ESCUELA DE POSGRADO
UNIVERSIDAD CÉSAR VALLEJO

Tratamiento jurídico penal de los delitos informáticos contra el patrimonio, Distrito Judicial de Lima, 2018

TESIS PARA OPTAR EL GRADO ACADÉMICO DE:

Maestro en Derecho Penal y Procesal Penal

AUTOR:

Br. Alejo Pardo Vargas

ASESOR:

Dr. Jesús Enrique Núñez Untiveros

SECCIÓN:

Derecho

LÍNEA DE INVESTIGACIÓN:

Derecho penal

LIMA – PERÚ

2018

ESCUELA DE POSGRADO
UNIVERSIDAD CÉSAR VALLEJO

DICTAMEN DE LA SUSTENTACIÓN DE TESIS

EL / LA BACHILLER (ES): **PARDO VARGAS, ALEJO**

Para obtener el Grado Académico de ***Maestro en Derecho Penal y Procesal Penal,*** ha sustentado la tesis titulada:

TRATAMIENTO JURÍDICO PENAL DE LOS DELITOS INFORMÁTICOS CONTRA EL PATRIMONIO, DISTRITO JUDICIAL DE LIMA, 2018

Fecha: 28 de agosto de 2018 Hora: 7:45 p.m.

JURADOS:

PRESIDENTE: Dra. Gliria Susana Mendez Ilizarbe **Firma:** .....

SECRETARIO: Mg. Roberto Santiago Bellido García **Firma:** .....

VOCAL: Dr. Angel Salvatierra Melgar **Firma:** .....

El Jurado evaluador emitió el dictamen de:

.....APROBADO POR UNANIMIDAD.....

Habiendo encontrado las siguientes observaciones en la defensa de la tesis:

.....

.....

.....

.....

Recomendaciones sobre el documento de la tesis:

.....Cumplir APA.....

.....

.....

.....

Nota: El tesista tiene un plazo máximo de seis meses, contabilizados desde el día siguiente a la sustentación, para presentar la tesis habiendo incorporado las recomendaciones formuladas por el jurado evaluador.

Página de jurados

Dra. Gliria Susana Mendez Ilizarbe

Presidente

Mg. Roberto Santiago Bellido García

Secretario

Dr. Ángel Salvatierra Melgar

Vocal

Dedicatoria

A mis profesores y a quienes cada día se esfuerzan a estar a la altura del avance de las nuevas tecnologías informáticas.

Agradecimiento

A mis entrevistados Drs. Santiago Acurio Del Pino (Ecuador), Daniel Peña Labrin (Perú), Andrés Álvarez Pérez (España), Iván Manjarres Bolaño (Colombia), Gustavo Silva Huaman (Perú) e Ing. Gaston Miguel Semprini (Argentina) por haber colaborado incondicionalmente con su opinión en esta investigación.

Declaración de autoría

Yo, Alejo Pardo Vargas, estudiante de la Escuela de Posgrado, Maestría en Derecho Penal y Procesal Penal, de la Universidad César Vallejo, Sede Lima Norte; declaro que el trabajo académico titulado "*Tratamiento jurídico penal de los delitos informáticos contra el patrimonio, Distrito Judicial de Lima, 2018*" presentada, en 190 folios para la obtención del grado académico de Maestro en Derecho Penal y Procesal Penal, es de mi autoría.

Por tanto, declaro lo siguiente:

He mencionado todas las fuentes empleadas en el presente trabajo de investigación, identificando correctamente toda cita textual o de paráfrasis proveniente de otras fuentes, de acuerdo con lo establecido por las normas de elaboración de trabajos académicos. No he utilizado ninguna otra fuente distinta de aquellas expresamente señaladas en este trabajo.

Este trabajo de investigación no ha sido previamente presentado completa ni parcialmente para la obtención de otro grado académico o título profesional. Soy consciente de que mi trabajo puede ser revisado electrónicamente en búsqueda de plagios.

De encontrar uso de material intelectual ajeno sin el debido reconocimiento de su fuente o autor, me someto a las sanciones que determinen el procedimiento disciplinario.

Lima, Agosto del 2018

Alejo Pardo Vargas
DNI Nº70197606

Presentación

Señores miembros del jurado calificador

Presento a ustedes mi tesis titulada “Tratamiento jurídico penal de los delitos informáticos contra el patrimonio, Distrito Judicial de Lima, 2018”, cuyo objetivo fue: “Analizar el tratamiento jurídico penal de los delitos informáticos contra el patrimonio, Distrito Judicial de Lima, 2018”, en cumplimiento del Reglamento de grados y Títulos de la Universidad César Vallejo, para obtener el Grado Académico de Maestro.

En el presente trabajo, se estudia el tratamiento jurídico penal de los delitos informáticos contra el patrimonio que se le da actualmente en nuestro sistema jurídico. El estudio comprende los siguientes capítulos: el capítulo I se refiere a la introducción; el capítulo II refiere al problema de investigación, el capítulo III trata respecto al marco metodológico, en el capítulo IV se presentan los resultados, V discusión, VI conclusiones, VII recomendaciones, VIII propuesta de solución al problema, IX referencias usadas y finalmente en el capítulo X se consignan los anexos respectivos.

Los resultados obtenidos en la presente investigación demostró que el tratamiento jurídico penal de los delitos informáticos contra el patrimonio es deficiente, toda vez que ilógicamente se comprende dentro de fraude informático todo los tipos o modalidades de delitos informáticos contra el patrimonio, el cual genera incertidumbre en la interpretación de la norma que no permite la sanción efectiva de los delitos informáticos contra el patrimonio.

Señores miembros del jurado esperamos que esta investigación sea evaluada y merezca su aprobación.

Los Olivos, Agosto del 2018

Br. Alejo Pardo Vargas

Índice

Índice de tablas

Índice de figuras

Resumen

La presente investigación titulada “Tratamiento jurídico penal de los delitos informáticos contra el patrimonio, Distrito Judicial de Lima, 2018” tuvo como objetivo general Analizar el tratamiento jurídico penal de los delitos informáticos contra el patrimonio, Distrito Judicial de Lima, 2018. Para el cual se utilizó serie de métodos de investigación, propias de la investigación cualitativa, de nivel descriptivo explicativo. Se utilizó como técnica la entrevista con su respectivo instrumento de recolección de datos, la guía de entrevista, con el cual se recopiló información de los expertos sobre el tema, nacionales y extranjeros, llegándose a conclusiones precisas.

En tal sentido, se concluyó que el tratamiento jurídico penal de los delitos informáticos contra el patrimonio es deficiente, toda vez que ilógicamente se comprende dentro de fraude informático todo los tipos o modalidades de delitos informáticos contra el patrimonio, el cual genera incertidumbre en la interpretación de la norma que no permite la sanción efectiva de los delitos informáticos contra el patrimonio.

Finalmente se recomienda que el Congreso de la República formule iniciativa legislativa de para la adhesión del Perú al convenio de Budapest, así como debe legislar en forma expresa y tipificar los delitos informáticos contra el patrimonio, diferenciando las modalidades, sean éstos delitos de fraude, estafa, sabotaje o hurto informático, se debe crear fiscalías especializadas en delitos informáticos, la Corte Penal internacional debe asumir competencia para conocer delitos informáticos de carácter trasnacional y en todas las Universidades se debe incluir un curso obligatorio de derecho informático, así como a nivel de la formación primaria y secundaria se debe incluir en la malla curricular el curso de informática, con énfasis en la prevención de todo tipo de delitos informáticos.

Palabras claves: Informática, delito informático, delitos informáticos contra el patrimonio, hurto informático, estafa informática, fraude informático y sabotaje informático.

Abstract

This research entitled "Criminal legal treatment of computer crimes against property, Judicial District of Lima, 2018" had as its general objective Analyze the criminal legal treatment of computer crimes against property, Judicial District of Lima, 2018. For which a series of research methods was used, typical of qualitative research, descriptive descriptive level. The interview was used as a technique with its respective data collection instrument, the interview guide, with which information was collected from experts on the subject, national and foreign, reaching precise conclusions.

In this sense, it was concluded that the criminal legal treatment of computer crimes against property is deficient, since illogically it is understood within computer fraud all types or modalities of computer crimes against the heritage, which generates uncertainty in the interpretation of the norm that does not allow the effective sanction of the computer crimes against the patrimony.

Finally, it is recommended that the Congress of the Republic formulate a legislative initiative for the accession of Peru to the Budapest Convention, as well as expressly legislate and criminalize computer crimes against the heritage, differentiating the modalities, be they fraud offenses, fraud , sabotage or computer theft, prosecutors specialized in computer crimes should be created, the International Criminal Court must assume competence to know cybercrimes of a transnational nature and in all the Universities a compulsory computer law course should be included, as well as at the level of the Primary and secondary education should include in the curriculum the computer course, with emphasis on the prevention of all types of computer crimes.

Key words: Computing, computer crime, computer crimes against computer theft, computer fraud, computer fraud and computer sabotage.

I.- Introducción

1.1 Trabajos previos

1.1.1 Trabajos previos extranjeros

Respecto al tratamiento jurídico penal de los delitos informáticos existen diversos trabajos previos a nivel extranjero, de las cuales se presenta en este punto a modo de resumen, de los aspectos relevantes y relacionados al problema en estudio:

Abdulai (2016), realizó la investigación titulada "*Determinantes del miedo a la victimización del crimen de cibernética: un estudio del fraude a la tarjeta de crédito / débito entre estudiantes de la Universidad de Saskatchewan*" que sustentó en el Departamento de Sociología de la Universidad de Saskatchewan para optar el grado de Magister en Artes, cuyo objetivo de estudio fue investigar el miedo a la victimización por delito cibernético (fraude con tarjeta de crédito / débito) entre los estudiantes de la Universidad de Saskatchewan. Los hallazgos del estudio indican que la experiencia previa de victimización y los comportamientos de uso de Internet están asociados positivamente con el miedo de los estudiantes y su riesgo de convertirse en víctimas de fraude con tarjeta de crédito / débito. Por otro lado, se descubrió que los factores sociodemográficos y el conocimiento del delito cibernético son predictores no significativos del miedo y el riesgo de los estudiantes de convertirse en víctimas de fraude con tarjetas de crédito / débito. Con base en los hallazgos, el estudio aboga por la necesidad de repensar los riesgos y examinar más a fondo la reflexividad, a medida que las personas negocian el desafío de permanecer en el umbral del riesgo y la victimización real. El estudio empleó una encuesta en línea de estudiantes en la Universidad de Saskatchewan durante un período de dos meses. Para facilitar la comprensión del problema en estudio, se utilizó el marco teórico de la Sociedad Mundial del Riesgo de Beck. Esencialmente en esta teoría, Beck argumenta que, dadas las diversas consecuencias involuntarias de las numerosas innovaciones tecnocientíficas, los riesgos y peligros se han convertido en una característica permanente de la era moderna. Se hicieron preguntas sobre varias variables clave, que la literatura identificó como importantes para predecir el temor de las personas a las victimizaciones criminales. Entre estas variables se incluyen el conocimiento del delito cibernético, las variables sociodemográficas, la

experiencia de la victimización y los comportamientos de uso de Internet. En términos generales, el estudio encontró que la experiencia de victimización y los comportamientos de uso de internet están asociados positivamente con el temor de los estudiantes y su riesgo de convertirse en víctimas de fraude con tarjetas de crédito / débito. Asimismo se encontró que los factores sociodemográficos no predicen significativamente el temor a la victimización por fraude con tarjetas de crédito / débito. Es decir, la identificación sociodemográfica de los estudiantes no estaba relacionada con su temor a la victimización por fraude con tarjetas de crédito / débito.

Wang (2016), realizó la investigación titulada "*Estudio comparativo de la ciberdelincuencia en Derecho Penal: China, Estados Unidos, Inglaterra, Singapur y el Consejo de Europa*" que sustentó en la Universidad Erasmo de Rotterdam para optar el grado de Doctor, cuyo objetivo de estudio fue hacer un estudio comparativo de la ciberdelincuencia de los países China, Estados Unidos, Inglaterra, Singapur y el Consejo de Europa. En tal sentido, entre sus conclusiones señala que China tiene un sistema de regulación de niveles múltiples en malas acciones cibernéticos, con el de los instrumentos básicos y principales y sus dos enmiendas. Aunque ambos de los dos Enmiendas ha ampliado el alcance de los delitos informáticos, las razones de expansiones eran diferentes. La Enmienda (VII) se publicó en 2009 para cubrir la brecha que se levantó junto con la creciente popularidad de los ordenadores personales. Después de esta modificación, se estableció el enfoque de dos puntos y una dimensión. Este enfoque hace una clara distinción entre el delito informático genuina (es decir, los delitos que tienen como objetivo la seguridad del sistema de información de la computadora y los datos) y los delitos tradicionales facilitados por computadoras (es decir, delitos en virtud de las disposiciones penales tradicionales). Señala que en los EE.UU. pese a que logra penalizar las malas acciones cibernéticos no está exenta de problemas. Una preocupación importante es su actitud hacia el equipo y los datos. En los delitos de piratería los legisladores eligen una perspectiva estrecha y proteger la seguridad de la computadora; mientras que en otros delitos como el tráfico de dispositivos, las secciones relacionadas se basan en el concepto de datos e información. A partir

de estos dos puntos de vista en consideración, la gente puede encontrar la legislación de los Estados Unidos sobre la ciberdelincuencia menos consistente, y esa incompatibilidad conduce a problemas en la práctica judicial. Inglaterra opta por introducir nuevas disposiciones y actos que se actúe con los 'genuino ciberdelincuencia' y se basan en sus disposiciones penales existentes que se ocupan de los delitos tradicionales facilitados por computadoras. Este enfoque, como sugiere la Comisión de Derecho, se llama el enfoque 'a medio camino', lo que significa que 'rechazar la creación de completamente nuevos delitos, excepto cuando éstos son absolutamente necesarios, pero se debe estar preparado para contemplar la ampliación de los delitos generales existentes. Considera que Singapur ha sido activo en la promulgación y modificación de su Ley sobre Abusos Informáticos. El enfoque implementó es notable por los solapamientos y repeticiones dentro de disposiciones. En primer lugar, se aprendió de la Ley de Inglaterra sobre el mal uso de computadoras e introdujo los delitos de piratería que amenazan la seguridad de los datos, incluyendo mera piratería, la piratería de nuevos delitos, modificación de datos, y otros. Al mismo tiempo, se tomó las disposiciones equivalentes Canadienses e introdujo los delitos de piratería, el cual se centra en la capacidad de procesamiento y almacenamiento de la computadora, como el uso de los servicios informáticos sin autorización. Finalmente concluye que el desarrollo de tecnología de la información y dispositivos digitales ofrece nuevas oportunidades para los delitos. El primero, facilita crímenes tradicionales como el fraude, y por el segundo, genera nuevos crímenes como la piratería. Los crímenes tradicionales facilitados por computadoras y los nuevos crímenes generados por computadoras son el llamado cibercrimen. Para combatir el cibercrimen, las jurisdicciones han desarrollado contramedidas en el campo del derecho penal tanto a nivel nacional como internacional. A nivel nacional, China, los Estados Unidos, Inglaterra y Singapur han experimentado reformas significativas para adaptar su legislación penal. A nivel internacional, el Consejo de Europa ha lanzado seminarios y proyectos que analizan el cibercrimen y exploran soluciones, y ha redactado la Convención sobre Ciberdelincuencia. Sin embargo, el cibercrimen todavía comúnmente ocurrido indica la insuficiencia de estas contramedidas para el cibercrimen. Las principales razones de esta insuficiencia son la cobertura

limitada de la ley penal, la naturaleza transitoria y transnacional del delito cibernético y las incoherencias entre las legislaciones nacionales sobre ciberdelincuencia.

Alanezi (2015), realizó la investigación titulada "*Las percepciones de fraude en línea y el impacto sobre las contramedidas para el control del fraude en línea en las instituciones financieras de Arabia Saudí*" que sustentó en la Facultad de Diseño de Ingeniería y Ciencias Físicas, Departamento de Ciencias de la Computación de la Universidad Brunel de London, para optar el grado de Doctor en Filosofía, cuyo objetivo de estudio fue examinar las contramedidas empleadas por las instituciones financieras en Arabia Saudita y el impacto de las contramedidas de forma individual y colectiva en el control y prevención del fraude en línea en Arabia Saudita. Señala que las personas son dependientes de Internet; la posibilidad de ser violado por los hackers y estafadores está creciendo, especialmente en lo que la socialización, compras en línea y la banca se llevan a cabo a través de computadoras personales o dispositivos móviles. El fraude en línea ha sido descrito como una epidemia que se ha extendido a la mayoría de las actividades en línea. Su prevalencia se ha observado que en las regiones donde hay un alto nivel de adopción del comercio electrónico, y, junto con él, grandes transacciones financieras en línea. Por lo tanto, el argumento es que las medidas tomadas son o son insuficientes o no han podido hacer frente con eficacia todos los problemas a causa del contexto organizacional y ambiental del país. La investigación fue de enfoque cualitativo, técnica de entrevista a expertos, la población del estudio estuvo conformada por doce grandes instituciones financieras de Arabia Saudita, incluyendo bancos y otras organizaciones que prestan servicios financieros, en especial los departamentos de Tecnología de la Información, departamentos de comercio electrónico y servicios de gestión de riesgos de los bancos más importantes. Finalmente, entre otros, el investigador concluye que la expansión del comercio electrónico y las actividades en línea están siendo atendidos por el gobierno de Arabia Saudita con el apoyo activo de los bancos, por la introducción de servicios de tecnología de la información para los servicios bancarios. Sin embargo, esta expansión de las actividades en línea y uso de información tecnologías en las transacciones

bancarias también crean oportunidades y lagunas explotadas por algunos estafadores en línea, lo que resulta en la pérdida de más de 20 millones de dólares en 2010 y 2012. La investigación identificó un aumento en el fraude en línea, debido a la gran concentración de bancos, el aumento de la base de usuarios, el gran número de transacciones financieras, la mala conciencia de seguridad y las percepciones de los involucrados (el entorno socio-cultural y mucho más). Precisa que las contramedidas no son exhaustivos ni suficientemente adecuadas para reducir la tasa de fraude en línea, que sigue siendo alta. No hay ningún enfoque sistemático adoptado por los bancos y el gobierno a la organización y coordinación de los componentes de las contramedidas, lo que confirma el estudio están relacionadas entre sí.

Rincón (2015), realizó la tesis titulada "*El delito en la cibersociedad y la justicia penal internacional*" sustentada en la facultad de Derecho de la Universidad Complutense de Madrid, para optar el grado de Doctor, tuvo como objetivo de investigación "Proponer la base de una elaboración teórica desde la dogmática penal internacional que permita discutir sobre la necesidad de incluir la investigación y juzgamiento de los delitos informáticos, electrónicos y de las telecomunicaciones en la competencia del Estatuto de Roma" en tal sentido señala que el uso de las tecnología y la racionalidad de la ciencia supo crear un nuevo paradigma con el cual el ser humano entró en una nueva época, de modo tal que el conocimiento y tecnología se convierten, rápidamente, en el mejor aliado de la producción de riqueza. Señala que el "problema del fraude internacional ha sido planteado por diversos sectores de la sociedad internacional, desde organizaciones internacionales hasta empresas transnacionales", como por ejemplo la empresa McAfee, sustentado en información del FBI y la inteligencia europea en diciembre de 2006 publicitado en apartes por la Asociación de Internautas, se señala que una de las causas del auge del cibercrimen en Europa del este, es el alto grado de desempleo y de los bajos salarios, "muchos de esos cibercriminales ven internet como una oportunidad de empleo". Que toda información debe ser objeto de protección tecnológica, y como muestra de ello se aprecia que los "Estados en ejercicio de su autonomía y soberanía han decidido perseguir penalmente a quienes ejecutan conductas que se tipifican como delitos

informáticos o delitos en contra de la información y los datos como bienes jurídicos tutelados". Sin embargo, al igual que en la persecución y sanción de cualquier otra categoría de delito, las fronteras creadas no solo por el territorio sino por el concepto de jurisdicción y competencia que son los delimitantes del ejercicio punitivo de los Estados, impiden que se investigue, juzgue y sancione a quienes hayan cometido la conducta desde un territorio pero con consecuencias en otro, es decir, el delito se cometió desde un Estado pero las víctimas o el daño se materializan en otro estado, por lo que estas limitaciones y fronteras crea impunidad en la búsqueda y persecución de los delitos informáticos. Entre otras conclusiones señala que Organismo Internacional más adecuado que debe tener competencia para sancionar los delitos informáticos es la Corte Penal Internacional, y la solución a largo plazo, como un punto de partida en la sanción internacional de los delitos informáticos sería la modificación del Estatuto de Roma, donde los ciberdelitos o delitos universales no sean conocidos por la Corte Penal Internacional de forma subsidiaria o residual, sino que, por el contrario, por tratarse de delitos Universales, es esta instancia de Derecho Penal Internacional quien cuenta con los requisitos y calidades para adelantar su persecución, siendo este órgano quien realice su investigación, juzgamiento y sanción.

González (2013), en su investigación titulada "*Delincuencia informática: daños informáticos del artículo 264 del Código Penal y propuesta de reforma*" sustentada en la facultad de Derecho, Departamento de Derecho Penal de la Universidad Complutense de Madrid, para optar el grado de Doctor, tuvo como objetivo de investigación ofrecer una visión general de la delincuencia informática en la actualidad, centrando su análisis en el marco legal de los delitos de daños informáticos, quien después de un análisis exhaustivo de los diferentes delitos informáticos, tipos y modalidades, entre sus principales conclusiones señala que la expansión exponencial de la ciberdelincuencia es innegable, y se trata de un fenómeno novedoso que cuyas prácticas delictivas requiere la intervención de los diferentes estados, que además tiene una característica inherente al desarrollo tecnológico; la tecnología avanza a un ritmo vertiginoso, y este tipo de delitos, su aparición y su desarrollo tienen, en contradicción con el lento avance del Derecho en el tratamiento jurídico penal de los delitos informáticos. Señala que la

informática tiene un carácter trasnacional, por lo que nunca es suficiente la regulación protectora en un único Estado, no existe ausencia en la regulación eficiente en los demás o resto de Estados, puesto que para la comisión de los delitos informáticos, no se requiere la cercanía física, puede hacerlo tan lejos como el medio de comunicación o el internet tiene alcance.

Piccirilli (2015), realizó la investigación titulada "*Protocolos a aplicar en la Forensia Informática en el marco de las nuevas tecnologías (Pericia – Forensia y Cibercrimen)*" que sustentó en la Facultad de Informática de la Universidad Nacional de La Plata para optar el grado de doctor en Ciencias Informáticas, cuyo objetivo de esta tesis doctoral fue desarrollar una propuesta metodológica para definir protocolos de base a utilizar en el uso de la forensia aplicada al tratamiento de la evidencia digital, en el marco de las nuevas tecnologías informáticas. En este sentido, el autor realiza un análisis de la prueba desde el secuestro hasta el análisis pericial correspondiente, el enfoque metodológico empleado en el desarrollo del estudio es analítico, señala que es bastante alto el nivel de la ciberdelincuencia, y que la constante evolución del delito es la que provoca generar nuevas inquietudes. Entre otras conclusiones señala que a la luz del nuevo Código Procesal Penal Argentino, tomando en cuenta la nueva paradigma legal de las pericias en general y en particular las pericias de carácter informático, es necesario cubrir las falencias de los procedimientos vigentes, por lo que es necesario contar con un protocolo actual y formalizado para afrontar los desafíos técnicos relativos a las nuevas tecnologías informáticas. Como recomendación señala que es necesario crear un órgano asesor técnico informático pericial.

1.1.2 Trabajos previos nacionales

Los trabajos previo a nivel nacional que sean actuales a nivel de posgrado son muy escasas respecto al problema objeto de investigación, o por lo menos de los delitos informáticos, por lo que la presentación de estos trabajos previos se limitan a los existentes a la fecha, siendo los mismos los siguientes.

