prmID=11020

Diazgranados, H. (21/08/2012). "Ciberataques en America Latina crecen un 24% durante los primeros ocho meses de 2021". Kaspersky daily. Recuperado https://latam.kaspersky.com/blog/ciberataques-en-america-latina-crecen-un-24-durante-los-primeros-ocho-meses-de-2021/22718/

Sazger, H. (2017). "La protección de datos y sistemas informáticos en el derecho penal alemán europeo. Tentativa de una comparación con la situación legal en Colombia". Recuperado de https://www.jura.uni-muenchen.de/fakultaet/lehrstuehle/satzger/unterlagen/mdp.pdf

Calderon, V. (2023). " Ley de delitos Informáticos N° 30096 y su influencia en La Población de Chiclayo en tiempos de Covid-19". Recuperado de https://repositorio.uss.edu.pe/bitstream/handle/20.500.12802/10627/Villanueva%20Calderon%20Juan%20Amilcar.pdf?sequence=1&isAllowed=y

Peralta, R. (2022). "los delitos informáticos y los dato en sistemas informáticos". Recuperado de http://repositorio.ulasamericas.edu.pe/bitstream/handle/upa/2572/1.Ricardo%20Peralta%20-%20Delitos%20informaticos%20-%2015%20Marzo.pdf?sequence=1&isAllowed=y

Flores, C.; Rodriguez, T.; Urbizagastegui, J.; et. All. (2022). "Ciberdelincuencia reporte de información estadística y recomendaciones para la prevención". Recuperado de

https://cdn.www.gob.pe/uploads/document/file/3562747/Reporte%20de%20Ciberdelincuencia.pdf.pdf

Pilmayquen, I. (2013). "Delitos informáticos en Latinoamérica. Estudio de sus legislaciones". Recuperado de https://www.pensamientopenal.com.ar/system/files/2015/03/doctrina40720.pdf

LIBROS:

Becerril, A.; Ortigoza, S. (2018). Habilitadores tecnológicos y realidades del derecho informático empresarial. Recuperado de http://www.scielo.org.mx/pdf/rius/v12n41/1870-2147-rius-12-41-11.pdf.

Malamud, S. (2018). Sabotaje Informático: ¿La Exigencia de Daño Grave como Elemento del Injusto?. N° 72. Universidad Buenos Aires: Argentina. Recuperado de https://www.researchgate.net/publication/328642554

Delgado, M. (2016). Delitos Informáticos Delitos Electrónicos. Recuperado de https://docplayer.es/2175196-Delitos-informaticos-delitos-electronicos-autora-lic-maria-de-lourdes-delgado-granados-prologo.html

Garavilla, M. (2021). "Delitos Informáticos". Recuperado de https://docer.com.ar/doc/s1sxs8x

Garcia, J. (2008). El fraude informático en España e Italia. Tratamiento jurídico-penal y criminológico. Revista cuatrimestral de las Facultades de Derecho y Ciencias Económicas y Empresariales. (pp. 292-305). Recuperado de https://revistas.comillas.edu/index.php/revistaicade/article/view/357/283

Bramont-Arias, L. (1997). "El delito informático en el Código Penal Peruano". Biblioteca de Derecho Contemporaneo. (Vol. 6). Recuperado de https://repositorio.pucp.edu.pe/index/handle/123456789/181585

ELEMENTOS NORMATIVOS

- Ley 30096
- Ley 30171

REVISTAS:

Mayer, L. y Oliver, G. (2020). "El Delito de Fraude Informático: Concepto y Delimitación". Vol. 9. Revista Chilena de Derecho y Tecnología. Recuperado de https://scielo.conicyt.cl/pdf/rchdt/v9n1/0719-2584-rchdt-9-1-00151.pdf

Mayer, L. y Oliver, G. (2020). “El Delito de Fraude Informático: Concepto y Delimitación”. Vol. 9. Revista Chilena de Derecho y Tecnología. Recuperado de https://scielo.conicyt.cl/pdf/rchdt/v9n1/0719-2584-rchdt-9-1-00151.pdf

Mayer, L. (2020). Elementos criminológicos para el análisis jurídico-penal de los delitos informáticos. Universidad de Talca. Recuperado de https://www.scielo.cl/pdf/iusetp/v24n1/0718-0012-iusetp-24-01-00159.pdf

Gonzáles, J.; Bermeo. J.; Villacreses, E. y Guerrero, J. (2018). Delitos Informáticos: una Revisión en Latinoamérica. Universidad Tecnica de Machala. Recuperada de http://investigacion.utmachala.edu.ec/proceedings/index.php/utmach/index

Leyva, C. (2021) “Estudio de los delitos informáticos y la problemática de su tipificación en el marco de los convenios internacionales”. Universidad Nacional de San Marcos. Recuperado de http://dx.doi.org/10.15381/lucerna.v0i1.18373

Roibon, M. (s.f.) “La estafa informática en el código Penal Argentino”. Recuperado de https://www.pensamientopenal.com.ar/system/files/2019/01/doctrina47322.pdf

Schurjin, D. (2022). “Delitos informáticos en argentina: normativa actual y posibilidades de cambio según el proyecto de nuevo código penal”. Revista Pensamiento Penal. Recuperado de www.pensamientopenal.com.ar

Gutiérrez, N. (2022). “30 Estadísticas Importantes de Seguridad Informática”. (Blog digital). Fundamentos de Ciberseguridad. Recuperado de https://preyproject.com/es/blog/30-estadisticas-seguridad-informatica