Sánchez (2017), realizó la investigación titulada "*Adopción de estrategias de Ciberseguridad en la protección de la información en la Oficina de Economía*

del Ejército, San Borja- 2017" sustentada en la escuela de posgrado del Instituto Científico Tecnológico del Ejército "Gral Div Edgardo Mercado Jarrín", para optar el grado académico de Magister en ingeniería de sistemas de armas, tuvo como objetivo principal fue "Determinar de qué manera la adopción de estrategias de ciberseguridad incide en la protección de la información en la Oficina de Economía del Ejército" para el cual tuvo como población de estudio a 30 oficiales, 40 técnicos y busoficiales y 180 empleados civiles, teniendo una muestra de 152 participantes, en la que utilizó como técnicas de estudio a la encuesta, entrevista y análisis documental, y como instrumentos de recolección de datos tales como el cuestionario, guía de entrevista y las fichas bibliográficas. El tipo de estudio fue no experimental con diseño transaccional o transversal, nivel de investigación descriptivo y explicativo. Una vez desarrollado los procedimientos metodológicos de la investigación, el estudio concluye que la adopción de estrategias de ciberseguridad incide significativamente en la protección de la información en la Oficina de Economía del Ejército, y entre otras conclusiones señala que en la Oficina de Economía del Ejército no existen planes de protección contra ciberterrortistas y se ponen en ejecución y que los dispositivos con las que cuenta el Ejército no son de última generación, por lo que no se garantiza la protección de la alteración de la información. Entre otras recomendaciones señala que la Oficina de Economía del Ejército debe tomar acciones legales y disciplinarias para sancionar a quienes coadyuven directa o indirectamente con los actos de los cibercriminales, asimismo, se debe prever y priorizar adquisición de softwares de última tecnología para el tratamiento o manejo de la información reservada y garantizar la protección efectiva evitando cualquier tipo de alteración.

Alarcón y Barrera (2017), realizaron la investigación titulada "*Uso de internet y delitos informáticos en los estudiantes de primer semestre de la Universidad Pedagógica y Tecnológica de Colombia, Sede Seccional Sogamoso 2016*", sustentada en la Escuela de Posgrado de la Universidad Privada Norbert Wiener para optar el grado académico de maestro en informática educativa tuvieron como objetivo general de investigación determinar la relación del uso del internet con los delitos informáticos en los estudiantes de primer semestre de la Universidad Pedagógica y Tecnológica de Colombia, seccional Sogamoso, 2016,

para el cual utilizaron el tipo de investigación básico, de nivel correlacional, enfoque cuantitativo y el diseño de estudio fue no experimental, cuya población de estudio estuvo conformada por los estudiantes, y tuvieron una muestra de 60 de dichos estudiantes. La técnica de recolección de datos utilizado fue la encueta y su respectivo instrumento, el cuestionario conformada por 36 preguntas cerradas. En este orden de ideas, el estudio concluye que el uso del internet que implica las competencias informacionales por habilidad, acceso a la información y aspectos sociales se relacionan con la comisión de delitos informáticos, es decir que la ocurrencia de los delitos informáticos depende del desarrollo de las competencias informacionales en el uso del internet. Finalmente, los investigadores recomiendan que se debe involucrar a los docentes y directivos de las instituciones a que implementen módulos prácticos que permita a los estudiantes alejarse de las prácticas inapropiadas con el uso de la informática, asimismo recomienda concientizar a los estudiantes respecto al uso de la información en la internet.

Tenorio y Tuesta (2012), realizaron la investigación titulada "*Legislación del secreto bancario y su relación con el delito de hurto informático de dinero mediante la violación de claves secretas, Iquitos- 2010*" que sustentaron en la Escuela de Posgrado "José Torres Vásquez" de la universidad Nacional de la Amazonía Peruana, para optar el grado académico de magister en derecho y ciencias penales, cuyo objetivo de investigación fue determinar cómo influye la regulación de la legislación del secreto bancario en el incremento del delito de hurto informático de dinero, mediante la violación de claves secretas, en Iquitos durante el 2010, en la que se tuvo como población de estudio a los usuarios que fueron víctimas, policías, abogados, funcionarios de las entidades financieras e INDECOPI que ven el delito objeto de estudio, el nivel de investigación fue correlacional, diseño no experimental. Como técnica de recolección de datos utilizaron la encuesta. Entre las principales conclusiones señala que la legislación del secreto bancario en el Perú, no es acorde con el avance tecnológico y el incremento de la criminalidad cibernética, asimismo señala que el secreto bancario constituye un obstáculo en la investigación del delito de hurto informático de dinero, puesto que el secreto bancario se levanta exclusivamente por orden

judicial en procesos concretos, el cual influye en la impunidad de los autores del delito de hurto informático de dinero, es más, ninguna de las instituciones cuenta con estadísticas del registro de casos de hurto de dinero a las cuentas de los clientes de las entidades financieras, en la modalidad de violación de las claves secretas.

Si bien es cierto que existen investigaciones sobre el tema a nivel de posgrado, pero los mismos son anteriores a la promulgación de la nueva Ley de delitos informáticos, por lo que no tiene mucho sentido citar como parte de los antecedentes, por el contrario, existen investigaciones de grado que no es posgrado, pero que a criterio del investigador cobrar relevancia académica y requieren ser citadas, investigaciones como los siguientes:

Espinoza (2017), realizó la investigación titulada "*Derecho penal informático: deslegitimación del poder punitivo en la sociedad de control*", que sustentó en la facultad de ciencias jurídicas y políticas de la Universidad Nacional del Altiplano para optar el título profesional de Abogado, tuvo como objetivo de estudio definir el Derecho Penal Informático, para el cual utilizó métodos de investigación como la dogmática jurídica, inductivo, deductivo, histórico, comparativo, analítico y sintético, señala que el Derecho Penal informático tiene por objeto de estudio la seguridad jurídica y las leyes penales sobre delitos informáticos, cuya finalidad es reducir el poder de vigilancia del poder punitivo y se caracteriza por ser represivo, público, fragmentador, continuo y normativo; los delitos informáticos son transnacionales y multidisciplinarios. El investigador recomienda que se formulen propuestas legislativas de acuerdo a los principios internacionales de Derechos Humanos sobre vigilancia de las comunicaciones y crear fiscalías especializadas en tecnologías de información y comunicación.

Sequeiros (2016), en la investigación titulada "*Vacíos legales que imposibilitan la sanción de los delitos informáticos en el Nuevo Código Penal Peruano-2015*" sustentada en la Facultad de Derecho y Ciencias Políticas de la Universidad de Huánuco para optar el título profesional de Abogado, tuvo como objetivo de estudio determinar qué vacíos legales en el Nuevo Código Procesal Penal Peruano y en sus leyes complementarias imposibilitan la sanción de los delitos informáticos en el Perú el 2015, para el cual tuvo como población a los

fiscales del distrito judicial de Huaura que laboran en el distrito de Huacho, cuya muestra estuvo conformada por 60 de ellos. El estudio fue de tipo básica, de enfoque cualitativa, diseño no experimental, se utilizó como técnicas de recolección de datos a la encuesta y la entrevista. Entre las principales conclusiones, la investigación señala que debido a la naturaleza virtual de los delitos informáticos, estos se pueden volver confusos en su tipificación, ya que a nivel general, se poseen pocos conocimientos y experiencias en el manejo de ésta área. Asimismo, considera que uno de los factores críticos es el impacto de los delitos informáticos en la sociedad frente a la falta de información que éstos tienen, por lo que se requieren mayores conocimientos en tecnologías de información para el manejo de las situaciones, los delitos informáticos no deben ser un obstáculo para el normal desarrollo de las actividades económicas con el uso de las tecnologías, sino, se deben formular retos profesionales en la informática, con el objetivo de encaminar esfuerzos en robustecer la seguridad, controles y la integridad de la información en las organizaciones. Finalmente, el estudio recomienda que se hagan reformas normativas en lo relativo a los delitos informáticos con el fin de eliminar la incertidumbre que existe sobre la responsabilidad penal para los casos donde exista vulneración de la seguridad de los datos o sistemas informáticos, para de este modo reducir o eliminar la impunidad de los delitos informáticos.

1.2 Marco teórico referencial

En esta parte de la investigación se presentan y desarrollan algunas teorías, conceptos y aspectos teóricos relevantes respecto al tratamiento jurídico penal de los delitos informáticos, así como en forma especial, en lo relativo al fraude, estafa, hurto y sabotaje informático.

De la invención de la computadora y su posterior implementación de las redes informáticas, internet y otras sistemas informáticos, el derecho se vio obligado a regular aspectos vinculados a la informática aunque en forma retrasada, en los diversos ámbitos y especialmente en el ámbito comercial, sin embargo, lo es también la necesidad de regular en el ámbito penal debido a que las conductas ahí desarrolladas constituyen intolerables por la sociedad, es así

como nace el derecho informático y específicamente el derecho penal informático, dada la necesidad de sancionar conductas que afectan bienes jurídicos penalmente relevantes.

Tratamiento jurídico penal

Con el tratamiento jurídico penal, en el desarrollo de esta investigación se hace referencia al tratamiento doctrinario, dogmático, jurisprudencial, teórico y normativo de los delitos informáticos, especialmente a los delitos informáticos contra el patrimonio, con énfasis en las modalidades de estafa, fraude, sabotaje y hurto informático, a su vez, el tratamiento jurídico penal se puede descomponer en dos subcategorías, como son, el tratamiento procesal y el tratamiento legislativo.

Tratamiento procesal

El tratamiento procesal de los delitos informáticos contra el patrimonio en su modalidad de hurto, estafa, sabotaje y fraude informático hace referencia a los actos de investigación de estos delitos, es decir, el tratamiento de los aspectos procesales para la sanción de los delitos informáticos. Al respecto, existe un problema bastante grave por la característica especial de estos tipos de delitos, es decir, que la consumación de los delitos informáticos se puede realizar sin tomar en consideración las limitaciones espaciales.

Es así, que es totalmente factible la comisión de los delitos informáticos de un país o continente, cuyos efectos y la víctima se encuentre en el otro extremo del planeta, e incluso el delincuente cibernético tiene la posibilidad de ocultar la identidad, lugar y tiempo de comisión de los actos ilícitos, es decir, es factible que de acuerdo a su IP del ordenador que usa se determine que se encuentra en un determinado país, sin embargo, dicho dato es totalmente falso y busca no ser identificado, por lo que los países presentan grandes dificultades en la investigación de estos ilícitos, topándose con un primer problema de jurisdicción, y el otro por la falta de mecanismos técnicos y normativos que facilite su investigación.

Tratamiento normativo

Por el tratamiento normativo se debe tener en cuenta las diversas normas, tanto derogadas como vigentes relativas a los delitos informáticos contra el patrimonio, ya sea de alcance nacional o internacional.

Así se tiene en el ámbito nacional el Código Penal, la ley de delitos informáticos y sus modificatorias, por otro lado, a nivel internacional o extranjero se tiene a las normas de los otros países, y en especial al convenio de cibercriminaliad o de Budapest, único convenio de alcance internacional, aplicable a los países que suscribieron, sin embargo, como dicho convenio es de 2001, se debe reconsiderar el contenido y someter a efectos de actualizar de acuerdo a la realidad de los países en la actualidad.

Derecho informático.

Antes de definir el derecho informático debemos previamente descifrar el término o palabra informática. La palabra informática es un neologismo que deriva de vocablos información y automatización, el cual fue históricamente sugerido por Phillipe Dreyfus en 1962. En este orden de ideas, es factible afirmar que la informática es el conjunto de técnicas dirigidas al tratamiento lógico y automatizado de la información con el objetivo de la toma de decisiones eficientes.

En tal sentido, conforme señala (Rodríguez, 2013, p. 13), el Derecho Informático es el tratamiento sistemático y normativo tendiente a regular la informática en sus múltiples aplicaciones (burótica, robótica, telemática etc.). Es una rama del derecho conformada por un conjunto de normas, doctrina, aplicaciones, procesos que tiene por objeto regular toda actividad o conductas vinculadas con las tecnologías informáticas.

El derecho penal informático.

Como se señaló anteriormente, siendo el derecho informático una rama del derecho que regula las relaciones o conductas para con las tecnologías informáticas, el derecho penal informático viene a ser una rama del derecho informático que regula y sanciona conductas penalmente relevantes que son

efectuadas por medio de las tecnologías informáticas, es decir, el derecho penal informático se encarga de la prevención y sanción de la comisión de delitos informáticos.

Actualmente la información de las empresas y las personas cada vez màs tiende a ser almacenada en bases de datos electrónicas, el cual ha provocado la aparición de diferentes formas de delitos informáticos derivados de la utilización de la información con fines lucrativos o maliciosos, o la alteración de la misma. (Chaparro, 2014, p. 32).

El derecho penal informático, en primer momento aparece principalmente como una institución del derecho penal, con la finalidad de sancionar conductas informáticas que afectaban al patrimonio de las personas y empresas, sin embargo, debido a la necesidad y por el avance de las nuevas tecnologías y las formas de comisión de actos socialmente reprochables, el rango de alcance del derecho penal informático se ha extendido a conductas en los sistemas informáticos que no afectan el patrimonio de las personas y/o empresas, sino también, comprende como bienes jurídicos penalmente protegidos a la integridad de las personas, de los datos, del mismo sistema, la fe pública, la seguridad y otros de similar relevancia.

La ciberdelincuencia.

La evolución de la tecnología de la información dio a luz al espacio cibernético donde en Internet ofrece igualdad de oportunidades a todas las personas a acceder a cualquier información. Debido al aumento en el número de internautas, el mal uso de la tecnología es cada vez mayor, que conduce a los delitos cibernéticos. Los delitos cibernéticos son, básicamente, suscritas por las personas en el grupo de edad de 13 a 25 años de edad que todos están bien educados. La ciberdelincuencia se refiere a los actos ilegales en qué parte del equipo es o bien una herramienta o de destino o ambos (Aggarwal, Arora, Ghai y Poonam, 2014, p.48).

Al respecto, (Das y Nayak, 2013, p. 142) señalan que la ciberdelincuencia es un término usado para describir en términos generales la actividad criminal en la que los ordenadores o redes de ordenadores son una herramienta, un objetivo,

o un lugar de actividad criminal e incluyen todo, desde el agrietamiento electrónico a ataques de denegación de servicio. También se utiliza para concretar delitos tradicionales en las que se utilizan los ordenadores o redes para realizar actividades ilícitas. El criminal cibernético puede detener cualquier ferroviaria donde está, puede confundir a los aviones en su vuelo al confundirlo con señales incorrectas, puede hacer que cualquier dato militar importante caiga en manos de países extranjeros, y puede detener los medios electrónicos y cada el sistema puede colapsar en una fracción de segundos.

En este orden de ideas, se puede, entonces, señalar que la ciberdelincuencia es cualquier conducta o actividad con el uso de la internet, sea éste de carácter privada o pública, o sistema informático cualquiera con la finalidad de lograr un objetivo ilícito que puede consistir en líneas generales en la destrucción o daño de ordenadores, base de datos, medios electrónicos, interceptaciones, así como sacar provecho indebido de los bienes, el cual se traduce en delitos informáticos o ciberdelitos.

Delito informático.

Definición.

Para definir cualquier tipo de delito, previamente debemos preguntarnos cuando es que un hecho constituye delito, esto es, en qué momento de la conducta humana pasamos de cualquier hecho a catalogar como delito, al respecto, Lamperti (2017) señala que un hecho constituye delito cuando es relevante jurídicamente, el cual implica que un hecho cualquiera para que sea delito debe estar regulado penalmente; entonces se podrá decir que el hecho encuadra en un tipo penal, es a ésta la que se le conoce como principio de legalidad, y el juez tiene la prohibición de sancionar otras conductas que no estén estrictamente tipificadas en la ley penal (p. 85).

Al decir de (Levin y Ilkina, 2013) el Ciberdelito (o delitos informáticos) es cualquier crimen donde la tecnología de la información y la comunicación es: 1) utilizado como una herramienta en la comisión de un delito; 2) el objetivo de un delito; 3) un dispositivo de almacenamiento en la comisión de un delito (p. 14).

Por su parte, (Villavicencio, 2014) considera que se entiende por criminalidad informática a aquellas conductas dirigidas a burlar los sistemas de dispositivos de seguridad, esto es, invasiones a computadoras, correos o sistemas de datas mediante una clave de acceso; conductas típicas que únicamente pueden ser cometidas a través de la tecnología. (p. 286). Con el cual coinciden (Laredo y Ramírez, 2013) al decir que el “Delito informático es el uso de cualquier sistema informático como medio o fin de un delito” (p. 45).

En este sentido, s puede establecer que una de las características fundamentales de los delitos informáticos es que para la configuración de dichos ilícitos, el sujeto activo de la conducta delictiva, necesariamente debe emplear o usar un sistema o dispositivo informático.

Al respecto, Ramírez y Castro (2018) sostienen que el “(…) delito informático es todo aquel acto antijurídico y de carácter culpable que se da por medios informáticos o que pretende manipular o dañar computadores, redes de internet o medios electrónicos” (p. 57). El delito informático implica actividades criminales que los países han tratado de encuadrar en figuras típicas de carácter tradicional, tales como robos, hurtos, fraudes, falsificaciones, perjuicios, estafas, sabotajes. Sin embargo, debe destacarse que el uso de las técnicas informáticas ha provocado nuevas posibilidades del uso indebido de las computadoras lo que ha creado la necesidad de regulación por parte del derecho. (Imbaquingo, *et. al*, 2016, p. 130).

Finalmente, (Besares, 2015, p. 53) señala que el “delito informático es la conducta típica antijurídica y culpable que afecta la seguridad informática y el derecho humano de la intimidad de las personas, mediante el tratamiento doloso de los datos, que se distinguen de los demás supuestos de los llamados delitos computacionales o electrónicos”. En consecuencia se puede afirmar que el delito informático es aquella conducta típica, antijurídica y culpable que se comete empleando los medios informáticos, con fines lucrativos o no.

Delitos de cuello blanco.

Muchos de los "delitos informáticos" encuadran dentro del concepto de "delitos de cuello blanco", término introducido por primera vez por el criminólogo

estadounidense Edwin Sutherland en 1943. Esta categoría requiere que: (1) el sujeto activo del delito sea una persona de cierto estatus socioeconómico; (2) su comisión no pueda explicarse por falta de medios económicos, carencia de recreación, poca educación, poca inteligencia, ni por inestabilidad emocional. Son individuos con una gran especialización en informática, que conocen muy bien las particularidades de la programación de sistemas computarizados, de forma tal que logran un manejo muy solvente de las herramientas necesarias para violar la seguridad de un sistema automatizado (Pecoy, 2012). (Alcívar, Domenech y Ortiz, 2015, p. 46).

Internacionalidad de los delitos informáticos.

Se debe tener en cuenta que los delitos informáticos, debido a la característica de que se puede cometer sin estar presenten en el lugar donde se afectan los bienes jurídicos protegidos, éste se puede cometer de cualquier parte del país o del mundo, es decir, no existe limitación espacial alguna para la comisión del ilícito penal, por lo que tiene una carácter internacional.

Al respecto (Temperini, 2014) precisa que entre los diferentes desafíos inherentes o característicos de los delitos informáticos a nivel mundial, encontramos la posibilidad de que estos puedan ser cometidos sin respetar barreras geográficas o jurisdiccionales. Esto implica que cualquier delincuente informático puede ejecutar acciones desde un determinado lugar, conectándose a sistemas o equipos en otra parte y finalmente atacar datos o sistemas ubicados en otro lugar. (p. 132).

Los delitos informáticos son cada vez más notables frente a la vulnerabilidad que muestran los sistemas y en especial los usuarios, puesto que “Los gobiernos en conjunto con millones de usuarios y empresas utilizan esta tecnología para el desarrollo de funciones que se desarrollan a diario. La seguridad en Internet se convierte en un trabajo crítico que causa estragos en la vida cotidiana. Cada día existen miles de ataques que se materializan principalmente por estados, naciones, gobiernos, y ciberdelincuentes”. (López, López y Jerónimo, 2017, p. 2).

Por otro lado, (García, 2017, p. 17) señala que la Internet, las redes y tecnologías similares se han convertido en instrumentos indispensables para los Estados Miembros de la OEA. La Internet ha impulsado un gran crecimiento en la economía mundial y ha aumentado la eficacia, productividad y creatividad en todo el Hemisfeno. Individuos, empresas y gobiernos cada vez utilizan más las redes de información que integran la Internet para hacer negocios; organizar y planificar actividades personales, empresariales y gubernamentales; transmitir comunicaciones; y realizar investigaciones.

Al decir (Ibrahim, 2016, citando a Wall y otros), a diferencia de los delitos tradicionales, un plan criminal en el ámbito del ciberespacio puede implicar múltiples naciones y actores e incluso impacto en varios países al mismo tiempo. Así, mientras el crimen tradicional tiende a ser considerada a nivel local, los delitos informáticos se suele considerar a escala global. Por ejemplo, supongamos que una persona en Rusia crea los "*virus / malware"* , mientras que otra persona en Nigeria lo alquila para enviar correos electrónicos para recopilar datos de las cuentas de crédito y un tercero en los Estados Unidos transfiere fondos usando los datos adquiridos ilegalmente, los tres individuos están implicados en diferentes fases (p. 45).

Dentro de este campo de los fenómenos jurídicos – económicos se inserta la profunda innovación de las comunicaciones cuyo efecto jurídico se manifiestan en nuevas características, entre ellas merecen mencionarse la existencia de una red internacional descentralizada, desregulada que no conoce, tampoco reconoce, autoridad nacional visible, un ejemplo es la telefonía, que hasta no hace muchos años atrás era considerada un monopolio natural, con derechos concentrados en unos pocos, hoy la tecnología aplicada a la cibernética permite derrumbar el mito del monopolio natural, abriendo un campo nuevo a la competencia, donde la conformación de una red universal permite transmitir, voces, imágenes, datos etc. (Rodríguez, 2013, p. 20).

Marco Jurídico Internacional de la Cibercriminalidad.

Ante el panorama de cibercriminalidad la comunidad internacional reaccionó con una serie de conferencias, convenciones, congresos y eventos internacionales,

que derivaron en acuerdos, criterios, principios y medidas tendentes a dar solución a los problemas generados por las nuevas conductas delictivas, ya que por el carácter transnacional de estos delitos y la posibilidad de cometerlos desde cualquier parte del mundo, pueden afectar intereses de un Estado distinto de aquel en el que se realiza la acción, lo que provoca una serie de problemas como son los de la legislación y la jurisdicción aplicable al caso y las necesidades de cooperación para extradición internacional. A continuación se mencionan las principales:

- 1981: El Consejo de Europa abre a la firma el Convenio número 108, para la Protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, constituyéndose como el primer instrumento internacional que contiene un marco normativo respecto al tratamiento automatizado de los datos de carácter personal.
- 1985: La Organización de Cooperación y Desarrollo Económico (OCDE), publica una lista mínima de los delitos informáticos que los gobiernos signatarios podían incluir dentro de sus códigos penales, tales como; el fraude informático, el acceso ilícito a un sistema informático, la reproducción no autorizada de un programa de computadora, el sabotaje electrónico, el daño a los datos o a los programas informáticos, la interceptación no autorizada de datos, entre otros.
- 1990. El décimo tercer congreso internacional de la Academia de derecho comparado en Montreal Canadá y el Octavo Congreso Criminal de la ONU.
- 1992. Conferencia de Wuzburgo Alemania.
- 2000: En el marco del Décimo Congreso de las Naciones Unidas sobre Prevención del Delito y Tratamiento del Delincuente, celebrado cada cinco años desde 1955, se propone la formulación de políticas gubernamentales encaminadas a la prevención y control de los delitos informáticos, así como la mejora de las capacidades en cuanto a enjuiciamiento de los mismos.
- 2001: El Consejo de Europa preocupado por el riesgo que implica la criminalidad cibernética, abre a la firma el Convenio sobre la ciberdelincuencia también conocido como Convenio de Budapest; instrumento internacional que reconoce la necesidad de cooperación internacional en materia penal,

garantizando la tipificación como delito de los actos que ponen en peligro la confidencialidad, integridad y disponibilidad de los sistemas, redes y datos informáticos, así como el abuso de los mismos. En éste se establecen tres aspectos fundamentales. A) armonización de las normas penales sustantivas aplicables a las conductas delictivas que tienen como ámbito el entorno informático, B) Establecimiento de reglas procesales penales para facilitar la investigación de la criminalidad informática y C) la instrumentación de un sistema de cooperación internacional en el combate a estas conductas.

- 2006. Protocolo Adicional a la convención sobre cibercrimen en materia de racismo y xenofobia.
- 2014. Convenio Iberoamericano de cooperación sobre investigación, aseguramiento y obtención de prueba en materia de ciberdelicuencia.
- Proyecto de Convenio de Stanford.
- Ley modelo de Commonwealth sobre delitos informáticos y relacionados con la informática. (Besares, 2015, pp. 35-38).

El convenio de Budapest (Convenio de cibercriminalidad).

Debido a la acelerada evolución de la informática y la comisión de los delitos con empleo de éstos, los países Europeos mostraron su preocupación respecto al tema, por lo que, a efectos de ponerse acuerdos político penales básicos decidieron aprobar el “Convenio de cibercriminalidad de Budapest (Hungría)” el cual fue elaborado por el Consejo de Europa el noviembre del año 2001. Dicho convenio se promovió con miras a la prevención de la cibercriminalidad en el ciberespacio, especialmente por medio de una legislación adecuada y uniforme, de forma tal que las conductas sancionables sean pasibles de ser investigadas por cualquiera de los Estados miembro.

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

Al respecto, Broadhurst y Chang (2013) consideran que un problema clave en la persecución de los delitos informáticos es que todos los elementos del delito rara vez se encuentran en la misma jurisdicción. A menudo, el delincuente y la víctima e incluso las pruebas se encuentran en la jurisdicción diferente por lo que requiere un alto grado de cooperación entre las agencias de la ley para investigar y procesar. La Convención de Budapest de 2001, aprobada por el Consejo de Europa 2001, sobre el delito cibernético, es actualmente el único acuerdo multinacional que proporciona los medios para procesar a los delincuentes y representa un importante intento de regular el ciberespacio. Con el fin de armonizar la legislación y los procedimientos penales en los estados de Europa para el enjuiciamiento de los delincuentes cibernéticos. La iniciativa se remonta a 1989, cuando el Consejo de Europa publicó una serie de recomendaciones sobre la necesidad de que el derecho penal sustantivo para penalizar las conductas nocivas cometidos a través de redes informáticas. En 1997 el Consejo de Europa formó un Comité de Expertos sobre la delincuencia en el ciberespacio para redactar una convención para facilitar la cooperación de los Estados en la investigación y persecución de los delitos informáticos y para proporcionar una solución a los problemas de la delincuencia cibernética a través de la adopción de un instrumento jurídico internacional (p. 10).

Cabe resaltar que, de la citada convención se desprende que la parte procesal del mismo, tiene por objeto, permitir el enjuiciamiento de los delitos informáticos mediante el establecimiento de normas comunes de procedimiento y la adaptación de las medidas tradicionales de lucha contra la delincuencia para estos tipos de delitos.

Crimen organizado en la ciberdelincuencia.

Existe una creencia generalizada y acrítica que el Internet y la sociedad se han traído a su entorno a grupos del crimen organizado impulsadas por la mafia. Sin embargo, esta narrativa retórica no es apoyada por la investigación sobre la organización de los grupos de delincuencia en línea, el cual encuentra a la organización de la delincuencia en línea, el cual sigue una lógica distinta a la organización de la línea del crimen, una diferencia que también se refleja en las agrupaciones del crimen organizado. Tales hallazgos identifican en lugar de un

modelo “desorganizado” o distribuida de organización, en lugar de una estructura de mando y control jerárquico (Wall, 2015, p. 71).

Tipos de delitos informáticos.

La clasificación de los delitos informáticos son diversos, que en muchos casos hace referencia al mismo tipo delictivo pero con diferentes denominaciones, al respecto, Loredo y Ramírez (2013, pp. 45-46) citando a INTERPOL señalan como delitos informáticos los siguientes:

- Ataques contra sistemas y datos informáticos.
- Botnets (redes de equipos infectados controlados por usuarios remotos).
- Difusión de virus.
- Distribución de imágenes de agresiones sexuales contra menores.
- Estafas a través de Internet.
- Intrusión en servicios financieros en línea.
- Phishing (adquisición fraudulenta de información personal confidencial).
- Usurpación de la identidad.

Adicionalmente a ello, los mismos autores señalan que no son los únicos delitos informáticos, sino que también existen riesgos relacionados al uso de las redes sociales, así como el acceso a todo tipo de información, como:

- Acceso a material inadecuado (ilícito, violento, pornográfico, etc.).
- Acoso (pérdida de intimidad).
- Adicción - Procrastinación (distracciones para los usuarios).
- Ciberbullying (acoso entre menores por diversos medios: móvil, Internet, videojuegos, etc.).
- Cibergrooming (método utilizado por pederastas para contactar con niños y adolescentes en redes sociales o salas de chat).
- Problemas de socialización.
- Robos de identidad.
- Sexting (manejo de contenido erótico).

Tomando otro enfoque, en base a los tipos de delitos citados, se puede clasificar los tipos de delitos desde la perspectiva de los bienes jurídicos protegidos, en tal sentido la propuesta de clasificación son de acuerdo a los siguientes:

- Delitos informáticos contra el patrimonio.
- Delitos informáticos contra la persona.
- Delitos informáticos contra la fe pública.
- Delitos informáticos contra la seguridad.
- Delitos contra datos informáticos.
- Delitos contra sistemas informáticos.

En este orden de ideas, dentro de cada tipo de delito se puede identificar otros sub tipos de delitos, así, dentro de delitos informáticos contra el patrimonio se puede identificar al fraude, hurto, estada y sabotaje informático; dentro de los delitos informáticos contra la persona está contra la libertad sexual, en delitos informáticos contra la fe pública se encuentra la falsedad y sucesivamente.

Por otro lado, respecto a la clasificación de los delitos informáticos Lamperti (2017) señala que, existe consenso en reconocer una clasificación de los delitos informáticos que guarda sentido con la definición más útil, es así que se define a los delitos informáticos como conductas que a) ataca a las propias tecnologías de la computación y las comunicaciones; b) incluyen la utilización de tecnologías digitales en la comisión del delito; o c) incluyen la utilización incidental de las tecnologías en la comisión de otros delitos y, siendo que la computadora viene a ser una de las fuentes digitales probatorios. (p. 95).

Como se puede evidenciar, los tipos o la clasificación de los delitos informáticos son diversos y de acuerdo del punto de vista que se desea clasificar, por lo que es evidente que existe una falta de uniformidad teórica en la clasificación de estos delitos, el cual es inicio de un tratamiento jurídico deficiente, más aún un tratamiento legislativo deficiente en sentido estricto, pues si no se tiene clara la visión teórica menos habrá en la legislación.

Características de los delitos informáticos.

Entre las principales características de los delitos informáticos, haciendo referencia al maestro Valdés, y un recuento y algunas otras características que podemos identificar en los delitos informáticos, son las siguientes:

- Es de carácter internacional, por cuanto no es requisito la cercanía para la comisión de estos ilícitos.
- Es reducida el alcance de la justicia en estos ilícitos, puesto que son escasas y reducidas las denuncias, el alcance normativo, persecutor especializado y la regulación en el derecho penal internacional.
- Generalmente son dolosos o intencionales, aunque es posible que haya de carácter culposo.
- Generan cuantiosos y graves desfalcos económicos, puesto que generalmente se afectan grandes sumas de dinero o patrimonios.
- Presenta graves problemas en su demostración por su caracterización técnica especializada.
- Requiere un diminuto espacio y tiempo, debido a que estos ilícitos se pueden concretar en cuestión de segundos o con un clic, además no se requiere generalmente grandes aparatos ni maquinas informáticas, puesto que desde un teléfono móvil de bolsillo se puede concretar.
- Se trata de acciones de oportunidad, debido a que los delincuentes informáticos se benefician del acelerado avance tecnológico, y las víctimas abundan, más la ausencia de conocimientos especializados.
- Se trata de conductas ocupacionales, en la medida que las víctimas laboran con el uso de los medios informáticos, los delincuentes cibernéticos aprovechan para cometer sus actos criminales.
- Se trata de delito emergente, que va en aumento y cada vez más especializada y sofisticada.
- Se trata de delitos de cuello blanco, toda vez que el sujeto activo ha de ser una persona con un nivel de conocimiento de computación e informática.
- Se trata de ilícito muy rebuscado y frecuente en el dominio militar.
- Son conductas informáticas, debido a que necesariamente se requiere de un medio informático para la comisión del delito.

- Son delitos de complejo investigación, debido a que se requiere altos especialistas para corroborar e investigar.
- Son delitos especiales, debido a que se puede cometer delitos ya regulados como el hurto, estafa, fraude entre otros delitos, pero con el empleo de los medios informáticos, además que requiere una regulación especializada.

La informática forense.

La Informática forense nos permite la solución de problemas íntimamente ligados con seguridad informática y la protección de datos. Basados en ella, las diferentes empresas obtienen una respuesta oportuna para sobreponerse a los delitos informáticos consagrados en la ley tanto nacional como internacional; algunos de ellos son: de privacidad, robo de identidad, acceso no autorizado a cuentas de email o redes sociales, competencia desleal, fraude, robo de información confidencial y/o espionaje industrial surgidos a través de uso indebido de las tecnologías de la información (…) (Conedo, 2013, p. 82).

En este orden de ideas, se puede decir que la informática forense es una disciplina que ayuda a la justicia con el fin de enfrentar y descubrir los diferentes delitos informáticos que se pueden cometer, asimismo se encarga de la custodia de la evidencia digital recolectada en la escena del crimen para que ésta sea aportada en los procesos judiciales (Ramírez y Castro, 2018, p. 21).

El internet.

García y Peña (2017), citando a García (2013) señalan que el internet como medio de comunicación utilizado por los ciudadanos del mundo, ha dado lugar a múltiples tendencias, una de ellas es la proliferación como dijimos de conductas desviadas y delictivas donde los cibernautas se comunican en línea a todo nivel, sin embargo, diversos comportamientos están orientadas a ocasionar daño a cuantiosas empresas, personas, jóvenes y menores de edad que a menudo interactúan sin conocimiento o ingenuidad (García y Peña, 2017, p. 10).

La seguridad informática.

Bracho y otros (2017), citando a Toth (2014) señalan que la seguridad informática es el conjunto de políticas, reglas, estándares, métodos y protocolos que se

emplean para la protección de la infraestructura de computadoras y toda la información contenida o administrada por ella. En tal sentido consideran que no se debe prestar atención únicamente a los ataques intencionales que se realizan al sistema, sino también a las posibles fallas que el software o hardware pueda presentar y atentar contra la seguridad, de tal modo, se debe buscar minimizar los riesgos relativos al acceso y utilización de un determinado sistema de forma no autorizada o malintencionada, para revelar, utilizar, modificar o destruir accidental o intencionalmente la información que en este se encuentre (p. 308).

Prevención de delitos informáticos.

Respecto a la prevención de los delitos informáticos o cibernéticos (Neghina y Scarlat, 2013, p. 98) precisan que todos los métodos de prevención y análisis de seguridad deben partir de la idea de que se obtenga acceso no autorizado y de que se utilicen indebidamente los datos empresariales centrales, lo que generará la seguridad adecuada. Las medidas de clasificación de información crítica (evaluaciones de alto a bajo riesgo). Como resumen general de las revisiones de TI, no hay muchas entidades que implementen niveles de seguridad y clasificación de datos basados en valores o consideraciones de riesgo.

Congreso de las Naciones Unidas sobre Prevención del Delito y Tratamiento del Delincuente en La Habana, Cuba. En el año 2000, la Resolución 55/63 sobre la lucha contra el uso indebido e ilícito de tecnologías de la información fue adoptado por la Asamblea General, e incluye las siguientes afirmaciones (Levin y Ilkina. 2013, pp. 7- 8):

“Los Estados deben asegurar que sus leyes y prácticas a eliminar los refugios para los que las tecnologías de información criminal mal uso.”

"Los sistemas legales deben proteger la confidencialidad, la integridad y la disponibilidad de los datos y los sistemas informáticos del daño no autorizado y garantizar que se penalice el abuso criminal".

Delitos informáticos en el Perú.

El Perú, al igual que demás países no es excepción de la comisión de delitos informáticos, es así que “En el Perú la tecnología de comunicación e informática

ha desarrollado bastante, la misma que contribuye con el desarrollo de las personas y paralelo se han proliferado las conductas delictivas en el marco de la tecnología" (Cconislla, 2017, p. 52).

Antecedentes en el Perú.

El delito informático en un inicio se encontraba tipificado en el artículo 186, inciso 3, segundo párrafo del Código Penal de 1991. Esta regulación no era propia de un delito autónomo, sino como una agravante del delito de hurto. Posteriormente se reguló, los delitos informáticos en el Capítulo X del Código Penal, cuyos artículos 207-A (delito informático, uso e ingreso indebido de datos, sistema o red), 207-B (alteración, daño o destrucción de base de datos), 207-C (circunstancias cualificantes agravantes), 207-D (tráfico ilegal de datos).

Con la aprobación de leyes especiales, los artículos antes citados han sido derogados en octubre del 2013, dicha normativa fue la Ley 30096 (Ley de Delitos Informáticos). Esta Ley de Delitos Informáticos está conformada por siete capítulos que se estructuran de la siguiente manera: finalidad y objeto de la ley (Capítulo I), delitos contra datos y sistemas informáticos (Capítulo II), delitos informáticos contra la indemnidad y libertad sexual (Capítulo III), delitos informáticos contra la intimidad y el secreto de las comunicaciones (Capítulo IV), delitos informáticos contra el patrimonio (Capítulo V), delitos informáticos contra la fe pública (Capítulo VI) y las disposiciones comunes (Capítulo VII).

Posteriormente se promulgó la Ley 30171 (Ley que modifica la Ley 30096, Ley de Delitos Informáticos). La finalidad de esta ley fue adecuar la Ley 30096 a los estándares legales del convenio sobre la cibercriminalidad (Convenio de Budapest), al incorporar en la redacción típica de los artículos 2, 3, 4, 7, 8 y 10 de la referida Ley la posibilidad de cometer el delito deliberada e ilegítimamente. (Villavicencio, 2014, p. 287).

En consecuencia, las principales normas en el Perú sobre la ciberdelincuencia o delitos informáticos, son las citadas y las normas complementaria que se citan a continuación.

Legislación.

Decreto Legislativo Nº 635 (Código Penal).

Ley Nº 30096 (Ley de Delitos Informáticos).

Ley Nº 30171 (Ley que modifica la Ley 30096, Ley de Delitos Informáticos).

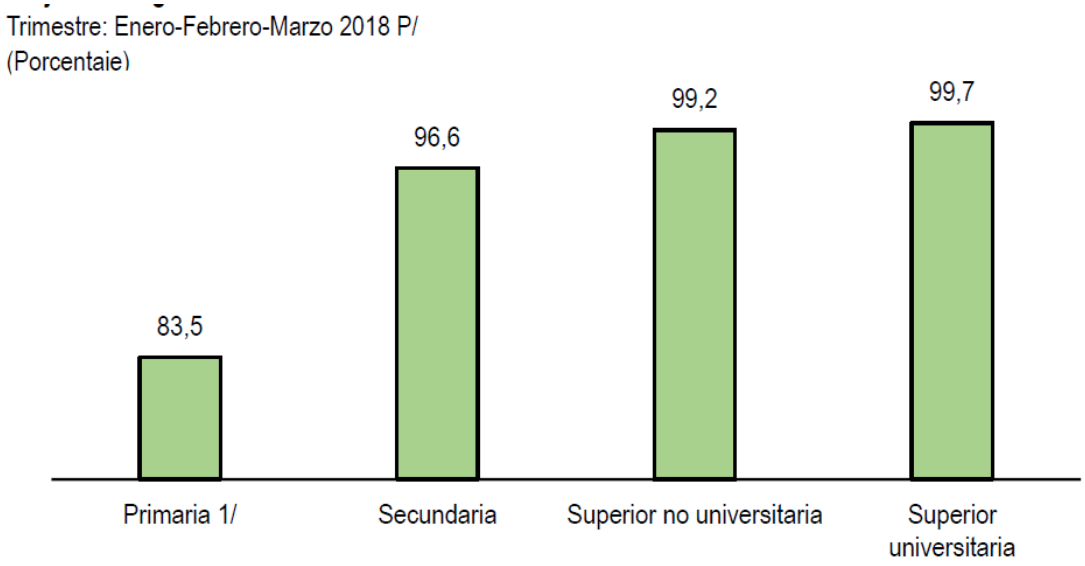
Decreto Legislativo Nº 1182 (Decreto Legislativo que regula el uso de los datos derivados de las telecomunicaciones para la identificación, localización y geolocalización de equipos de comunicación, en la lucha contra la delincuencia y el crimen organizado).

Decreto Legislativo Nº 1237 (Decreto Legislativo que modifica el Código Penal, aprobado por el Decreto Legislativo Nº 635).

Ley Nº 28493, Ley que regula el uso del correo electrónico comercial no solicitado (SPAM) y su reglamento D.S. Nº 031-2005-MTC.

Estadísticas del cibercrimen o delitos informáticos en el Perú.

Antes de abordar la estadística sobre la comisión de los delitos informáticos en el Perú cabe resaltar en primer lugar, el acceso que la población tiene a las tecnologías de información, debido que se trata de un factor muy importante, puesto que a mayor cantidad de usuarios, habrá mayor posibilidad de comisión de los delitos informáticos, así como la vulnerabilidad de los usuarios será de acuerdo a la formación y las especializaciones que pueda tener. Así, respecto a los hogares con acceso a las tecnologías de información en el trimestre enero a marzo del 2018 se puede apreciar lo siguiente:



1/ Incluye sin nivel e inicial. A partir del 2017, se incluye nivel básica especial.
P/ Preliminar.
Fuente: Instituto Nacional de Estadística e Informática - Encuesta Nacional de Hogares.

Figura 1: *Hogares que acceden a las Tecnologías de Información y Comunicación, según nivel de educación del jefe del hogar*

En el gráfico se observa que "El acceso a alguna Tecnología de Información y Comunicación, es casi universal en hogares cuyo jefe tiene educación superior. Así, 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%" (INEI, 2018, p. 2).

En este sentido, habiendo una población casi global que tiene acceso a las tecnologías de información, los delitos informáticos en el Perú ha ido evolucionando, por lo que se requiere nuevas normas para sancionar los actos criminales con el uso de la informática, en tal sentido, para efectos de la presente investigación de solicitó información estadística al Instituto Nacional de Estadística e Informática, en el cual, respecto a los otros delitos contra el patrimonio (Donde se encuentra delitos informáticos) ingresados a las fiscalías provinciales penales y mixtas, según distrito fiscal, periodo 2012 – 2016, se tiene lo siguiente:

Tabla 1:

Otros delitos contra el patrimonio ingresados en las Fiscalías Provinciales Penales y mixtas, según Distrito Fiscal, 2012-2016

OTROS DELITOS CONTRA EL PATRIMONIO INGRESADOS EN LAS FISCALÍAS PROVINCIALES PENALES Y MIXTAS, SEGÚN DISTRITO FISCAL, 2012-2016

Distrito fiscal	OTROS c/				
	2012	2013	2014	2015	2016
Total a/	**21.480**	**25.064**	**32.896**	**25.421**	**26.565**
Amazonas	**471**	470	402	324	556
Áncash	**105**	175	202	351	217
Apurímac	**56**	77	74	71	144
Arequipa	**1.113**	1.111	1.723	2.102	2.016
Ayacucho	**303**	284	556	260	623
Cajamarca	**387**	297	263	333	320
Callao	**601**	669	843	644	557
Cañete	**451**	1.248	1.384	678	1.448
Cusco	**565**	589	2.637	1.825	2.329
Huancavelica	**36**	51	74	35	42
Huánuco	**258**	595	1.427	603	375
Huaura	**436**	535	461	292	313
Ica	**579**	820	719	685	654
Junín	**608**	455	752	360	313
La Libertad	**1.188**	1.705	2.462	778	812
Lambayeque	**3.185**	4.179	4.397	4.617	5.177
Lima b/	**5.101**	5.388	5.669	4.997	3.842
Lima Norte	**894**	935	365	1.011	861
Lima Sur	**509**	524	434	405	400
Loreto	**290**	276	1.078	304	303
Madre de Dios	**524**	338	290	432	668
Moquegua	**206**	290	416	293	392
Pasco	**84**	64	102	92	82
Piura	**1.157**	1.865	2.058	2.155	2.263
Puno	**328**	244	151	181	245
San Martín	**528**	254	1.251	193	195
Santa	**502**	485	673	492	419
Sullana	**440**	457	523	286	383
Tacna	**145**	197	298	222	207
Tumbes	**220**	277	329	143	153
Ucayali	**210**	210	883	257	256

Fecha de corte de información: 31/12/2016

Nota: Las cifras corresponden al número de presuntos delitos registrados en el Ministerio Público, exclusivamente en las bases de datos interconectadas (SIATF y SGF). Las cifras no se refieren al número de casos ni al número de denuncias, ya que un único caso puede estar referido a uno o más delitos. Tampoco se puede equiparar el número de delitos al número total de imputados o detenidos porque puede ocurrir que un único caso tenga más de un imputado o detenido. Asimismo, los datos corresponden a todos los delitos sin discriminar la situación jurídica o el estado de las investigaciones. Los datos han sido generados por el Sistema Inteligente para el Análisis del Delito y la Violencia (SIADEV) y corresponden sólo a la información disponible de las sedes interconectadas integrada por la Oficina de Sistemas y tiene carácter preliminar, no oficial.

a/ Las variaciones registradas en las sumas torales de los datos registrados, se debe a la integración de la información de las sedes no conectadas.

b/ Distrito fiscal de Lima incluye al distrito fiscal de Lima Este-

c/ En la categoria otros se incorpora los delitos contra la apropiación ilícita, delitos informáticos, fraude en la administración de persona jurídica, abigeo y receptación.

Fuente: Ministerio Público - Sistema de Información de Apoyo al Trabajo Fiscal (SIATF) y Sistema de Gestión Fiscal (SGF)

Elaboración: Instituto Nacional de Estadística e Informática

Como se observa en la tabla, respeto a los otros delitos contra el patrimonio (Donde se encuentra delitos informáticos) en el año 2012 se registraron 21,480 casos el cual ascendió para el 2016 a 26,565 casos registrados, siendo el distrito fiscal con mayor casos registrados, el distrito fiscal de Lima.

Asimismo, se solicitó información respecto a la cantidad de personas detenidas según el tipo de delito para el periodo comprendido 2008 – 2016, en el cual se presenta la siguiente información:

Tabla 2:
Personas detenidas por cometer delito, según tipo de delito, 2008 - 2016

PERSONAS DETENIDAS POR COMETER DELITO, SEGÚN TIPO DE DELITO, 2008 - 2016

(Casos registrados)

Tipo de infracción	2008	2009	2010	2011	2012	2013	2014	2015	2016
Total	**60 053**	**66 331**	**75 412**	**74 597**	**92 868**	**91 698**	**95 265**	**96 698**	**111 233**
Contra la vida, el cuerpo y la salud	**5 355**	**5 617**	**5 664**	**5 247**	**6 361**	**6 857**	**5 488**	**5 943**	**6453**
Homicidio	1 162	1 168	823	862	1 047	1 052	1 029	1 168	1203
Aborto	267	110	67	109	52	38	56	76	62
Lesiones	3 834	4 275	4 701	4 178	4 903	5 427	3 848	3 991	4999
Otros 1/	92	64	73	98	359	340	555	708	189
Contra la familia y la persona	**1 877**	**2 058**	**2 967**	**1 682**	**2 069**	**2 376**	**1 838**	**1 980**	**2750**
Atentado contra la Patria Potestad	115	120	143	97	103	184	268	275	243
Omisión de asistencia familiar	1 549	1 873	2 765	1 454	1 781	1 931	1 213	1 218	1888
Matrimonio ilegal	20	34	17	111	132	79	147	285	254
Contra el estado civil	193	31	42	20	53	182	210	202	365
Contra la libertad	**5 038**	**4 508**	**3 472**	**3 652**	**4 246**	**3 869**	**4 345**	**4 659**	**4935**
Violación a la libertad personal	491	578	462	448	491	509	574	530	692
Violación a la intimidad	97	52	22	23	29	25	25	29	39
Violación de domicilio	131	189	278	144	142	142	174	254	270
Violación a la libertad sexual	3 434	3 073	2 250	2 355	2 674	2 403	2 293	3 390	3485
Proxenetismo	342	144	94	143	185	74	161	204	161
Ofensa al pudor público	257	303	151	69	70	43	78	69	88
Otros 2/	286	169	215	470	655	673	1 040	183	200
Contra el patrimonio	**24 695**	**29 133**	**29 942**	**29 187**	**30 804**	**30 622**	**29 373**	**29 148**	**32 480**
Hurto	9 665	10 475	10 350	10 878	12 136	11 826	12 207	12 570	15138
Robo	12 517	16 329	16 143	15 227	15 857	15 926	13 449	12 817	13461
Apropiación ilícita	353	297	375	280	186	218	227	110	379
Estafas y otras defraudaciones	775	707	735	776	600	117	102	587	102
Abigeato	518	503	783	590	299	509	574	319	463
Fraude en la Administración	17	31	43	19	18	17	17	14	10
Daños simples y agravados	148	145	209	103	178	8	-	162	58
Delitos Informáticos	-	-	-	-	7	201	181	29	225

Otros 3/	702	646	1 304	1 314	1 523	1 800	2 616	2 540	2644
Contra el orden económico	**188**	**145**	**81**	**57**	**54**	**25**	**30**	**46**	**230**
Acaparamiento, especulac.y adulteración	89	46	25	8	5	3	4	6	179
Negociación de bienes destinados a donac.	-	-	-	-	-	1	-	4	1
Función ilegal de casinos de juego	-	-	-	-	1	-	4	4	14
Lucro indebido en importaciones	-	-	-	-	2	3	-	-	4
Otros 4/	99	99	56	49	46	18	22	32	32
Contra el orden financiero	-	-	-	**267**	**368**	**323**	**311**	**386**	**424**
Delito financiero	**-**	**-**	**-**	22	22	18	26	30	152
Delito monetario	**-**	**-**	**-**	245	346	305	285	356	272
Contra el delito tributario	**215**	**131**	**116**	**123**	**210**	**158**	**198**	**240**	**258**
Contrabando	186	121	85	102	169	130	143	154	218
Elaboración clandestina de productos	-	-	-	21	41	28	55	86	40
Otros	29	10	31	-	-	-	-	-	-
Contra la fe pública	**574**	**525**	**676**	**699**	**1 142**	**1 089**	**952**	**729**	768
Falsificación de documentos en general	442	376	482	480	877	924	711	575	531
Falsificación/sellos,timbres-marcas oficina	-	-	-	23	64	13	16	13	18
Otros 5/	132	149	194	196	201	152	225	141	219
Contra la seguridad pública	**13 393**	**13 452**	**18 403**	**21 409**	**32 561**	**33 792**	**38 935**	**40 140**	**47 281**
Peligro común	-	-	-	7 727	15 802	21 123	25 083	25 192	33256
Tráfico ilícito de droga	2 372	2 504	3 557	3 338	3 120	2 542	2 623	2 951	3851
Microcomercialización de droga	7 030	6 808	6 625	6 824	9 803	6 652	7 743	8 690	6757
Tenencia ilegal de armas	-	-	-	1 972	1 921	1 976	2 384	2 158	2094
Otros 6/	3 991	4 140	8 221	1 548	1 915	1 499	1 102	1 149	1323
Contra la tranquilidad pública	**955**	**1 201**	**1 014**	**646**	**1 048**	**529**	**796**	**493**	**376**
Terrorismo - Apología	103	77	121	202	198	110	135	93	26
Otros 7/	852	1 124	893	444	850	419	661	400	350
Contra la humanidad	**-**	**5**	**7**	**-**	**-**	**-**	**-**	**-**	-
Desaparición forzada	-	5	1	-	-	-	-	-	-
Otros	-	-	6	-	-	-	-	-	-
Contra la administración pública	**760**	**822**	**1 276**	**1 423**	**1 936**	**2 132**	**2 847**	**3 276**	**3 226**
Cometidos por particulares	-	660	1 067	1 336	1 589	1 664	2 333	2 464	2796
Cometidos por Funcionarios Públicos	-	83	146	58	140	137	244	155	119
Contra la Administración de Justicia	-	79	63	29	207	331	270	657	311
Delitos agravados	**106**	**206**	**-**	**-**	**-**	**-**	**-**		
Contra el pandillaje pernicioso	**638**	**848**	**652**	**1 862**	**1 638**	**448**	**286**	**128**	216
Posesión de arma de guerra	**129**	**129**	**49**	**32**	**15**	**32**	**26**	**54**	44
Otros delitos (*)	**6 130**	**7 551**	**11 093**	**8 311**	**10 416**	**9 446**	**9 840**	**9 476**	11792

(1) Exponer al peligro o abandono de personas en peligro.

(2) Violación al secreto comunicación y secreto profesional, violación a la libertad de reunión, trabajo y violación a la libertad de expresión.

(3) Receptación, usurpación y extorsión.

(4) Abuso poder económico y venta ilícita de mercaderías.

(5) Falsificación en general, posesión de instrumentos de falsificación.

(6) Peligro común, d. c/medio de transporte, comunicación y otros servicios públicos, y contra la salud pública.

(7) Contra la paz pública (disturbio colectivo, apología y organización criminal).

(*):Contra el honor, c/confianza y buena fe, negocio, c/derechos intelectuales, c/patrimonio cultural, c/ecología, c/orden financiero y monetario, c/el Estado y Defensa Nacional, c/Poderes del Estado y Orden Constitucional, y c/voluntad popular.

Fuente: Ministerio del Interior - MININTER - Dirección de Gestión en Tecnología de la Información y Comunicaciones.

En la información presentada, relativo a los delitos contra el patrimonio, especialmente delitos contra el patrimonio, en el año 2008, 2009, 2010 y 2011 no

se registró ningún caso, que se haya detenido a una persona por delitos informáticos contra el patrimonio, posterior a ello, en el año 2012 se detuvieron a 7 personas; en el año 2013 se detuvieron a 201 personas; año 2014 181 personas; año 2015 a 29 personas y en el 2016 se detuvieron a 225 personas por delito informáticos contra el patrimonio.

En comparación del año 2008 hasta el 2016 consideramos que hay un pequeño avance en las acciones contra los delitos informáticos contra el patrimonio, sin embargo, estas cifras muestran la debilidad del sistema jurídico penal para la detección, prevención y sanción de los delitos informáticos, puesto que las cifras de las personas detenidas no concuerda razonablemente con la cantidad total de otros tipos de delitos contra el patrimonio cometidos en los periodos comparados, conforme a las cifras de casos registrados en el fuente estadístico anterior.

DELITOS REGISTRADOS EN FISCALÍAS PROVINCIALES PENALES Y MIXTAS SEGÚN TIPO DE DELITO SUB GENÉRICO A NIVEL NACIONAL - LEY Nº 30096, LEY DE DELITOS INFORMÁTICOS ENERO A DICIEMBRE 2016 - 2017

DELITOS SUB GENÉRICOS	2016 ENERO - DICIEMBRE		2017 ENERO - DICIEMBRE	
	N° DELITOS	%	N° DELITOS	%
LEY Nº 30096, LEY DE DELITOS INFORMÁTICOS				
DELITOS INFORMÁTICOS CONTRA EL PATRIMONIO	189	20.17	778	30.75
DELITOS INFORMÁTICOS CONTRA LA FE PUBLICA	44	4.70	112	4.43
DELITOS CONTRA DATOS Y SISTEMAS INFORMÁTICOS	33	3.52	105	4.15
DELITOS INFORMÁTICOS CONTRA LA INDEMNIDAD Y LIBERTAD SEXUALES	31	3.31	59	2.33
DELITOS INFORMÁTICOS CONTRA LA INTIMIDAD Y EL SECRETO DE LAS COMUNICACIONES	21	2.24	44	1.74
DISPOSICIONES COMUNES	6	0.64	33	1.30
SIN ESPECIFICAR DELITO SUB GENÉRICO	613	65.42	1,399	55.30
TOTAL	937	100.00	2,530	100.00

FUENTE: Sistema de Información al Trabajo Fiscal - SIATF y Sistema de Gestión Fiscal - SGF
ELABORADO: Oficina de Racionalización y Estadística - ORACE

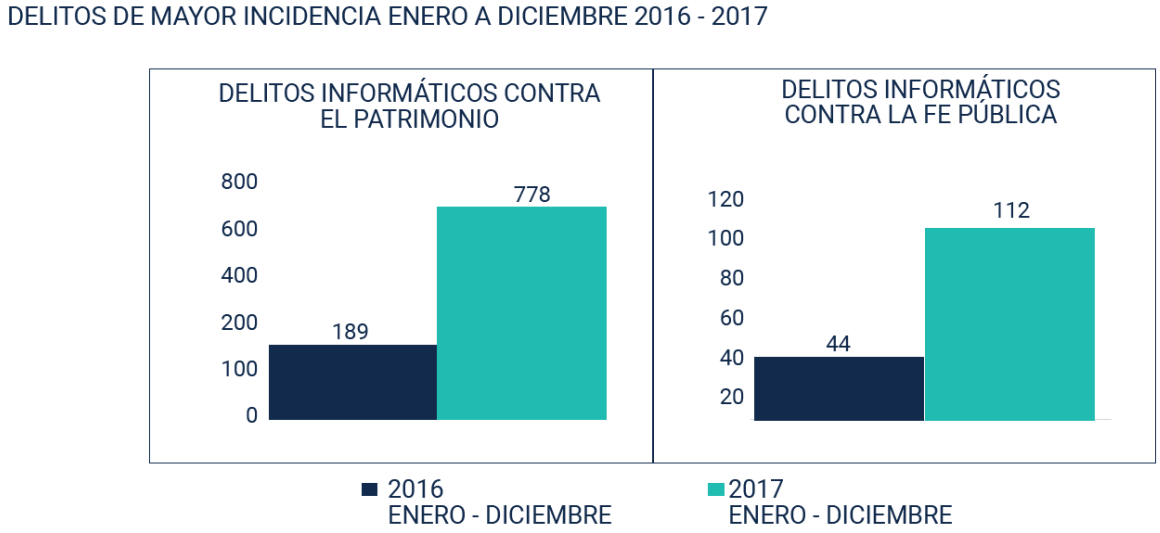
Fuente: Boletín estadísticos del Ministerio Público (diciembre de 2017).

Figura 2:

Delitos registrados en Fiscalías Provinciales Penales y Mixtas según tipo de delito sub genérico a nivel Nacional – Ley Nº 30096, Ley de Delitos Informáticos Enero a Diciembre 2016 – 2017.

En el periodo comprendido de enero a diciembre del 2016, el (20,17%) del total de los delitos informáticos registrados a nivel nacional, fueron los delitos informáticos contra el patrimonio, el cual se traduce en 189 casos de este delito. Dicha cifra aumentó considerablemente para el periodo enero a diciembre del año 2017, donde el (30,75%) del total de los delitos informáticos registrados a nivel nacional, fueron los delitos informáticos contra el patrimonio, el cual, a diferencia el periodo anterior, está representada por 778 casos.

Si comparamos los delitos informáticos contra el patrimonio contra otro delito informático, podemos apreciar lo siguiente:



Fuente: Boletín estadísticos del Ministerio Público (diciembre de 2017).

Figura 3:
Delitos de mayor incidencia Enero a Diciembre 2016 – 2017.

En el periodo enero a diciembre del año 2016, los delitos informáticos contra el patrimonio (189 casos) fueron los ilícitos más cometidos a diferencia de los delitos informáticos contra la fe pública (44 casos). Lo mismo ocurre en el periodo enero a diciembre de 2017, los delitos informáticos contra el patrimonio registra 778 casos, mientras los delitos informáticos contra la fe pública registra 112 casos.

Por otro lado, de acuerdo al boletín estadístico de enero de 2018, el Ministerio Público, señala que en el mes de enero del año 2017 hubieron 62 (22,96%) delitos contra el patrimonio cometidos, en comparación a ello, en enero

del 2018 se evidencia que aumentó a 116 casos que se traduce en el (42,18%) de delitos informáticos son contra el patrimonio, siendo este último el de mayor incidencia de todo los demás modalidades de delitos informáticos. Similar ascendencia tuvo en el mes de febrero de 2018.

Por otro lado, en el periodo correspondiente a marzo de 2018, se detalla lo siguiente:

DELITOS SUB GENÉRICOS	2017 MARZO		2018 MARZO	
	N° DELITOS	%	N° DELITOS	%
LEY N° 30096, LEY DE DELITOS INFORMÁTICOS				
DELITOS INFORMÁTICOS CONTRA EL PATRIMONIO	101	23.39	216	40.07
DELITOS INFORMÁTICOS CONTRA LA INDEMNIDAD Y LIBERTAD SEXUALES	13	3.01	20	3.71
DELITOS INFORMÁTICOS CONTRA LA FE PÚBLICA	16	3.70	16	2.97
DELITOS CONTRA DATOS Y SISTEMAS INFORMÁTICOS	12	2.78	14	2.60
DELITOS INFORMÁTICOS CONTRA LA INTIMIDAD Y EL SECRETO DE LAS COMUNICACIONES	7	1.62	9	1.67
DISPOSICIONES COMUNES	3	0.69	6	1.11
SIN ESPECIFICAR DELITO SUB GENÉRICO	280	64.81	258	47.87
TOTAL	432	100.00	539	100.00

NOTA: Delitos registrados a través de denuncias penales, no se incluyen denuncias en estado de derivación, acumulados ni cuadernos.

FUENTE: Sistema de Información al Trabajo Fiscal - SIATF y Sistema de Gestión Fiscal - SGF
ELABORADO: Oficina de Racionalización y Estadística - ORACE

Fuente: Boletín estadísticos del Ministerio Público (Marzo 2018).

Figura 4:

Delitos registrados en fiscalías provinciales penales y mixtas según tipo de delito sub genérico a nivel nacional - Ley Nº 30096, ley de delitos informáticos Marzo 2017 - Marzo 2018.

En el grafico se observa que en l mes de marzo de 2017 se registraros 101 casos de delitos informáticos contra el patrimonio, mientras en marzo de 2018 los casos registrados son más de doble, siendo 2016 casos en específico, asimismo cabe resaltar que en el año 2017 los delitos informáticos contra el patrimonio representaban el 23,39% de la totalidad de los delitos informáticos, sin embargo,

en marzo de 2018 representa el 40,07% del total de los delitos informáticos, siendo éste un delito de mayor incidencia de los demás modalidades de delitos informáticos actualmente sancionados.

Tipos de delincuentes informáticos.

López, López y Yedra (2017) señalaron que al igual que existen una gran cantidad de delitos informáticos, también existen una amplia gama de delincuentes informáticos, en la informática se le conoce a los expertos en seguridad informática con el término de “hacker”, que hace referencia, como se señaló, a la persona que usa su habilidad para obtener acceso sin autorización a los archivos informáticos o redes, esta definición, de hecho, es asociada a la conducta delictiva, sin embargo debemos tener en cuenta que existe una clasificación de los hackers, la primera es el hacker de sobrero blanco y el segundo es el hacker de sombrero negro.

Conforme al citado autor, los *White hat hacker (*Hackers de sombrero blanco)*:* se dedican a buscar vulnerabilidades en redes y sistemas sin realizar un uso malicioso de estas y posteriormente reportando los fallos. Las formas en que se monetiza esta actividad son varias: se busca reputación en el sector, sistema de recompensas, trabajando como consultor o responsable de seguridad en una compañía; mientras los *Black hat Hacker* (Hackers de sombrero negro) *son* individuos con amplios conocimientos informáticos que buscan romper la seguridad de un sistema buscando una ganancia, ya se obtener bases de datos para su posterior venta en el mercado negro, venta de “xploits” (vulnerabilidades de seguridad), robo de identidad, cuentas bancarias, etc. otro tipo de delincuentes que son aquellos que hacen uso del anonimato en internet con el fin de realizar conductas poco éticas: acoso cyberbullying, estafas, pornografía infantil, turismo sexual, etc. (López, López y Jerónimo, 2017, p. 7).

Sin embargo, recurriendo a los expertos informáticos Aggarwal, Arora, Ghai y Poonam (2014, p. 49) podemos encontrar una variedad de tipos de hackers, tales como:

Script Kiddies.

Estos son los piratas aspirantes que quieren ser hacker o se adelgaza que son pero carecen de los conocimientos técnicos avanzados. Ellos sólo son capaces de hackear los sistemas débilmente garantizados. Ellos no pueden causar ningún daño serio a las víctimas.

Los estafadores (Scammers).

Estos hackers envían los correos electrónicos falsos para las víctimas como productos farmacéuticos de descuento, premios de lotería, el fraude de tiempo compartido a través del cual son capaces de acceder al sistema de la víctima y corrompe por completo.

Grupos de hackers (Hacker Groups).

Estos hackers trabajan de forma anónima y piratear ordenadores por razones no criminales. Ellos son contratados por las organizaciones, agencias gubernamentales, etc., para poner a prueba la seguridad y manejar los casos de fraude.

Los suplantadores de identidad (Phishers).

Se solicita información confidencial a través de Internet de manera fraudulenta con el fin de obtener fraudulentamente números de tarjetas de crédito, contraseñas u otros datos personales. *Phishing* normalmente se lleva a cabo por la suplantación de correo electrónico o de mensajería instantánea y que a menudo dirige a los usuarios a entrar en detalles en una página web falsa cuyo aspecto y el tacto son casi idéntica a la legítima.

Grupos comerciales, políticas y religiosas.

Estos hackers no están interesados en la ganancia financiera, sino que se dedican a desarrollar software malicioso para fines políticos. Ellos tratan de obtener acceso de la confidencialidad de la información de los grupos oponentes. El gusano *Stuxnet* que atacó el programa atómico de Irán de sus instalaciones nucleares se cree que fue creado por un gobierno extranjero.

Insiders.

Estos atacantes son considerados como los de más alto riesgo, ya que residen dentro de la organización. Ellos tienen el conocimiento de todos los detalles de una organización y atacan fácilmente la seguridad de la empresa y hacen y deshacen el sistema.

Amenaza persistente avanzada (APT) Agentes (Advanced Persistent Threat (APT) Agents)

Este grupo de hackers es responsable de ataques muy concretas llevadas a cabo por grupos patrocinados por Estados extremadamente organizados. Sus habilidades técnicas son profundas y tienen acceso a grandes recursos de computación. Se refiere a un grupo, tal como un gobierno, tanto con la capacidad y la intención de manera persistente y eficazmente objetivo a una entidad específica.

Hackers sombrero blanco (White Hat Hackers).

Se hace referencia a los hackers éticos que por lo general se centran en la obtención de los sistemas de TI. El término hacker de sombrero blanco también se utiliza a menudo para describir a aquellos que tratan de irrumpir en los sistemas o redes con el fin de ayudar a los propietarios del sistema, haciéndolos conscientes de las fallas de seguridad. Muchas de estas personas son empleados de empresas de seguridad informática.

Hackers sombrero negro (Black Hat Hackers).

Un hacker de sombrero es una persona que compromete la seguridad de un sistema informático sin el permiso o autorización del titular, por lo general con malas intenciones. Estos hackers utilizan sus conocimientos para explotar los sistemas para la ganancia privada. Se aprovechan de robo y resultados en la destrucción de los archivos seguros y robar la información.

Hackers de sombrero gris (Grey Hat Hackers).

Un hacker de sombrero gris en la comunidad de seguridad informática, se refiere a un hacker experto que a veces actúa legalmente, a veces de buena voluntad, ya

veces no. Son un híbrido entre hackers de sombrero blanco y negro. Por lo general no piratear para beneficio personal o tienen intenciones maliciosas, pero pueden o no pueden cometer crímenes, de vez en cuando durante el transcurso de sus hazañas tecnológicas.

Análisis del tipo penal de delitos informáticos contra el patrimonio.

Tipicidad objetiva.

Conducta típica.

La conducta típica en los delitos informáticos contra el patrimonio viene a ser la vulneración de la seguridad de los sistemas informáticos para el aprovechamiento indebido, ya sea sustrayendo bienes, valores, datos, programes. Asimismo es conducta típica el uso de las tecnologías informáticas para inducir en error a las personas con fines de aprovechamiento indebido, así como los acatos de destrucción, borrado, alteración de bases de datos, bienes, sistemas y cualquier pieza y sistema informático con el fin de perjudicar o reducir la competitividad de una persona o empresa, para provecho propio o de terceros.

Sujeto activos.

A los delitos informáticos se le denomina delitos de cuello blanco, debido a la característica especial que el sujeto activo posee, el cual es el conocimiento avanzado de las tecnologías informáticas, puesto que es casi imposible que cualquier persona pueda cometer el delito, si tener conocimientos suficientes de cómo funcionan los sistemas informáticos, más cuando se trata de vulnerar las medidas de seguridad implementadas contra piratas informáticos.

Sujeto pasivo.

El sujeto pasivo en el caso de los delitos informáticos puede ser individuos, instituciones crediticias, órganos estatales, etc. que utilicen sistemas automatizados de información, generalmente conectados a otros equipos o sistemas externos. (Alcívar, Domenech y Ortiz, 2015, p. 46).

Bien jurídico protegido.

(Mayer, 2017) en forma general considera que el bien jurídico protegido en los delitos informáticos es la información, es la contenida en un sistema de tratamiento automatizado de la misma, “en cuanto tal”, resulta difícilmente conciliable con una definición del interés protegido que apunte al libre desarrollo de la persona en un Estado democrático de derecho (p. 240).

Sin embargo, podemos afirmar que no solo la información contenida en los sistemas informáticos o automatizados son los bienes jurídicos protegidos, sino también diferentes, como es la fe pública, la seguridad de los sistemas, la imagen, libertad personal, privacidad, el patrimonio entre otros.

En este orden de ideas, en específico, en los delitos informáticos contra el patrimonio, el bien jurídico protegido es propiamente el patrimonio, tales como dinero electrónico, valores, fondos de cuentas, softwares, entre otros, puesto que éstos forman parte del patrimonio del sujeto pasivo, cabe resaltar que para considerar patrimonio no necesariamente los bienes tienen que ser físicos, sino también lo son las digitales o electrónicos, por ejemplo si a una persona le sustraen de la nube una base de datos de una aplicación que ha estado desarrollando años o meses, para un proyecto grande, donde invirtió tiempo y dinero, pues la sustracción de dicha base de datos constituye patrimonio del sujeto pasivo, el cual es similar que se sustraigan a una fábrica de coches un vehículo de último modelo que acababa de culminar y estuvo para la primera exhibición.

Tipicidad subjetiva.

Los delitos informáticos, por su naturaleza y el nivel de conocimiento que requiere, son delitos netamente dolosos, sin embargo también se podría concretar por culpa o por descuido, en la que no te tenía ninguna intención de la comisión del ilícito, sin embargo vulnera el bien jurídico penalmente protegido.

Móvil o motivo de los delincuentes informáticos.

Las motivaciones que pueda provocar delinquir a los cibercriminales son diversas, los mismos que pueden tener carácter económico y otros de carácter no

económico. Los delitos informáticos contra el patrimonio se caracteriza por tener motivaciones económicas para su comisión (Hurto, fraude, sabotaje y estafa), sin embargo el sabotaje podría no ser con fines de aprovechamiento económico directo, por generar pérdidas en el sujeto pasivo más no provecho directo del sujeto activo, pero si el sabotaje es para reducir la competitividad de una empresa de competencia, entonces, tiene carácter patrimonial, puesto que dicho sabotaje se habría cometido para que la otra empresa repunte en el mercado del rubro.

Otra de las motivaciones que podemos encontrar en los cibercriminales, como refiere también Han y Dongre (2014), son también por aspectos políticos (motivaciones políticas), donde se busca destruir, alterar o tomar el control de los objetivos, espionaje, o incluso hacer declaraciones políticas, ejercer represalia a grupos y realizar protestas.

Otra de las terceras motivaciones que encontramos es nada menos que en aspecto socio culturales (motivación sociocultural), en la que los delitos cibernéticos se cometen con fines filosófico, teológicos, así como por diversión, curiosidad e incluso por mostrar la superioridad o gratificaciones de ego.

Delitos informáticos contra el patrimonio.

La piratería de software.

Citando a Aggarwal, Arora, Ghai y Poonam (2014) podemos señalar que la piratería informática es el aprovechamiento indebido del software a través de la copia ilegal de programas y distribución de los productos destinados al pase a la original genuinos. Esto se puede hacer mediante la copia del usuario final, la carga de disco duro, la falsificación, las descargas ilegales de internet entre otros (p. 49).

Delitos informáticos objeto de estudio.

Los delitos informáticos materia de estudio son los delitos informáticos contra el patrimonio, en la modalidad de hurto, fraude, estafa y sabotaje.

Hurto informático.

La apropiación o hurto de software y datos: en este caso el sujeto accede a un computador ajeno o a la sesión de otro usuario, retirando archivos informáticos, mediante la ejecución de los comandos copiar o cortar, para luego guardar ese contenido en un soporte propio. (Alcívar, Domenech y Ortiz, 2015, p. 45).

No hay que olvidar que los avances tecnológicos y el empleo de los mismos para apropiarse ilícitamente del patrimonio de terceros a través de clonación de tarjetas bancarias, vulneración y alteración de los sistemas de cómputo para recibir servicios y transferencias electrónicas de fondos mediante manipulación de programas y afectación de los cajeros automáticos, entre otras, son conductas cada vez más usuales en todas partes del mundo y en nuestro país (…) (Conedo, 2013, p. 83).

Rodríguez (2013) señala que dentro de los actos que afectan al soporte físico (hardware) o al lógico (software) se encuentran los delitos contra la propiedad como es el daño al hardware o software, puesto que se trata de apoderamiento furtivo de estos elementos que integran el sistema informático, hurto, o robo, de acuerdo a la tipificación del acto jurídico que realiza el Código Penal (p. 110).

Los sistemas electrónicos de transferencia de fondos han comenzado a proliferar, y también el riesgo de que tales transacciones puedan ser interceptadas y desviadas. Los números válidos de tarjetas de crédito pueden ser interceptados electrónicamente, así como físicamente; la información digital almacenada en una tarjeta puede ser falsificada. Del mismo modo que un ladrón armado puede robar un automóvil para facilitar una escapada rápida, también puede uno robar servicios de telecomunicaciones y utilizarlos con fines de vandalismo, fraude o fomento de una conspiración criminal. Los delitos informáticos pueden ser de naturaleza compleja, combinando dos o más de las formas genéricas descritas anteriormente (Das, Nayak, 2013, p. 147).

Hurto sistemáticos

Constituye hurto sistemático la sustracción continua de patrimonio de una persona por medio de sistemas informáticos, como es el caso de las cuentas bancarias, donde el delincuente, al obtener las claves de seguridad de las tarjetas de crédito o débito, en forma periódica y continua extrae los ahorros o los montos que se encuentran en dicha cuenta, transfiriendo a otra cuenta o incluso realizando compras virtuales como si fuera suyo la cuenta, puesto que por tan solo saber todo los datos de la tarjeta, sin la necesidad de tener presencial, se puede realizar un sin número de transacciones.

En este sentido, se puede advertir que el sujeto activo extrae, es decir, hace suyo bienes ajenos en forma ilegítima en perjuicio de la víctima, por lo que constituye hurto informático, por usar los medios informáticos para cometer los actos ilícitos.

Hurto de valores

En la era informática como la actualidad, no solo el dinero (con valor patrimonial) puede ser objeto de hurto informático, sino también cualquier otro bien, en su mayoría, valores digitales de relevancia patrimonial, puesto que con el avance de la tecnología se está conduciéndose a una etapa de cero papel, por lo que los bienes, como títulos valores, programas (patrimonio electrónico o digital) es totalmente factible de ser objeto de hurto informático, por lo que la necesidad de regulación y sanción de los actos ilícitos que atenten contra dichos bienes jurídicos penalmente tutelables.

Fraude informático.

¿Qué es el fraude informático?

El fraude informático es el acceso indebido a datos y cualquier bien material o inmaterial con valor patrimonial burlando las medidas de seguridad de sistemas, redes y medios electromagnéticos con el fin de aprovechamiento indebido de los frutos del acto fraudulento. El fraude informático de puede concebido como un engaño a las medidas de seguridad de medios informáticos para el

aprovechamiento indebido, y a diferencia de ello, la estafa informática se puede concebido como el uso de medios informáticos para engañar a las personas.

Como se puede apreciar, el fraude informático recae sobre la seguridad de los medios informáticos, mientras la estafa informática recae sobre la persona.

Vásquez, Regalado y Guadron (2017) acotan que el fraude informático es el perjuicio patrimonial que se genera a otra persona por medios de la manipulación de datos informáticos o la interferencia en el funcionamiento de un sistema informático, cuya finalidad es la obtención ilegítima de un beneficio económico para sí o terceras personas (p. 65).

El fraude informático, conforme al Artículo 8 del Convenio de Budapest penaliza los actos deliberados e ilegítimos que generan perjuicio patrimonial a la persona por medio de introducción, alteración, borrado, supresión de datos informáticos; o por cualquier interferencia en el correcto funcionamiento del sistema informático, donde el sujeto activo interviene con la intensión dolosa de obtener en forma ilegítima un beneficio económico para sí o para otra persona.

Delitos informáticos ligados a los medios de pago electrónico.

Los avances de las tecnologías de la información y las comunicaciones (TIC) y el crecimiento de las operaciones comerciales en Internet han propiciado el surgimiento de nuevas conductas fraudulentas relacionadas con el uso de instrumentos de pago electrónicos. La dificultad de encuadrar estos supuestos en los tipos penales tradicionales ha motivado la revisión de las diferentes codificaciones y legislaciones con la finalidad de evitar la impunidad de estas conductas delictivas. (Rico, 2013, p. 208).

Las acciones más frecuentes vinculadas al uso de los medios de pago electrónicos son con el empleo de las tarjetas que involucra una serie de conductas dentro y fuera de internet, en donde se emplea la informática como en los supuestos de clonación o falsificación.

El citado autor además precisa que los mecanismos de pago de mayor uso son las tarjetas en sus distintas modalidades y transferencias electrónicas de fondos, junto a las operaciones comerciales por internet, que ha incitado la

creación de las diversos mecanismos de pago, tales como con letras de cambio, cheques electrónicas, dinero efectivo electrónico, entre otros medios de pago. Estas nuevas modalidades de pago ha traído consigo, junto al avance tecnológico, el surgimiento de nuevas conductas delictivas y que debido a sus características especiales de comisión de la conducta reprochable dificultan su encuadramiento en los tipos penales tradicionales (Rico, 2013, p. 211).

Asimismo podemos identificar otro de los delitos de fraude vinculado a los medios de pago, especialmente vinculados a las tarjetas de crédito, como es la clonación, sobre el cual Roldán, Rincón y Taborda señalan que la clonación de tarjeta también conocida como "*skimming*" es un tipo de fraude por medio del cual se duplican tarjetas y para luego realizar transacciones y retiros sin la autorización del titular de la cuenta. Esta modalidad de delito ocurre tanto en cajeros automáticos como en establecimientos comerciales o restaurantes. Los delincuentes pueden cargar consigo un dispositivo conocido como "*skimmer*", que les permite leer la banda magnética tan solo con deslizarla por una ranura. (2017, p. 13).

Fraude al sistema

Por definición, se hace referencia que en el fraude el sujeto activo del delito, a diferencia de la estafa informática, engaña a las medidas de seguridad de los medios o sistemas informáticos, es decir, logra cometer el fraude al sistema, utilizando su expertis y conocimientos de informática, a efecto de que las medidas de seguridad de los sistemas informáticos sean insuficientes para impedir el acceso del ciberdelincuente.

Cabe resaltar que el delincuente rompe las claves del sistema a efectos de aprovecharse económicamente en forma ilegítima, esto implica que el sujeto activo puede cometer un concurso de delitos, donde por un lado burla las medidas de seguridad de los sistemas informáticos (fraude al sistema), para acceder ilegítimamente al patrimonio digital o virtual (inmaterial), y como consecuencia de este acceso, puede, por ejemplo, sustraer en forma sistemática los saldos de una cuenta, cometiendo por consiguiente adicionalmente delito de hurto informáticos. Esto implica que es un delito independiente burlar las medidas de seguridad de

los sistemas informáticos para acceder a ella con la finalidad de aprovechamiento y otra es sustraer los bienes o valores que ahí se encuentran o destruir, secuestrar, modificar o suprimir el mismo en perjuicio económico del sujeto pasivo.

Fraude en los datos

A diferencia del fraude al sistema, en el fraude en los datos, el delincuente informático lo que realiza es alterar los datos de los sistemas informáticos a efectos de beneficiarse económicamente, por decir un ejemplo, el acceso a una plataforma de venta en línea (tienda virtual), burlando las medidas de seguridad del sistema, con la finalidad de modificar los datos como el precio (bajar precio) de los accesorios a adquirir, para de esta forma el pago que se efectúe sobre dichos productos sea inferior y que la misma plataforma procese el pago al igual que de cualquier otro cliente.

Estafa informática.

¿Qué es la estafa informática?

La estafa informática es una conducta delictiva que consiste en el uso de los medios informáticos para engañar a la víctima con el fin de que se desprenda de su patrimonio y el aprovechamiento indebido del sujeto activo de dicho patrimonio. Véase que los elementos típicos del delito de estafa informática son extremadamente similares al delito de estafa común, con la especial característica de que en la estafa informática, para crear la falsa realidad en la víctima del delito se emplea los medios informáticos. Es decir, para hacer caer en error a la víctima se emplean los medios informáticos.

Se puede advertir que en la legislación peruana la estafa como delito informático no se encuentra tipificado como tal, pese a que con el fraude se pretende cubrir de alguna manera, es evidente que es insuficiente, por cuanto genera interpretaciones ambiguas y contradictorias que finalmente conducen a la impunidad. Al respecto García (2017) bien señala al decir “(…) es de gran importancia que esta exista como un delito independiente ya que las penas establecidas entre Apropiación fraudulenta por medios electrónicos y la estafa

difieren en gran medida, y sobre todo la conducta penalmente relevante entre una y otra difiere, existiendo una clara desproporcionalidad ante un delito que debe ser considerado de manera irrefutable como estafa". (p. 15)

Estafa a través de instrumentos de pago.

Aunque la estafa informática se encuentra directamente relacionada con el tema de los medios electrónicos de pago, toda vez que se refiere a la manipulación informática realizada con ánimo de lucro con la finalidad de obtener una transferencia no consentida de un activo patrimonial, en la práctica también se han presentado problemas para encuadrar las operaciones de pago fraudulentas realizadas a través de Internet en el concepto de manipulación informática. (Rico, 2013, p. 218).

Veamos un ejemplo de estafa informática con el empleo de medios de pago: Un usuario durante su navegación por la red se encuentra con una oferta imperdible de un aparato, objeto, prenda o cualquier bien de su interés, cuando sigue la publicidad le manda a una página web donde tiene las opciones de compra y pago por medios electrónicos como la tarjeta de crédito o débito, una vez verificado el producto de su interés procede a pasar por la pasarela de pago, incluso la plataforma le indica las opciones de envío, el tiempo estimado, estimado, las características del producto, las formas de devolución, seguro y todo los demás pormenores que permitan al usuario sentirse seguro (crear una falsa realidad de seguridad), una vez decidido para la compra del producto procede llenar los casilleros y datos de seguridad de la tarjeta de crédito o débito, una vez hecho la transacción espera la fecha de llegada del producto y nunca llega, y cundo se busca a la plataforma no encuentra o es que ya tiene otro interfaz que nadie puede reconocer. en este sentido, en el ejemplo planteado, se creó una falsa realidad en la víctima usando los medios informáticos, hasta que se logró con el desprendimiento de su patrimonio como consecuencia de dicha falsa realidad creada, beneficiándose el criminal informático, no solo con el monto de la transacción del valor del producto, sino que, además, obtiene todo los códigos de seguridad de la tarjeta empleada, el cual puede utilizar para realizar hurto sistemático de la cuenta o emplear para realizar otras compras por internet.

Al respecto Wall (2015) señala que varias estadísticas muestran claramente que el Internet es cada vez más utilizado por los estafadores para robar grandes cantidades de dinero de las víctimas inocentes, o por los hackers para obtener información e interrumpir los procesos empresariales o gubernamentales. El principal desafío, sin embargo, para los políticos y profesionales es identificar exactamente que los estafadores y hackers son y cómo se organizan, porque comparativamente poco se sabe acerca de ellos o cómo se organizan (p. 76).

Modalidades de estafa

Phreaking.

Es la metodología más antigua dentro de los denominados ciberdelitos, consiste en ingresar en las redes de telecomunicaciones para realizar llamadas telefónicas a larga distancia utilizando la cuenta ajena. Resulta ser una modalidad primitiva de hacking. (Alcívar, Domenech y Ortiz, 2015, p. 46).

Phishing.

En el *phishing*, la captación ilícita de datos tiene lugar a través del envío masivo de correos electrónicos que simulan la identidad de una institución financiera con el objetivo de solicitar a los receptores los datos de sus respectivas tarjetas, alegando diversos motivos (promoción de productos o servicios, participación en concursos, problemas de seguridad, técnicos, etcétera). Los correos electrónicos incluyen enlaces a sitios Web que imitan los de las entidades bancarias donde el usuario suministra los datos del instrumento de pago. (Rico, 2013, p. 214).

Es una modalidad de fraude informático diseñada con la finalidad de robarle la identidad al sujeto pasivo. El delito consiste en obtener información tal como números de tarjetas de crédito, contraseñas, información de cuentas u otros datos personales por medio de engaños. (Imbaquingo, *et. al*, 2016, p. 140).

Pharming.

La técnica utilizada en el *pharming* también remite a los usuarios a páginas Web falsas, creadas en formato similar a las de las entidades bancarias con el objeto

de captar los datos de los clientes. En estos casos, el procedimiento no se lleva a cabo mediante el envío masivo de correos electrónicos; el acceso indebido se produce por una vulnerabilidad en el DNS (*Domain Name System*) o en el de los equipos de los usuarios, que permite al atacante redirigir el nombre de dominio de la entidad a una página Web que en apariencia es idéntica. (Rico, 2013, p. 214).

Sabotaje informático.

Bashir y Khalique (2016) considera que el sabotaje es el uso no autorizado de instalaciones informáticas, alteración o destrucción de información, sabotaje archivo de datos y el vandalismo en contra de un sistema informático. Las computadoras deben ser protegidos de sabotajes para evitar cualquier inconveniente (, p. 16).

Asimismo, en ese orden de ideas, Alcívar, Domenech y Ortiz, (2015) señalan que el sabotaje informático Implica que el "delincuente" recupere o busca destruir el centro de cómputos en sí (las máquinas) o los programas o informaciones almacenados en los ordenadores. Se presenta como uno de los comportamientos más frecuentes y de mayor gravedad en el ámbito político. (p. 45).

La palabra sabotaje informático se entiende como todas aquellas diligencias encaminadas a provocar daños en el hardware o en el software de un sistema. (Herrera, 2018, p. 21).

El sabotaje informático; que consiste básicamente en borrar, suprimir o modificar (alterar) sin autorización funciones o datos de las computadoras con intención de obstaculizar el funcionamiento normal del sistema, que se conoce comúnmente como virus informático (Villavicencio, 2014, p. 293).

Destrucción de datos

A diferencia de las otras modalidades de delitos informáticos contra el patrimonio, el sabotaje informático tiene una particularidad, es que la comisión de este delito implica la destrucción, alteración, o la realización de cualquier otro acto que haga al sistema, software o cualquier otro bien informático, que no permita operar con

las mismas potencialidades, generando en este sentido, grandes pérdidas en la víctima.

La pérdida puede ser directa consecuencia de la conducta o provocada por esta, por ejemplo, si la base de datos de desarrollo de una aplicaciones de un diseñador de aplicaciones móviles es destruida sin que queda ningún archivo, éste (víctima) pierde todo en forma directa, la inversión, el tiempo dedicado y si el producto ya contaba con titular, genera desprendimiento patrimonial, siendo que esta modalidad de delitos informáticos presente en organizaciones que compiten entre sí, y a efectos de ganar ventaja en el mercado, uno de ellos destruye la información de la otra, o deja inoperativa la misma, o en todo caso, lo secuestra (inmoviliza) la información con la finalidad de pedir grandes sumar de dinero por su rescate, como lo ocurrido el agosto de 2018 en diversos bancos, cuya finalidad de los delincuentes informáticos era, conforme a las noticias vertidas al respecto, encriptar las bases de datos de los bancos para luego solicitar grandes sumas de dinero por su rescate.

Alteración de datos

En correlación de lo ya antes citado, el sabotaje informático, entre otros, implica la alternación de los datos de los sistemas con la finalidad de generar daños económicos en la víctima o fines lucrativos para sí o terceros. Siendo que con la alteración, el sistema puede quedar inoperativa o bajar su rendimiento, no solo generando pérdidas por el defecto directo, sino, además la contratación de otros especialistas para reparar las alteraciones generadas.

Medidas de prevención.

Se debe bloquear la cuenta bancaria si se utiliza la tarjeta de crédito en un lugar donde no te encuentras, esto es, si no se está haciendo la transacción en un lugar donde no está el teléfono del propietario de la tarjeta.

Se debe verificar que la página web en la que se navega, sea verdaderamente en la original, esto, verificando el dominio, las medidas de seguridad y otros indicadores.

Si se encuentra alguna oferta inusual, se debe, previamente investigar sobre la veracidad del mismo, esto se puede hacer a través de buscadores, noticias, foros, blogs y otras publicaciones sobre la oferta.

Debe verificar la seriedad, certificados y toda información referente a la originalidad y veracidad de lo que se ofrece en las redes, plataformas de comercio electrónico desconocidos y en caso de ser conocidos verificar que no esté clonada, y de preferencia digitar directa y manualmente la ruta.

Ante las falsas alarmas de virus, no ejecutar programas sugeridas ni desconocidas, si es propia del sistema, se debe, previamente verificar que sea del proveedor, caso contrario no ejecutar, puesto que el delincuente puede tener control del ordenador.

1.3 Marco espacial

El marco espacial del presente estudio constituye en medio geográfico en la que se lleva a cabo la investigación, siendo éste Lima, la Capital del Perú. Cabe resaltar que la información que en el desarrollo de la investigación se recopile corresponde no solo a este marco espacial, sino a aquellas a las que desde este medio geográfico se pueda tener acceso, ya sean estas fuentes documentales y/o informantes entrevistadas.

1.4 Marco temporal

El marco temporal es el eje en cualquier investigación histórica, mediante el cual se delimita en la información a procesar o analizar, sin embargo, el presente estudio no es de naturaleza histórica, por lo que la información que en su desarrollo se recopila y analiza corresponden a fuentes con una antigüedad no mayor a cinco años, pudiendo válida y justificadamente utilizar en el desarrollo fuentes más antiguas de acuerdo a su relevancia de su contenido y vinculación con el problema de estudio.

Asimismo, en el aspecto temporal, la presente investigación es desarrollada en el periodo correspondiente al año dos mil dieciocho, por lo que los resultados que se obtienen son de acuerdo a tal periodo, puesto que si el tiempo de desarrollo de la investigación fuera anterior o posterior a esta fecha, es posible

que haya alguna variación, no solo en el problema objeto de estudio, sino también en las fuentes y el tratamiento que se le pueda dar a los mismos.

1.5 Contextualización: histórica, política, cultural, social.

1.5.1 Contexto histórico

El primer crimen cibernético tuvo lugar en 1820. En 1820 Joseph-Marie Jackquard, un fabricante textil en Francia, produjo el telar, un dispositivo que permite la repetición de una serie de pasos en el tejido de telas especiales. Esto conduce al miedo en las mentes de los empleados Jackquard y que cometió el acto de sabotaje. Esta fue la primera registrada ciberdelincuencia. (Aggarwal, Arora, Ghai y Poonam, 2014, p. 48).

En el Perú los delitos informáticos en un inicio se encontraba tipificado en el artículo 186, inciso 3, segundo párrafo del Código Penal de 1991 como agravante del delito de hurto, luego se incorporó como un capítulo (Capítulo X.- Delitos Informáticos). Sin embargo este capítulo ya fue derogado por una ley especial en octubre del 2013, dicha normativa fue la Ley 30096 (Ley de Delitos Informáticos), el cual a su vez sufrió modificaciones en 2014 por la promulgación de la Ley 30171 (Ley que modifica la Ley 30096, Ley de Delitos Informáticos), cuya finalidad fue adecuarse al convenio sobre la cibercriminalidad (Convenio de Budapest).

1.5.2 Contexto político

En el contexto político, se observa que a la fecha de la realización de la presente investigación, en la política criminal hubieron intenciones y propuestas legislativas diversas para la lucha contra la cibercriminalidad, de los cuales se encuentran archivadas y la que prosperó son únicamente la que es ahora la Ley 30096 y la Ley 30171.

1.5.3 Contexto cultural

En el aspecto cultural, el Perú es uno de los países que tiene la multiculturalidad, junto con la extensión territorial que se expande entre las tres regiones, siendo la extensión territorial y las alturas y lejanías uno de los factores que limitan la intercomunicación, de ahí viene las brechas de acceso a la internet y a las

tecnologías informáticas, puesto que en las alturas y en las lejanías del Perú aún no hay un alcance pleno ni suficientes de las empresas de telecomunicaciones y por otro lado, también constituya las limitaciones del acceso a la educación de los pobladores de culturas alejadas a las ciudades.

1.5.4 Contexto social

En el contexto social e incluso económico, la sociedad peruana, al igual que los demás países es consumista, asimismo las adecuaciones de tecnologías informáticas, computadoras, teléfonos móviles y otros aparatos similares es cada vez más usual y cotidiano. Sin embargo, un grupo considerable de población no tiene acceso aún a dichos aparatos, principalmente aquellos que radican en zonas donde las redes de comunicación aún no alcanzan o por cuestiones económicas.

Asimismo, vivimos en una sociedad donde los jóvenes y los menores de edad son los más familiarizados con el uso de las tecnologías informáticas, por consiguiente lo son también los más vulnerables y propensos a ser víctimas de delitos informáticos.

1.6 Supuestos teóricos

1.6.1 Supuesto teórico general

El tratamiento jurídico penal de los delitos informáticos contra el patrimonio es deficiente, toda vez que ilógicamente se comprende dentro de fraude informático todo los tipos o modalidades de delitos informáticos contra el patrimonio, el cual genera incertidumbre en la interpretación de la norma que no permite la sanción efectiva de los delitos informáticos contra el patrimonio.

1.6.2 Supuestos teóricos específicos

El tratamiento jurídico penal de los delitos informáticos contra el patrimonio en su modalidad de hurto es deficiente, en la medida que en la legislación peruana no se regula en forma expresa el delito informático contra el patrimonio, por lo que dicho vacío genera dificultades en la investigación y sanción de los delitos informáticos de hurto, más cuando no se cumple con el principio de tipicidad.

El tratamiento jurídico penal de los delitos informáticos contra el patrimonio en su modalidad de fraude es deficiente, puesto que dentro de esta modalidad

directiva se ha comprendido todas las modalidades de delitos informáticos contra el patrimonio, y al ser este tipo penal muy abierto y ambiguo no permite la efectiva sanción de los delitos informáticos contra el patrimonio.

El tratamiento jurídico penal de los delitos informáticos contra el patrimonio en su modalidad de estafa es deficiente, toda vez que la legislación peruana no regula expresamente este ilícito penal, por lo que, al no cumplirse con el principio de tipicidad, dificulta la investigación y sanción de los delitos informáticos contra el patrimonio en su modalidad de estafa.

El tratamiento jurídico penal de los delitos informáticos contra el patrimonio en su modalidad de sabotaje informático es deficiente, puesto que, pese a que en la vigente legislación se sanciona la destrucción de datos, no se regula en forma clara y expresa la afectación al patrimonio por medio sistemas informáticos, con o sin fines lucrativos, el cual genera impunidad de los actos de sabotaje informático contra las empresas o personas para reducir su competitividad.

II. Problema de Investigación

2.1 Aproximación temática: observaciones, estudios relacionados, preguntas orientadoras

En la actualidad se observa que cada vez más las nueves sistemas de información, nuevas tecnologías, sistemas informáticos y en específico las nuevas tecnologías informáticas ha ido avanzando, donde existen muchos expertos en la materia, quienes hacen y desasen diversos softwares, así como cometen actos ilícitos.

Es así que estas tecnologías informáticas definitivamente se pueden usar para muchas y buenas cosas, pero también para causar perjuicio a terceros, sustraer patrimonios, bienes, alterar sistemas de seguridad, extraer, modificar y eliminar datos, realizar un sin número de fraudes e incluso acceder a los datos de las entidades públicas y privadas rompiendo medidas de seguridad.

En este orden de ideas, el problema de la ciberdelincuencia ha aumentado y desarrollados nuevos sofisticados modos de operación, difícil de descubrir, frente a este realidad el derecho penal de muchos países ha quedado en el tiempo, la peruana no es la excepción, a pesar de las modificatorias introducidas en forma genérica en relación a la ciberdelincuencia no basta, por lo que el derecho penal ya queda y lo es aparente frente a esta situación.

En tal sentido, existen un sin número de modalidades en las que los ciberdelincuentes pueden cometer delitos contra el sistema informático ya sea mediante acceso o alteración de los sistemas informáticos, así como cometer delitos contra el patrimonio, ya sea mediante cualquier tipo de fraude informático, hurtos, estafas, pero también se puede cometer delitos contra la privacidad de las personas, instituciones y el Estado mismo, en este aspecto, las pequeñas y medianas empresas son las más vulnerables debido a que no cuentan con un sistema de ciberseguridad, en las plataformas o nubes que usan, pues todo los datos que se almacenan en la nube pueden estar siendo objeto de intercepción.

Es así que los delitos informáticos contra el patrimonio se realizan en afectación de las personas naturales y jurídicas, en la modalidad de hurto, fraude, estafa y sabotaje informático, los mismos que a todas luces pasa desapercibido debido a la debilidad del tratamiento jurídico penal que los países le dan a estas conductas ilícitas, también por las especiales características que distinguen a estas conductas, como la condición cualificada de los sujetos activos quienes tienen un alto grado de expertís en la informática, es así como los nuevos delitos informáticos que pasan desapercibidos y difíciles de descubrir aunque son denunciadas.

Que los avances tecnológicos son utilizados para beneficiarse ilícitamente del patrimonio de terceros por medio de clonación de tarjeras bancarias, alteración o vulneración de sistemas informáticos con el objetivo de beneficiarse de servicios, así como las trasferencia de fondos ajenos por medio de manipulación de sistemas informáticos de seguridad.

En términos comerciales, las empresas o instituciones que no estén en la red simplemente no existen y mantienen desventaja frente a los que están disponibles en el internet, en este sentido, las transacciones comerciales de diversa naturaleza cada vez más va en aumento y mucho más consolidado, sin embargo, la contra que pone en duda y por consiguiente la limitación de realizar operaciones por medios electrónicos es justamente el fraude, estafa o hurtos informáticos que puedan afectar a los usuarios como consecuencia de que por las plataformas virtuales, para concretar transacciones es necesario proporcionar los datos y claves de la tarjeta electrónica, pudiendo ser utilizadas los datos para hurtos sistemáticos del fondo de la tarjeta, si opere el cobro del monto pero nunca pueda recibir el bien adquirido o el servicio contratado, siendo el usuario víctima de estafa, puesto que se le indujo en error al ofrecer un bien o servicio y logrando que se desprenda del patrimonio, el cual de hecho genera desconfianza

En el derecho penal informático, la legislación penal (derecho penal) cumple el rol de simbólico, que carece de sistematicidad y exhaustividad en la calificación de las conductas que afectan bienes jurídicos penalmente tutelables, como es el patrimonio.

De acuerdo a la estadística proporcionada por el Instituto Nacional de Estadística e Informática, en el Perú, las denuncias realizadas por los delitos informáticos en los periodos 2008 al 2011 no existe una sola denuncia o caso registrado sobre delitos informáticos, cabe preguntarse entonces ¿Por qué es que no existe una sala denuncia?

Posteriormente a ello, con las modificaciones introducidas en el 2013 y 2014 se observa que el aumento de los casos registrados de los delitos informáticos, conforme a los informes estadísticos del Ministerio Públicos, ha aumentado considerablemente y se está multiplicando, entonces, las denuncias presentadas o los casos registrados, si no se tiene una regulación adecuada para sancionarlos penalmente, es evidente que va quedar impune, puesto que en la legislación peruana no existe una regulación expresa de hurto, estafa y sabotaje informático, más por el contrario, se ha introducido fraude informático como un delito genérico, pues éste genera más ambigüedades y vaguedad en su interpretación que bridar soluciones y permitir una sanción que corresponda a la conducta penalmente relevante y reprochada por la sociedad.

El artículo 8 de la “ley de delitos informáticos” tipifica una sola modalidad de delitos informáticos contra el patrimonio, al cual se rotula con el *nomen iuris* de “fraude informático”, dicha regulación genérica que no permite delimitar e identificar plenamente las conductas en el tipo penal, esto es, la subsunción de la conducta con el tipo penal (tipificación).

Otro de los problemas de alcance nacional e incluso internacional es la investigación y sanción de los delitos informáticos, toda vez que los ciberdelincuentes tienen la plena posibilidad de cometer actos ilícitos estando físicamente en un continente pero generando los daños otro continente o país, y lo peos es que se pueden programar ataque masivos que en tiempo real puede tener efectos en diferentes países, entonces qué país es que tendría facultades de investigar y sancionar dichos ilícitos, pues la respuesta no es nada fácil, en la medida que, sea uno o el otro país, requiere la colaboración y cooperación.

Como ejemplo de ataque generalizado y con efectos en varios países, tenemos como último evento el efectuado el pasado 17 de agosto del 2018, en la que por ataques cibernéticos de nivel internacional bancos peruanos y antes de dicha fecha bancos chilenos y otros países sufrieron graves generalizados al mismo tiempo, afectándose sus operaciones, con la directa afectación de los usuarios por inoperatividad de sistemas. Las diferentes fuentes señalaron que se trataba de un ataque en la modalidad de "*Ramsomware*" que consiste en encriptar la información, datos o valores de la víctima para luego pedir altas sumas de dinero por su rescate.

Sobre este problema, ¿qué soluciones se ha planteado en el Perú?, ¿Están realmente preparados, tanto las instituciones, funcionarios, empresas y la sociedad civil para afrontar?, ¿la legislación penal es adecuado para investigar y sancionar los delitos informáticos contra el patrimonio?, ¿existe un adecuado tratamiento jurídico penal de los delitos informáticos contra el patrimonio?, éstas y otras cuestiones necesitan respuestas urgentes, en una época donde el uso de los sistemas informáticos es masivo, continuo y en constante crecimiento, y por el otro lado, los delincuentes informáticos actúan cada vez más sofisticadas frente a la creciente y expuesta vulnerabilidad de los usuarios víctimas.

La vigente regulación de los delitos informáticos contra el patrimonio es deficiente, debido a que al tratarse de delitos informáticos en la modalidad de hurto, sabotaje o estafa, la legislación no permite la sanción efectiva de las acciones ilícitas, puesto que se ha comprendido dentro de la figura de fraude todo los posibles ilícitos, pues esta figura jurídica no tiene alcance.

En la legislación penal peruana no se cumple con el principio de tipicidad para la sanción del delito de hurto informático, sabotaje informático, estafa informática y es bastante genérica y dentro de fraude informático se pretende comprender todas las modalidades de delitos informáticos contra el patrimonio.

2.2 Formulación del problema de investigación

2.2.1 Problema general

¿Cómo es el tratamiento jurídico penal de los delitos informáticos contra el patrimonio, Distrito Judicial de Lima, 2018?

2.2.2 Problemas específicos

¿Cómo es el tratamiento jurídico penal de los delitos informáticos contra el patrimonio en su modalidad de hurto?

¿Cómo es el tratamiento jurídico penal de los delitos informáticos contra el patrimonio en su modalidad de fraude?

¿Cómo es el tratamiento jurídico penal de los delitos informáticos contra el patrimonio en su modalidad de estafa?

¿Cómo es el tratamiento jurídico penal de los delitos informáticos contra el patrimonio en su modalidad de sabotaje informático?

2.3 Justificación

2.3.1 Justificación teórica

La presente investigación adquiere su justificación teórica, en la medida que en el desarrollo de la parte teórica se desarrollan y hacen tratamiento de las modernas teorías referidos a la sanción penal en los delitos informáticos contra el patrimonio, dentro del cual el hurto, estafa, fraude y sabotaje informático, por otro lado, se desarrolla también la ciberdelincuencia como una figura como consecuencia del desarrollo de las nuevas tecnologías y la comisión de los delitos informáticos, ya sea contra los sistemas y datos, contra la persona o contra el patrimonio.

2.3.2 Justificación práctica

En la práctica se observa que a la fecha existen varias modificaciones del tipo penal referente a los delitos informáticos, en este sentido, lo que antes se regulaba en forma expresa este tipo penal en el código Penal, a la fecha este es regulado mediante una ley especial, esto es, Ley Nº 30096 (Ley de delitos

informáticos) y su modificación. En tal sentido, se aprecia que en la actualidad existe una inestabilidad legislativa para la sanción de los delitos informáticos, debido a que la legislación existente no logra comprender y no se ajusta a los hechos que deben ser sancionados, es más, sin número de delitos informáticos no son detectados debido a la alta sofisticada de las operaciones que en la red negra se realiza.

2.3.3 Justificación metodológica

En relación a la justificación metodológica, en la producción de los conocimientos científicos en esta investigación se emplea un conglomerado de técnicas, métodos e instrumentos de recolección y análisis de datos, así como el uso de la metodología distinta a las investigaciones ya existentes relacionados al tema en estudio.

2.4 Relevancia

Esta investigación cobra relevancia jurídica, doctrinaria y académica, toda vez que trata de un tema poco o nada investigada, puesto que son pocas las investigaciones realizadas respecto a los delitos informáticos contra el patrimonio, menos a nivel de tesis. En este orden de ideas, otro aspecto fundamental de la relevancia del estudio es la clasificación de los delitos informáticos contra el patrimonio como es el hurto, sabotaje, estafa y fraude informático,

2.5 Contribución

La contribución de la presente investigación es a nivel académico, puesto que se desarrollan los conceptos y teorías vinculadas a los delitos informáticos contra el patrimonio, en cuatro modalidades; por otro lado, la presente investigación tiene contribución jurídica, puesto que las propuestas de solución del problema de investigación constituyen *lege ferenda* que deben tomarse en cuenta cuando se realicen las futuras reformas legislativas respecto a los delitos informáticos contra el patrimonio.

2.6 Objetivos

2.6.1 Objetivo general

Analizar el tratamiento jurídico penal de los delitos informáticos contra el patrimonio, Distrito Judicial de Lima, 2018.

2.6.2 Objetivos específicos

Analizar el tratamiento jurídico penal de los delitos informáticos contra el patrimonio en su modalidad de hurto.

Analizar el tratamiento jurídico penal de los delitos informáticos contra el patrimonio en su modalidad de fraude.

Analizar el tratamiento jurídico penal de los delitos informáticos contra el patrimonio en su modalidad de estafa.

Analizar el tratamiento jurídico penal de los delitos informáticos contra el patrimonio en su modalidad de sabotaje informático.

III: Marco Metodológico

3.1 Categorías y categorización

Tabla 3:
Matriz de construcción de categorías y subcategorías apriorística

Categoría	Sub categoría	Fuente (informante)	Técnica	Instrumento
Tratamiento jurídico penal	• Tratamiento procesal. • Tratamiento legislativa	Expertos en informática y delitos informáticos	Entrevista	Guía de entrevista
Hurto	• Hurto sistemático • Hurto de valores			
Fraude	• Fraude al sistema • Fraude en los datos			
Estafa	• Estafa informática • Modalidades de estafa			
Sabotaje informático	• Destrucción de datos • Alteración de sistemas			

Fuente: Elaboración propia

3.2 Metodología

Señala que “La Metodología es la ciencia que nos enseña a dirigir determinado proceso de manera eficiente y eficaz para alcanzar los resultados deseados y tiene como objetivo darnos la estrategia a seguir en el proceso” (Cortés e Iglesias, 2004, p. 8). En la producción de conocimientos científicos se pueden utilizar una serie de métodos, es decir, la metodología a aplicarse es variable, sin embargo, dicha metodología debe aplicarse de acuerdo a los objetivos que busca la investigación y debe ser apropiada para que los resultados del estudio revelen

una respuesta al problema de investigación que ha sido formulada y cumplir con el objetivo de estudio propuesto.

En este orden de ideas, el desarrollo de la presente investigación se desarrolla en aplicación de las metodologías propias y aplicables a la investigación cualitativa de nivel descriptivo explicativo, con diseño de teoría fundamentada de acuerdo a los parámetros interpretativos y analíticos de la investigación.

Paradigma

El paradigma del presente estudio es interpretativo y analítico, toda vez que las instituciones jurídicas comprendidas en el problema de investigación han sido objeto de análisis interpretativo, los mismos que se han descompuesto en categorías y subcategorías para su interpretación y análisis.

Enfoque

Esta investigación es de enfoque cualitativo, el cual consiste en la realización de prácticas interpretativas que conduce a describir, analizar y discutir el fenómeno objeto de estudio a través de entrevistas, conversaciones, recurriendo a fuentes documentales para dar sentido a la interpretación del problema en estudio y responder a los cuestionamientos o interrogantes fácticos jurídicos, sociales, dogmáticos y prácticos.

Al respecto, Jaramillo, Valarezo y Astudillo (2014) precisan que el “análisis de información en la investigación cualitativa consiste en reducir, categorizar, clarificar, sintetizar y comparar la información con el fin de obtener una visión lo más completa posible de la realidad objeto de estudio” (p. 11).

Diseño

El diseño de la presente investigación es teoría fundamentada, el cual “(…) se refiere a una teoría derivada de datos recopilados de manera sistemática y analizados por medio de un proceso de investigación. En este método, la recolección de datos, el análisis y la teoría que surgirá de ellos guardan estrecha relación entre sí. Un investigador no inicia un proyecto con una teoría preconcebida (a equilibrio entre la ciencia y la creatividad existen procedimientos que proporcionan algún grado de estandarización y rigor al proceso” (Strauss y

Corbin, 2002, p. 15). Por otro lado, Álvares-Gayou (2009) señala que “El planteamiento básico de esta revolucionaria postura de investigación en las ciencias sociales consiste en que la teoría se elabora y surge de los datos obtenidos en la investigación, y no como tradicionalmente se hacía, en el sentido inverso”(p. 90). “Los teóricos fundamentados recolectan datos a través de observaciones e entrevistas y a partir de fuentes como documentos, escritura creativa, artículos de periódicos, y diarios” (…) (Mayan, 2001, p. 9).

Desde el punto de vista de Hernández (2014), una de las posibilidades metodológicas más completas a la hora de trabajar con entrevistas es la Teoría Fundamentada (*Grounded Theory*). Señala que dicha teoría fue enunciada por Strauss y Glaser en 1967 y consiste en una metodología que trata de desarrollar una teoría basándose en la recolección y análisis sistemático de datos empíricos, no partiendo de ninguna teoría o hipótesis inicial (p. 192). Y señala que los conceptos y las hipótesis se van formulando a lo largo de la propia investigación.

En este orden de ideas, en el desarrollo de la presente investigación, se partió de la concepción de la realidad empírica, el cual se traduce en la comisión de ilícitos en uso de los medios informáticos, y verificado el estado de arte del problema de descubre una gama de delitos informáticos, para luego centrarse únicamente en delitos informáticos que afectan el patrimonio, llegándose a precisar las modalidades, tales como fraude, estafa, hurto y sabotaje informático, donde, a lo largo de la investigación se identificó diversos conceptos vinculados al problema objeto de estudio y se llegó a formular las hipótesis del problema de investigación.

Las investigaciones, de acuerdo al diseño, tipo, enfoque y otros aspectos, para el logro de los objetivos que se formulan, deben seguir una serie de pasos metodológicos, es decir, tiene su propia trayectoria metodológica, en este orden de ideas, el desarrollo de la presente investigación, a líneas generales, se siguió la siguiente trayectoria metodológica desde el principio hasta el final, toda vez que el diseño de estudio es teoría fundamentada en aplicación de entrevistas y el enfoque de estudio es cualitativa.

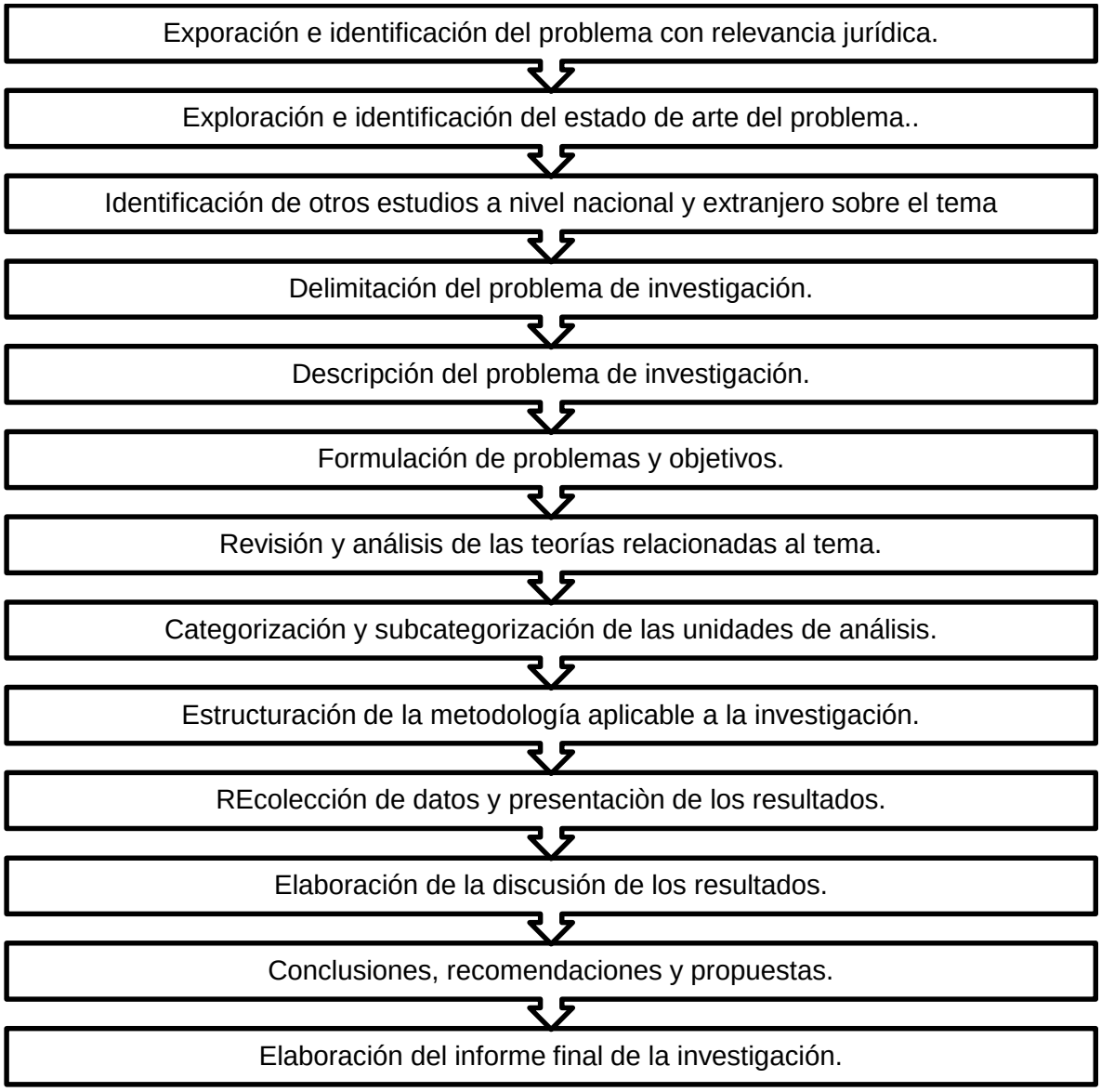


Figura 5:
Trayectoria metodológica de la investigación

3.3 Escenario de estudio

El escenario en la que se desarrolla el presente trabajo de investigación es el Distrito Judicial de Lima, sin embargo, las fuentes de información y los entrevistados no necesariamente son los que radiquen lo laboren en dicho lugar, así como las fuentes documentales son obtenidas de las principales bibliotecas de la capital y los importantes repositorios a nivel nacional e internacional.

3.4 Caracterización de sujetos

Por la caracterización de los sujetos se entiende a aquellas personas o instituciones que proporcionarán la información fundamental y relevante para la culminación de la presente investigación.

En este orden de ideas, los entrevistados en esta investigación fueron los expertos en informática y en delitos informáticos, tales como:

Tabla 4:
Caracterización de sujetos.

Experto	Nacionalidad	Descripción
Experto 1	Ecuador	Juez penal de la corte, docente en derecho informática e informática forense de las facultades de derecho e ingeniería de sistemas en la Universidad Católica de Ecuador.
Experto 2	Colombia	Abogado, investigador sobre delitos informáticos, con publicaciones en revistas científicas sobre el tema.
Experto 3	España	Profesional destinado en la Unidad Orgánica de la Policía Judicial, que forma parte de equipo de Delitos Tecnológicos.
Experto 4	Argentina	Jefe de departamento de informática forense del Poder Judicial en Argentina.
Experto 5	Perú	Abogado y sociólogo, Magíster en Derecho Penal, con especialidad en Derecho Informático y comercio electrónico, docente universitario y miembro de la Comisión Consultiva de Criminología del Ilustre Colegio de Abogados de Lima.
Experto 6	Perú	Fiscal Provincial Penal del Distrito Judicial de Lima Norte.

3.5 Procedimientos metodológicos de investigación

3.5.1 Recojo de datos

En el recojo de datos de ha empleado la técnica de entrevista, cuyo instrumento fue la guía de entrevista, así como el análisis de fuentes bibliográficas.

3.5.2 Análisis de datos

En el análisis de los se ha utilizado diversos métodos que son propios de la investigación cualitativa, entre las cuales son:

Método analítico: Empleado para descomponer las categorías en subcategorías con la finalidad de que es estudio sea mucho más profundo e integral.

Método comparativo: Este método ha sido aplicado para la estructuración de análisis comparativo de los resultados de las entrevistas, así como las legislaciones, opiniones y posturas en la materia.

Método dogmático: Empleado para el análisis de las dogmas e instituciones del derecho penal y la informática, a fin de analizar, criticar, cuestionar y proponer teorías sobre el problema de investigación.

Método descriptivo: Para describir las instituciones dele derecho penal informático, sus características y los aspectos relevantes para la investigación.

Método inductivo: Siendo el método inductivo propio de la investigación cualitativa, éste se ha empleado para expandir y descubrir nuevos aspectos del conocimiento en los delitos informáticos contra el patrimonio, desde el principio de la investigación.

3.6 Técnicas e Instrumentos de recolección de datos

Tanto las técnicas como los instrumentos de recolección de datos son herramientas metodológicas que permiten recopilar y analizar la información válidamente con el rigor exigido para la obtención de los resultados, en tal sentido, las técnicas e instrumentos aplicados en esta investigación son los siguientes:

3.6.1 Técnicas de recolección de datos

Las técnicas de recolección de datos utilizados en el desarrollo de la presente investigación son las siguientes:

Entrevista: Al respecto, Ramallo y Roussos, (2008) sostienen que la entrevista es un instrumento que permite relevar información en forma verbal, a través de preguntas formuladas por el investigador. Los cuales se pueden aplicarse en forma individual o en grupos. Además pueden efectuarse de modo personal es decir, mediante el contacto directo e inmediato, cara a cara, o mediatizadas por otros canales de comunicación, ej. por teléfono, videoconferencia, etcétera (p. 12). En este sentido, la entrevista, en el desarrollo de la presente investigación ha sido aplicada usando canales de comunicación, esto es, por medios electrónicos, donde a través de cual se ha remitido las preguntas de entrevista formuladas de acuerdo a los objetivos de la investigación, dándose la libertad al entrevistado responde las preguntas de acuerdo a su convicción.

3.6.2 Instrumentos de recolección de datos

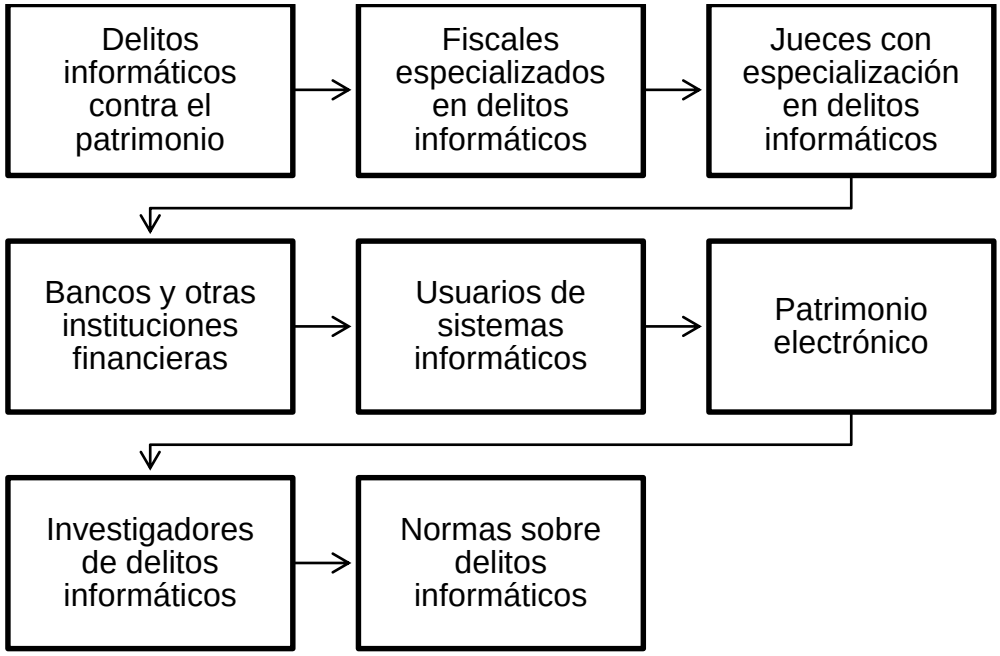
Los instrumentos de recolección utilizados en el desarrollo de la presente investigación son las siguientes:

Guía de entrevista: Por medio de este instrumento de recolección de datos, el investigador formulará un listado de preguntas abiertas de acuerdo a los objetivos de la investigación, el cual estará en forma ordenada, con el título y objetivo que busca el instrumento, dirigida al entrevistado, para de este modo facilitar al entrevistador y lograr la información que realmente se quiere obtener.

3.7 Mapeamiento

En aplicación del mapeamiento, para efectos de la presente investigación se ha verificado los aspectos relevantes del objeto de estudio en el escenario de investigación, el tal sentido se ha identificado el estado del arte del problema de investigación, siendo identificado los intervinientes, tales como, el Poder Judicial a través de sus funcionario, el Ministerio Público a través de sus funcionarios, los autores de los delitos informáticos, el objeto del delito, las víctimas de los delitos informáticos, entre otros aspectos que hacen relevante el tema en estudio, de

modo tal este proceso de identificación de los rasgos característicos del objeto de estudio ha permitido conocer los aspectos relevantes del problema y objeto de estudio.



Fuente: Elaboración propia

Figura 6: *Mapeamiento*

3.8 Rigor Científico

Esta investigación cumple con el rigor científico exigida por la comunidad académica científica, toda vez que las fuentes que se emplean en el desarrollo de esta investigación son confiables, con la debida citación de la fuente conforme a las normas internacionales de referencias bibliográficas, en este caso, en aplicación de las normas APA, asimismo, la información de campo el fidedigna a la fuente de información que ha proporcionado, se han empleado las técnicas e instrumentos de recolección y análisis de datos metodológicamente permitidos y aceptados por la comunidad científica, de acuerdo al tipo, diseño y nivel de la investigación. La investigación cumple con los criterios de credibilidad, Transferibilidad, y Confirmabilidad:

Credibilidad.

Es el grado o nivel en el cual los resultados de la investigación reflejen una imagen clara y representativa de una realidad o situación dada. Entonces, credibilidad se refiere a cómo los resultados de un estudio son verdaderos para las personas que fueron estudiadas, y para quienes lo han experimentado, o han estado en contacto con el fenómeno investigado (Rada, s.f. p. 6). En este orden de ideas, los resultados de la presente investigación son fidedignos a la realidad, pudiéndose corroborar en las fuentes originales que se encuentran en las referencias e incluso, corroborando directamente con los informantes.

Transferibilidad.

Con la transferibilidad de los resultados de la investigación se busca extender el conocimiento sobre el contexto o problemática objeto de estudio a otros escenarios similares, es decir, los resultados de la presente investigación pueden ser útiles en otros contextos similares, pero no se pueden aplicar en estricto, toda vez que el aspecto característico del problema de estudio es que no todas las realidades comparten mismo problema, o pese a que se comparta el contexto social, legislativo y académico es va variable. Sin embargo, a nivel nacional es totalmente generalizable y de hecho los resultados tienen alcance nacional al analizar una regulación de alcance nacional.

Confirmabilidad o auditabilidad.

La confirmabilidad implica que los resultados de la investigación pueden ser obtenidas por otro investigador siguiendo la ruta de la investigación o aplicando las técnicas, métodos y demás procedimientos aplicados. En este sentido se señala que “Esta estrategia permite examinar los datos y llegar a conclusiones iguales o similares, siempre y cuando se tengan perspectivas análogas” (Rada, s.f. p. 7). En este sentido, usando los mismos procedimientos de estudio utilizados, otros o futuros investigadores podrán llegar a iguales o similares conclusiones, lógicamente, tomando en cuenta el contexto, el tiempo y las circunstancias en las que se realiza la investigación.

IV. Resultados

Presentación de los resultados

Tabla 5:
Presentación de los entrevistados

Entrevistados
Dr. Santiago Martín Acurio Del Pino (Ecuador) Juez de la Corte Provincial de Pichincha de la Sala Única Penal, docente de Derecho Informático e Informática Jurídica de las Facultades de Ingeniería en Sistemas y Derecho de la Pontificia Universidad Católica del Ecuador.
Abg. Ivan Manjarres Bolaño (Colombia) Abogado, investigador y experto en delitos informáticos.
Dr. Andrés Álvarez Pérez (España) Destinado en la U.O.P.J. (Unidad Orgánica de policía Judicial) de Cádiz, Equipo de Delitos Tecnológicos (E.D.I.T.E.).
Ing. Gaston Miguel Semprini (Argentina) Jefe del Departamento de Informática Forense del Poder Judicial de Rio Negro. Argentina.
Mg. Daniel Peña Labrin (Perú) Abogado & Sociólogo, Magíster en Derecho Penal, Segunda Especialidad en Derecho Informático y Comercio Electrónico, Profesor de la Facultad de Derecho y Ciencias Políticas de la Universidad Inca Garcilaso de la Vega, Lima- Perú. Miembro de la Comisión Consultiva de Criminología del Ilustre Colegio de Abogados de Lima.
Dr. Gustavo Adolfo Silva Huamán (Perú) Fiscal Provincial Penal del Distrito Judicial de Lima Norte.

Resultados de la entrevista.

La entrevista de profundidad, para la recolección de la opinión de los expertos en el tema de investigación, se ha formulado dos distintas guías de entrevista bastante vinculadas cada una de ellas, cuyas preguntas fueron previamente formuladas de acuerdo a la información requerida para el cumplimiento de los objetivos de la investigación. De ambos instrumentos, uno de ellos ha sido aplica do para expertos en Ecuador, Colombia, España, Argentina y Perú, mientras el otro instrumento ha sido aplicado concretamente a un experto nacional, esto con la finalidad de lograr con la obtención de algunos datos más precisos de relevancia interna, con la finalidad de que el análisis de los resultados sea mucho más completo e interesante, tomando el problema de investigación desde diversas perspectivas.

Cabe resaltar también que los resultados de la entrevista se presentan de acuerdo a los objetivos de la investigación, en la medida que las preguntas de entrevista fueron formuladas de acuerdo a los objetivos planteados, asimismo, la presentación de los resultados son acordes a las categorías y subcategorías, ya que el objetivo general es la fusión de las categorías y los objetivos específicos fueron formulados de acuerdo a las subcategorías.

Respecto al objetivo general, que consiste en analizar el tratamiento jurídico penal de los delitos informáticos contra el patrimonio, Distrito Judicial de Lima, 2018.

Categoría: Tratamiento jurídico penal

Tabla 6:
El acelerado avance de las tecnologías informáticas y comisión de delitos

Experto	País	Respuestas
Acurio (2018)	Ecuador	El uso y masificación de las Tecnologías de la Información y la Comunicación, a supuesto varios avances en la ciencia y la tecnología, pero también se ha convertido en un factor criminógeno que ha permitido la comisión de nuevas modalidades de delitos, los cuales dependiendo de la legislación

		podrían no encontrarse tipificados, lo cual es una problema al momento de su persecución, desde la perspectiva del principio de legalidad.
Manjarres (2018)	Colombia	Pareciera que van al mismo ritmo, sobre todo en lo que concierne al robo de datos. Las diferentes entidades, sean de comercio o de servicios, en su afán de captar más usuarios, incitan en un momento dado, a que las personas para hacer uso de estos ofrecimientos, exponen sus datos personales, exponiéndolos con esto a que sean víctimas potenciales para la comisión de este tipo de delitos.
Álvarez (2018)	España	Hoy en día, el avance de las tecnologías y el fácil uso de las mismas, han proporcionado herramientas a los delincuentes, con los que cometer delitos más sofisticados y mucho más difícil de identificar.
Semprini (2018)	Argentina	*Creo que la el avance tecnológico va de la mano de los distintos delitos cometidos con dispositivos tecnológicos. Pero más allá de eso, considero que es necesario que los organismos de investigación especializados, cuenten con personal capacitado y formado para llevar adelante esas investigaciones y así obtener resultados favorables en la investigación.*
Peña (2018)	Perú	*La tecnología, no solo ha traído la mejora de la calidad de vida de la población global, sino también las actividades delictivas se han modernizado en su actuar delincuencial mejorando obstenciblemente su performance criminal.*
Silva (2018)	Perú	*Que el aumento de la criminalidad en el ámbito de tecnologías informáticas obedece al propio avance de la criminalidad en nuestro País, atendiendo a que dicho fenómeno no solo se encuentra relacionado*

	con este tipo de delitos sino con la delincuencia en general, que al no ser contrarrestadas oportunamente por el Estado su incremento crece exponencialmente, mas aún si se tiene presente el creciente avance y permanente innovación del sector tecnológico.

Análisis interpretativo

Los entrevistados coinciden que la criminalidad informática va de la mano con el acelerado avance de las tecnologías informáticas, permitiendo nuevas modalidades de comisión de delitos cada vez más sofisticados, difíciles de identificar, por lo que es necesario contar con organismos y funcionarios especializados para llevar adelante las investigaciones con resultados favorables.

Tabla 7:
Eficiencia de la legislación para sancionar las nuevas formas delictivas con el uso de las tecnologías informáticas

Experto	País	Respuestas
Acurio (2018)	Ecuador	En el Ecuador con la expedición del Código Orgánico Integral Penal, se amplió el espectro de los delitos informáticos, mejorando la redacción y ampliando tipos que no existían contemplados antes en el Código Penal anterior, eso fue un avance en la legislación.
Manjarres (2018)	Colombia	La intangibilidad de estos delitos hacen parecer o dan la sensación, en un momento dado, que la legislación existente no es capaz de enmarcar estos delitos y sancionarlos de una forma eficaz.
Álvarez (2018)	España	Cada día es más eficiente y efectiva la legislación referente a los Delitos Informáticos. En España se ha realizado un gran avance en legislar en referencia en esta clase de delitos, con la actualización del Código

		Penal en el año 2015, se dio un gran paso en este asunto.
Semprini (2018)	Argentina	No creo que sea eficiente nunca, porque siempre la tecnología y las nuevas formas delictivas, va más rápido que el derecho. Pero si considero que es necesario ir trabajando para mejorar la legislación y/o adherirse a distintos convenios internacionales para ir combatiendo dichos delitos.
Peña (2018)	Perú	Aún falta no solo legislar sobre las nuevas actividades delictivas, sino también difundir y explicar la nueva criminalidad informática en su connotación holística.
Silva (2018)	Perú	La legislación existente resulta insuficiente, toda vez que continuamente se renuevan las modalidades delictivas en el ámbito informatice, asimismo si se tiene presente que en nuestro país las herramientas existentes para contrarrestar dichos ilícitos no resultan ser suficientes, y que poco es el efecto disuasivo en la proliferación del mismo.

Análisis interpretativo

En Ecuador y en España se han realizado buenas reformas respecto a los delitos informáticos, ampliándose la redacción de los tipos penales no contemplados, actualizándose la legislación penal. Por otro lado, los entrevistados de Colombia y Argentina consideran que la legislación sobre delitos informáticos es insuficiente para sancionar en forma eficaz las nuevas formas delictivas con el uso de las tecnologías informáticas. Con esta última respuesta coinciden los entrevistados nacionales señalando que la legislación es insuficiente y esto va acompañado de la falta de difusión de la criminalidad informática.

Tabla 8:
Inclusión de estafa, hurto y sabotaje informático dentro del nomen iuris "fraude informático

Experto	País	Respuestas
Acurio (2018)	Ecuador	No me parece, los fraudes informáticos son específicos, pertenecen a las defraudaciones en genérico, es un delito de carácter patrimonial, pero diferente del hurto y sabotaje.
Manjarres (2018)	Colombia	La comisión de estos delitos en lo que respecta a espacio, tiempo y forma, no da para que se les nomine de esta forma.
Álvarez (2018)	España	Si claro, El Modus Operandi actual de este tipo de delitos, está basado en el uso de las nuevas tecnologías, en especial, el uso de Internet, es por ello que el encajarlo en “Fraude Informático”, es totalmente correcto.
Semprini (2018)	Argentina	Si por supuesto, siempre en todos los casos debiéndose demostrar con las distintas pericias que sean necesarias el fraude cometido.
Peña (2018)	Perú	Sí, porque todo los delitos tienen un componente de dañosidad de engaño, de allí que esta circunscritos en el fraude informático, para que guarde relación con el convenio de Budapest, pero a mi punto de vista no es suficiente.
Silva (2018)	Perú	Al respecto el delito de fraude informatice se encuentra previsto y sancionado en el artículo 8 de la Ley N° 30096, que sanciona la alteración, supresión, borrado de datos informáticos o cualquier interferencia o manipulación en el funcionamiento de un sistema informático, por lo que en estricto se refiere a cualquier tipo de manipulación de datos o el funcionamiento de un sistema, por lo que la estafa, no corresponde ser comprendidas dentro del mismo, sin embargo respecto al sabotaje, se entiende que ello corresponde a la alteración en cualquier modalidad de datos en un sistema informático, por lo

	que puede entenderse dentro del mismo, empero respecto al hurto no existe un verbo rector que incluya dicha modalidad, lo cual más bien podría ser contemplada dentro del tipo penal Interceptación de Datos informáticos previsto en el artículo 7 de la citada ley.

Análisis interpretativo

Se concluye que los entrevistados de España y uno de Perú manifiestan que es adecuado comprender a la estafa, hurto y sabotaje informático dentro del *nomen iuris* "fraude informático, sin embargo, Acurio (2018) entrevistado de Ecuador, Manjarres (2018) entrevistado de Colombia y Silva (2018) entrevistado de Perú discrepan con dicha postura, puesto que el primero considera que el los fraudes informáticos son específicos, pertenecen a las defraudaciones en genérico, es un delito de carácter patrimonial, pero diferente del hurto y sabotaje, y no da para que se les nomine solo como fraude, y finalmente, se señala que el fraude se refiere a cualquier tipo de manipulación por lo que la estafa no corresponde ser comprendida, pero el sabotaje podría cuadrar dentro del fraude por tratarse de alteración de datos, pero sobre el hurto no existe un verbo rector.

Respecto al primer objetivo específico, que consiste en analizar el tratamiento jurídico penal de los delitos informáticos contra el patrimonio en su modalidad de hurto.

Categoría: Hurto informático

Tabla 9:
Disposición de los bancos para denunciar penalmente delitos de hurto sistemáticos de cuentas bancarias y otros

Experto	País	Respuestas
Acurio (2018)	Ecuador	Bueno el hurto sistemático, hay que aclararlo, ya que por principio de legalidad en el Ecuador no existe el hurto informático, lo que existe es el Fraude

		Informático o puede ser Peculado Bancario, dependiendo de los hechos.
Manjarres (2018)	Colombia	En cuanto a si los Bancos denuncian esos tipos penales, hay que recordar que muchos de ellos quedan como cifra negra, debido a que podrían constituir un atentado a la imagen corporativa del Banco, y por ello en muchos casos buscan solucionar esos problemas de forma interna. Sin acudir a la Administración de Justicia o a la Fiscalía General del Estado. Si lo deben hacer tanto por el bien de los clientes como el de su misma imagen, aunque en algunos casos tratan de minimizar el daño que les han causado para, precisamente, mantener su clientela.
Álvarez (2018)	España	Si, Por supuesto, mi experiencia en la investigación relacionadas con entidades bancarias, me ha proporcionado la evidencia de total colaboración y disposición, no solo a la denuncia de los mismos, si no a prestar total colaboración en las investigaciones que se llevan a cabo.
Semprini (2018)	Argentina	No, porque en realidad sería un desprestigio como institución y haría denotar que no cuenta con la seguridad necesaria, y haría perder la confianza de sus clientes o posibles nuevos clientes.
Peña (2018)	Perú	Solo cuando estos son significativos, ya que no lo hacen públicos con frecuencia, por el tema de no provocar “pánico financiero” y de eso se aprovecha la criminalidad informática.
Silva (2018)	Perú	Considero que en la mayoría de casos no, por la imagen de su entidad, dado que ello pone en evidencia las falencias de su seguridad, y que también implica un resarcimiento económico, de verificarse que la falla fue del sistema de la propia

	entidad, sin embargo en los casos que fuere por descuido y negligencia del propio cliente lo común es que lo pongan en conocimiento de los usuarios o la autoridad competente, pero ello es cuando existe una significativa cantidad de casos similares.

Análisis interpretativo

Casi todo los entrevistados coinciden que los bancos no están dispuestos a denunciar penalmente delitos de hurto sistemáticos de cuentas bancarias y otros por la protección de su imagen corporativo, para mantener la clientela, para evitar su propio desprestigio y no hacer denotar la inseguridad, por no perder la confianza de sus clientes y futuros clientes y evitar el pánico financiero, sin embargo, Álvarez (2018) entrevistado de España señala que los bancos Españolas si están dispuestos a colaborar en la denuncia e investigación criminal.

Tabla 10:
Regulación específica del delito de hurto informático, tipicidad y prevención

Experto	País	Respuestas
Acurio (2018)	Ecuador	No existe en la legislación penal del Ecuador, doctrinalmente puede existir el hurto de servicios de telecomunicaciones.
Manjarres (2018)	Colombia	Sí. En nuestro código penal con la expedixción de la ley 1273 de 2009 allí se tipifica el delito de Hurto informático en el artículo 13.
Álvarez (2018)	España	Como tal no existe, pero está incluido en el artículo 248 del Código Penal Español, con el concepto “Fraudes Informáticos”.
Semprini (2018)	Argentina	Contamos en la Argentina con la ley 26388 de delitos informáticos, pero no está especificado el hurto informático.
Peña (2018)	Perú	Existió en el artículo 186 del C.P., segundo párrafo numeral 3, modificado por la ley 26319, que disponía

		además “la pena será no menor de 4 años ni mayor de 8 años, “si el hurto es cometido mediante la utilización de sistemas de transferencia electrónica de fondos de la telemática en general o la violación del empleo de claves secretas”, y fue derogado por la DCD única de la ley 30096, modificada por la ley 30171.
Silva (2018)	Perú	Al respecto existe la Ley N° 30096, que sanciona la interceptación ilegitima de datos informáticos, el cual podría entenderse como hurto al apoderarse de datos de manera ilegal pertenecientes a un tercero, y que si bien de alguna manera se protege los datos informáticos, nuestra regulación resulta incipiente en este aspecto. Al resultar incipiente la regulación de los delitos informáticos, ello implica ciertas falencias tales como la tipificación, y que de acuerdo a nuestra legislación el hurto informático como tal no se encuentra previsto, sino a través del apoderamiento de datos informáticos, o la manipulación, supresión, clonación de los mismos.

Análisis interpretativo

En la legislación penal ecuatoriana no existe regulación expresa del hurto informático, mientras en la legislación Española, tampoco existe regulación expresa, pero está comprendido dentro de fraudes informáticos, en el caso peruano si había una regulación en el artículo 186 del código Penal, sin embargo fue derogada por la Ley 30096 modificada por la Ley 30171. A diferencia de las demás legislaciones, en Colombia si existe regulación expresa del delito de hurto informático, el cual está tipificada en la Ley 1273.

Al cual, en el ámbito nacional, Silva (2018) señala que interceptación ilegitima de datos informáticos, el cual podría entenderse como hurto al apoderarse de datos

de manera ilegal pertenecientes a un tercero, sin embargo, admite que la legislación peruana es incipiente y tiene ciertas falencias.

Respecto al segundo objetivo específico, que consiste en analizar el tratamiento jurídico penal de los delitos informáticos contra el patrimonio en su modalidad de fraude.

Categoría: Fraude informático

Tabla 11:
Vulnerabilidad de las personas y empresas de ser víctimas de fraude informático, y tipificación de todo los delitos informáticos contra el patrimonio como fraude

Experto	País	Respuestas
Acurio (2018)	Ecuador	Los atacantes informáticos, buscan aprovechar la falta de conocimiento y previsión de las víctimas. Falta una cultura de Ciberseguridad que es aprovechada por los atacantes para cometer este tipo de delitos. En especial la llamada ingeniería social.
Manjarres (2018)	Colombia	Totalmente. En esta época el uso masificado de los elementos para comunicación y la aparición de las llamadas redes sociales nos exponen a que nuestros datos personales estén expuestos para que de allí sean utilizados por este tipo de delincuentes para iniciar su accionar delictivo.
Álvarez (2018)	España	Por supuesto, En las ponencias que de vez en cuando hago, es un tema en la hago especial insistencia. Nunca se puede estar completamente seguro en este mundo en el que vivimos, siempre hay que estar en alerta y preparados ante cualquier fraude. El más común en estos últimos tiempos es el que se comete a través de “CRYPTOLOCKER”, consistente en encriptar todos los archivos del disco

		duro y a continuación solicitar una elevada cantidad de dinero, para desencriptarlos.
Semprini (2018)	Argentina	Si y siempre lo estarán, porque la seguridad absoluta no existe, si se deben tomar todos los recaudos de seguridad pertinentes, pero siempre hay acciones delictivas nuevas que el usuario común o personal de empresas no está al tanto o capacitados, permitiendo accesos indebidos a datos valiosos personales o de la empresa por ejemplo los casos de Ramsomware.
Peña (2018)	Perú	Si, por la naturaleza de sus actividades donde el factor económico es determinante para la delincuencia online.
		Todas las personas, naturales o jurídicas, son susceptibles de ser agraviados en este tipo de delitos, por cuantos ello implica el aprovechamiento a través de tecnologías en un sistema determinado, o los datos que se transfieren a través de medios tecnológicos.
Silva (2018)	Perú	Considero que es el punto de partida para el desarrollo de una legislación contra este tipo de delitos, puesto que resulta insuficiente un solo tipo penal para dicha tipificación, pero ello ya es un avance, teniendo presente, que con anterioridad a la presente legislación especial, existía solo unos artículos dentro del Código Penal, y que debido al avance de la actividad criminal en este ámbito el legislador tuvo a bien la dación de la referida norma.

Análisis interpretativo

Todo los entrevistados coinciden que tanto las personas como las empresas están expuestos a ser víctimas de fraudes informáticos, los atacantes informáticos se aprovechan de la falta de conocimiento y cultura de ciberseguridad de sus

víctimas, nunca de puede estar de todo seguro y siempre se estará expuesto a potenciales fraudes, y últimamente se viene practicando nuevas modalidades como la “CRYPTOLOCKER” y Ramsomware, modalidad, mediante el cual se encripta o restringe el acceso a archivos de la víctima, pidiendo grandes cantidades de dinero para desincriptarlos, es decir, para que su propietario pueda obtener la clave y acceder a los archivos “secuestrados”.

De la respuesta de Silva (2018) se desprende que legislación contra los delitos informáticos contra el patrimonio resulta insuficiente al establecer en un solo tipo penal para todas las modalidades para de delitos informáticos contra el patrimonio, sin embargo considera que es un avance por lo menos en sanción de estos delitos.

Tabla 12:
Existencia de estrategias claras para la prevención y sanción de delitos de fraude informático

Experto	País	Respuestas
Acurio (2018)	Ecuador	Para la sanción de los Fraudes existen las normas del Código Orgánico Integral Penal. En el campo de la prevención, falta la aplicación de normas como la ISO 27000 sobre la Seguridad de la Información por parte de las entidades públicas y privadas. Las instituciones financieras deben emprender campañas de información sobre las modalidades de fraudes informáticos, tales como el pishing o el pharming a fin de que los usuarios de la banca virtual no sean perjudicados. Al igual sobre las tarjetas de crédito y débito que pueden ser clonadas fácilmente y así perjudicar a sus tenedores.
Manjarres (2018)	Colombia	Si, sobre todo en las entidades bancarias y en las dependencias del gobierno, el tratamiento de y uso de los datos personales están protejidos por ley.
Álvarez (2018)	España	Si, efectivamente, en España existe claras estrategias para la lucha y prevención de este tipo de

		fraudes, entre otras el refuerzo en las leyes que tratan de estos temas, como también una campaña de información para detectar estos delitos y saber actuar ante ellos.
Semprini (2018)	Argentina	Creo que el convenio de Budapest lo considera.
Peña (2018)	Perú	No las hay, el estado no formula una cultura de prevención de criminalidad informática. En Argentina, el estado tiene un protocolo de grooming que lo difunde a la sociedad igualmente en chile, aca no existe nada parecido, tampoco existe el delito de sexting (muy comun en la posmodenidad).
Silva (2018)	Perú	Tengo entendido que a través de la SBS se realizan campañas de información a las personas respecto a las actividades delictivas en entidades financieras, y que por intermedio de la Policía Nacional del Perú también se informa preventivamente sobre diversos ilícitos en este área, sin embargo, resulta insuficiente, puesto que at igual que los delitos de Lavado de Activos o Trafico de Drogas es necesario una política criminal especifica.

Análisis interpretativo

A diferencia de Ecuador, Colombia, España y Argentina, en el Perú no existen estrategias claras para la prevención y sanción de delitos de fraude informático.

En ecuador existe ISO 27000 sobre la Seguridad de la Información por parte de las entidades públicas y privadas, en España aparte de la legislación, existen campañas de información para detectar estos delitos y saber actuar ante ellos y en Argentina existe el protocolo de grooming que lo difunde a la sociedad sobre los fraudes informáticos.

Del cual se desprende que en el Perú no se ha tomado en cuenta la real dimensión de los delitos informáticos, puesto que se actúa únicamente en forma

reactiva, no existe legislación adecuada ni políticas de prevención de delitos informáticos contra el patrimonio.

Respecto al tercer objetivo específico, que consiste en analizar el tratamiento jurídico penal de los delitos informáticos contra el patrimonio en su modalidad de estafa.

Categoría: Estafa informática

Tabla 13:
Confiabilidad de las plataformas informáticas para realizar compras y contratar servicios a través de internet y tipicidad de estafa informática

Experto	País	Respuestas
Acurio (2018)	Ecuador	Todo depende de la plataforma, si esta cumple con los estándares como: **ISO 27001:2013:** Buenas prácticas para el manejo de sistemas de información y proceso de datos. **PCI DSS:** Transacciones y pagos con tarjetas de crédito. **OWASP ASVS:** Seguridad de aplicaciones web Si el sitio o página web tiene estas seguridades se puede realizar transacciones seguras.
Manjarres (2018)	Colombia	Personalmente no realizó ningún tipo de compras por internet. Tramites si, donde este seguro que la información suministrada va a tener un tratamiento adecuado.
Álvarez (2018)	España	Soy una persona que compra a menudo por Internet, y me generan mucha confianza, claro está, que siempre realizo estas comprar en plataformas de compañías de confianza y de renombre. Los problemas pueden surgir, cuando se realizan en páginas web extranjeras que no tienen los certificados de seguridad mínimos, ni con un nombre conocido.
Semprini	Argentina	Sí, siempre tomando las precauciones pertinentes.

(2018)		
Peña (2018)	Perú	No genera confianza, y principalmente por la brecha digital, el Perú tiene el porcentaje más bajo de comercio electrónico en la Región.
Silva (2018)	Perú	Al respecto existen ciertas medidas de seguridad a seguir, tales como la fiabilidad de las páginas web de compra, y seguir las políticas de seguridad de dichas entidades. Si, dado que las modalidades más frecuentes se encuentran tipificadas, sin embargo aún es insuficiente dado la creciente actividad criminal en dicho ámbito.

Análisis interpretativo

Se concluye que las plataformas informáticas generarán confianza para realizar compras y contratar servicios a través de internet siempre que cumplan estándares de seguridad que garanticen realizar las transacciones sin riesgo, o que la compañía sea uno conocido de renombre, puesto las compañías extranjeras que no tengas los certificados de seguridad mínimos genera desconfianza para realizar cualquier tipo de transacción. Al cual agrega Silva (2018) al decir que la legislación penal peruana resulta insuficiente dado la creciente actividad criminal, pese a que considera que se cumple con el principio de tipicidad en la sanción de la estafa informática.

Tabla 14:
R regulación específica del delito de estafa informática

Experto	País	Respuestas
Acurio (2018)	Ecuador	La estafa informática es básicamente un delito computacional, más no informático. Es decir que para lograr el engaño del sujeto pasivo se lo hace a través por ejemplo de un anuncio en la página web, donde se vende un producto a menor precio que el que se puede conseguir en una tienda, por ejemplo un reloj ROLEX en USD. 1.000 dólares. El sujeto

		pasivo ve ese anuncio, se contacta con el sujeto activo, quien le dice que debe hacer una transferencia a una cuenta, o a través de Western Union o Money Gram, luego el sujeto activo, recibe la transferencia y envía el paquete al sujeto pasivo, quien al recibirlo encuentra una foto del ROLEX, por tanto se da cuenta que ha sido estafado, siendo medio fraudulento el engaño o abuso de confianza que generó el error sicológico en el sujeto pasivo que le llevo a la disposición patrimonial lesiva.
Manjarres (2018)	Colombia	Si está regulado. (ver Ley 1273 de 2009 Colombia)
Álvarez (2018)	España	En nuestra legislación, en concreto en el artículo 248 del Código Penal, referente a La Estafa, aunque no se especifica la estafa informática, el desarrollo de dicho artículo, es de gran utilidad para poder tratar estos delitos.
Peña (2018)	Perú	En el Perú no se sancionan correctamente los delitos informáticos como la estafa informática: solo el acceso ilícito; atentados contra la integridad de datos; delitos contra la indemnidad sexual; delitos contra la intimidad y secreto de las comunicaciones y contra la fe pública. (Copia del convenio de budapest).

Análisis interpretativo

Acurio (2018) entrevistado de Ecuador señala que la estafa es un delito computacional que consiste en lograr engañar a la víctima, es decir, generar error psicológico en la víctima que le conduzca al desprendimiento patrimonial, por otro lado, Manjarres (2018) entrevistado de Colombia señala que en su país si existe la regulación específica de la estafa informática, el cual se encuentra en la Ley 1273 de 2009, por el contrario, Álvarez (2018) advierte que en la legislación Española no existe en concreto la regulación específica de estafa informática,

pero el artículo 148 referente a la estafa es de gran utilidad para tratar el delito de estafa.

Por otro lado, Peña (2018) entrevistado peruano, señala que en el Perú no se sancionan correctamente los delitos informáticos como la estafa informática. En este sentido, se puede concluir que en el Perú no se ha tipificado en forma expresa la estafa informática.

Respecto al cuarto objetivo específico, que consiste en analizar el tratamiento jurídico penal de los delitos informáticos contra el patrimonio en su modalidad de sabotaje informático.

Categoría: Sabotaje informático

Tabla 15:
Afectación al patrimonio de la víctima con la destrucción de la información y softwares en la red y tipicidad de sabotaje

Experto	País	Respuestas
Acurio (2018)	Ecuador	Depende de la información, si esa información está en la nube o almacenada en un dispositivo de almacenamiento. Ya que esta puede tener respaldo. También depende del tipo de información que ha sido destruida, ya que ahora la información puede tener una valor económico para la víctima y eso puede causarle un perjuicio patrimonial, pero como esta clase de delitos son de tipo pluriofensivo también puede afectar a la disponibilidad de la información y a su integridad.
Manjarres (2018)	Colombia	Si claro sobre todo el llamado patrimonio intelectual porque la victima ha dedicado tiempo, estudio e investigación en la elaboración de estos.
Álvarez (2018)	España	En muchos casos, si, efectivamente, a nivel particular, muchas personas que han sufrido algún caso de destrucción de información, han tenido que recurrir a empresas externas, que se dedican a

		recuperar datos perdidos, con el consecuente gasto monetario. A nivel de empresas, la destrucción de datos, aparte del gasto en su recuperación, también está el descredito ante sus clientes, los cuales pueden optar por cambiar de empresa.
Semprini (2018)	Argentina	Si porque esa información y/o datos que se encuentran dentro de un software o sistema es información personal, es por ello que la ley 26388 prevé condenas para esos casos.
Peña (2018)	Perú	Si ya que el patrimonio de la víctima no solo es material sino también inmaterial, en esta posmodernidad de la dictadura de la NTICS.
		Si, dado que resulta un bien no tangible de la víctima, más aún, si la misma puede ser susceptible para la obtención de bien económico, tales como códigos de seguridad que permitan el acceso cuentas bancarias u otros.
Silva (2018)	Perú	Lo que se tipifica es la manipulación de datos en diversas modalidades, lo cual se traduce en la alteración de los datos informáticos, por lo que si bien es cierto se señala cuáles son los hechos sancionados, estos aún resultan insuficientes para todas las modalidades existentes.

Análisis interpretativo

Los entrevistados consideran que cuando un pirata informático destruye información y softwares en la red afecta el patrimonio de la víctima, puesto que como señala Acurio (2018) ahora la información puede tener una valor económico para la víctima y eso puede causarle un perjuicio patrimonial, con ello concuerda Manjarres (2018) al decir que la víctima ha dedicado tiempo, estudio e investigación en la información destruida.

Se debe tener en cuenta que el perjuicio patrimonial no solo es en razón a la destrucción de la información en sí, sino que, además, la empresa o persona, a

efectos de recuperar la información destruida suele contratar profesionales o empresas externar, cuya contratación se traduce en un desprendimiento patrimonial como consecuencia de la destrucción de la información. El patrimonio no solo es material, sino también inmaterial. Agrega Silva (2018), que la legislación penal peruana es insuficiente para la sanción de sabotaje informático.

Tabla 16:
Regulación específica del delito de sabotaje informático

Experto	País	Respuestas
Acurio (2018)	Ecuador	En el caso ecuatoriano existe el delito de daños informáticos. Art. 232 COIP.
Manjarres (2018)	Colombia	Si existe este tipo penal (ver Ley 1273 de 2009).
Álvarez (2018)	España	En el Código Penal Español, como tal, no está reflejado, pero concretamente en el Artículo 264, viene especificado como Daños Informáticos y en cual, entra ese delito.
Peña (2018)	Perú	Estuvo en el artículo 207-b del Código Penal, y ahora en la Ley 30096 y modificada por la ley 30171, en el artículo 3: atentado contra la integridad de datos informáticos.

Análisis interpretativo

Conforme señala Acurio (2018) en Ecuador existe un delito símil al sabotaje informático, el cual es el delito de daños, asimismo, en la Legislación colombiana también existe regulado en la Ley 1273 de 2009, sin embargo, en el Código Penal Español no se encuentra tipificado como tal, pero el Artículo 264 del Código Penal Español, al igual que de Ecuador, regula como Daños informáticos, tipo penal en la que se puede cuadrar correctamente el sabotaje informático. A diferencia de los países antes nombrados, en la legislación penal peruana no existe en forma expresa la tipificación de delito de sabotaje informático, pero es posible que se puede encuadrar como atentado contra la integridad de datos informáticos conforme al artículo 3 de la Ley 30171 que modificó a la Ley 300096, sin

embargo, se puede advertir que no se estaría cumpliendo con el principio de tipicidad para sancionar los delitos de sabotaje informático.

Tabla 17:
Vigente regulación de los delitos informáticos contra el patrimonio y su efectividad en la prevención de delitos

Experto	País	Respuestas
Acurio (2018)	Ecuador	En la legislación ecuatoriana están comprendidas viarias modalidades de fraudes informáticos que permite su persecución, la única limitante puede ser que al ser delitos de tipo transnacional las evidencias o pruebas estén en otra jurisdicción, por ello la necesidad se suscribir el Convenio del Cibercrimen de la Comunidad Europea que permitiría una mejor cooperación internacional en el caso de los delitos informáticos y cibernéticos.
Manjarres (2018)	Colombia	La regulación por si sola no contribuye con la prevención de estos delitos. Se necesitan campañas educativas eficaces que alerten a las personas cuando utilicen cualquier medio informático del riesgo de ser víctima de estos delitos y la forma de evitarlos.
Álvarez (2018)	España	Las leyes Españolas, previenen los delitos informáticos contra el patrimonio, existe una extensa jurisprudencia al respecto. Pero si es verdad, que debería ser más concreta y una legislación Global, ya que en el momento que esos delitos, provienen de fuera de nuestras fronteras, la investigación se hace más difícil.
Peña (2018)	Perú	No completamente, se tiene que incluir: la estafa informática de manera indubitable, asimismo, la usurpación de identidad (la suplantación no basta).

Silva (2018)	Perú	Es insuficiente, dado que solo se prevee un solo tipo penal contra el patrimonio.

Análisis interpretativo

Álvarez (2018), señala que leyes Españolas, previenen los delitos informáticos contra el patrimonio, pero advierte que debería ser más concreta y una legislación Global, ya que en el momento que esos delitos, provienen de fuera de nuestras fronteras, la investigación se hace más difícil, concordante a ello Acurio (2018) señala que el limitante puede ser que al ser delitos de tipo transnacional las evidencias o pruebas estén en otra jurisdicción. Por otro lado, Manjarres (2018) señala que la regulación por sí sola no contribuye con la prevención de estos delitos. Se necesitan campañas educativas eficaces.

La legislación peruana no previene los delitos informáticos contra el patrimonio, dado que la norma es una sola y genérica para todas las modalidades de delitos contra el patrimonio, por lo que se está lejos de la prevención.

Tabla 18:
Necesidad de reforma legislativa para prevenir y sancionar los delitos informáticos contra el patrimonio

Experto	País	Respuestas
Acurio (2018)	Ecuador	En el caso ecuatoriano no es necesario, con el actual COIP
Manjarres (2018)	Colombia	La legislación debe ir a la par de los diferentes cambios tecnológicos y sobre todo en lo que respecta a la seguridad cuando se manejan datos personales o corporativos.
Álvarez (2018)	España	Considero, que siempre es necesario mejorar las leyes y reformarlas, los delincuentes siempre están actualizando sus métodos y procedimientos para la realización de delitos, es por ello, que la reforma legislativa para la lucha del Delito Informático, y no solo, el referente al Patrimonio, si no, a todos lo que

		abarcan este tipo de Delitos Informáticos.
Peña (2018)	Perú	Si para perfeccionar los delitos informáticos contra el patrimonio de manera específica: estafa informática y usurpación de identidad.
Silva (2018)	Perú	Considero que debe extenderse los tipos penales en esta ley especial.

Análisis interpretativo

La mayoría de los entrevistados consideran que es necesario una reforma legislativa para prevenir y sancionar los delitos informáticos contra el patrimonio, y se hace énfasis que no solo debe ser respecto a los delitos informáticos contra el patrimonio, sino, sobre las demás modalidades de delitos informáticos, puesto que de acuerdo a las nuevas tecnologías informáticas existen nuevas modalidades de comisión de delitos y la legislación penal debe estar a la altura para prevenir y sancionar.

Tabla 19:
Opinión o aporte adicional de los expertos sobre el tema en estudio

Experto	País	Respuestas
Acurio (2018)	Ecuador	Debe haber claridad terminológica en el tema de los delitos informáticos en especial sobre los fraudes informáticos desde el punto de vista de la tipicidad objetiva.
Manjarres (2018)	Colombia	Este tipo de investigación contribuye a que se tenga una mayor y mejor información sobre los delitos informáticos y su legislación lo cual sirve para prevenir a las personas que la consultan, ser víctima de este tipo de delitos.
Álvarez (2018)	España	Este tipo de asuntos, son desgraciadamente muy desconocidos por la población en general, y es interesante que se dé información al respecto, para no caer en esta clase de delitos.

		Si entre muchas, que se proponga al Congreso de la República por parte de las instituciones con iniciativa legislativa y la sociedad civil, la adhesión del Perú al convenio de Budapest.
Peña (2018)	Perú	En América solo lo han ratificado: USA, Canadá, Panamá, República Dominicana y el 2017 Chile, el no existir una legislación uniforme en delitos informáticos genera dualidad de delitos y problemas de interpretación dogmática, y además, la migración de la delincuencia on line a esta parte del planeta ya que la criminalidad informática, sabe que la legislaciones diferentes en cada país latinoamericano son una ventaja para que estas nuevas conductas delictivas sigan cubiertas bajo el manto de la impunidad.
Silva (2018)	Perú	Que para la resolución de estos tipos de delitos, es necesario el apoyo técnico del área encargada, esto es, la División de Delitos Informáticos de la PNP la cual no se abastece debido a la carga delictiva, más aun si se encuentra centralizada en la DIRINCRI en Lima, y que tampoco cuenta con todas las herramientas necesarias para encontrarse a la par con la delincuencia que se innova a diario.

Análisis interpretativo

Entre los principales aportes u opiniones de los expertos, claridad terminológica en el tema de los delitos informáticos en especial sobre los fraudes informáticos desde el punto de vista de la tipicidad objetiva, los delitos informáticos son muy desconocidos por la población en general, el Perú se debe adherir al convenio de Budapest y que en el Perú se debe ampliar el radio de acción de División de Delitos Informáticos de la PNP e implementar las herramientas necesarias.

V. Discusión

Respecto a la discusión de los resultados de la investigación, Lerma (2011) señala que el objetivo de la discusión es “(…) mostrar las concordancias y diferencias de los propios resultados con los encontrados por otros investigadores, y que ya fueron mencionados en el marco de referencia del estudio (…)” (p. 70). En este orden de ideas, tomando en cuenta que la discusión es el contraste crítico de los resultados de la investigación con los antecedentes o trabajos previos respecto al problema de estudio, así como con las teorías relacionadas al tema, el cual, en la presente investigación se presenta de la siguiente manera.

En el supuesto general de la presente investigación se enfatizó que el tratamiento jurídico penal de los delitos informáticos contra el patrimonio es deficiente por comprender dentro de fraude informático todo los tipos o modalidades de delitos informáticos contra el patrimonio, generando éste incertidumbre en la interpretación de la norma, no permitiendo la sanción efectiva de los delitos informáticos contra el patrimonio.

En el ámbito extranjero, citado como trabajos previos, Wang (2016) encontró que China tiene un sistema de regulación de niveles múltiples en malas acciones cibernéticos, sin embargo, los EE.UU. pese a que logra penalizar las malas acciones cibernéticos no está exenta de problemas puesto que la legislación de los Estados Unidos sobre la ciberdelincuencia menos consistente, y esa incompatibilidad conduce a problemas en la práctica judicial. Por otro lado, encontró que Singapur ha sido activo en la promulgación y modificación de su Ley sobre Abusos Informáticos.

Es así que se pudo advertir que los países como China, los Estados Unidos, Inglaterra y Singapur han experimentado reformas significativas para adaptar su legislación penal. Mientras a nivel internacional, el Consejo de Europa ha lanzado seminarios y proyectos que analizan el cibercrimen y exploran soluciones, y ha redactado la Convención sobre Ciberdelincuencia, sin embargo, estas contramedidas son insuficientes todavía para el cibercrimen, por la naturaleza de delitos y limitación en la cobertura de la ley penal.

En este sentido, si bien en la legislación peruana existen legislaciones, modificaciones normativas con fines investigación y sanción de los delitos informáticos, como se encontró en los resultados del estudio, la legislación es insuficiente para sancionar las diversas modalidades de los delitos informáticos contra el patrimonio, mucho menos se logra con la prevención de dichos ilícitos.

Del censo llevado a cabo en el año 2018, conforme al informe del Instituto Nacional de Estadística e Informática, el 99.7% de los hogares donde el jefe del hogar es con instrucción superior universitaria, tienen acceso a las Tecnologías de Información y Comunicación, 99.2% superior no universitaria y 96.6% secundaria, siendo entonces un alto índice de acceso a las Tecnologías de Información y Comunicación en los hogares peruanos, el cual constituye una oportunidad bastante grande para los ciberdelincuentes, toda vez que mientras mayor población tenga acceso a las tecnologías informáticas y menos sea el conocimiento de las medidas de seguridad, la posibilidad de comisión de diversos delitos informáticos contra el patrimonio aumenta, es decir, el riesgo de ser víctima de ciberdelito aumenta.

Uno de los delitos informáticos más notables y comunes es el hurto sistemático de los fondos de las cuentas bancarias, al respecto Abdulai (2016) encontró que la experiencia de victimización y los comportamientos de uso de internet están asociados positivamente con el temor de los estudiantes y su riesgo de convertirse en víctimas de fraude con tarjetas de crédito / débito. El cual implica que es todavía riesgosa la realización de transacciones por medios informáticos, en la medida que se exige revelación de los datos secretos de la tarjeta.

El uso masificado de internet ha aumentado la posibilidad de ser víctimas de cualquier tipo de delitos que se pueden concretar por dicho medio, es así que Alanzi (2015) en el estudio que realizó respecto a las percepciones de fraude en línea y el impacto sobre las contramedidas para el control del fraude en línea en las instituciones financieras de Arabia Saudí encontró que las personas son dependientes de Internet; la posibilidad de ser violado por los hackers y estafadores está creciendo, especialmente en lo que la socialización, compras en línea y la banca se llevan a cabo a través de computadoras personales o

dispositivos móviles, siendo que el fraude en línea ha sido descrito como una epidemia que se ha extendido a la mayoría de las actividades en línea.

Dicho estudio encontró que expansión de las actividades en línea y uso de información tecnologías en las transacciones bancarias crean oportunidades y lagunas explotadas por algunos estafadores en línea, lo que generó pérdida de más de 20 millones de dólares en 2010 y 2012 para Arabia Saudí. A diferencia de este estudio, si bien en el Perú no existen datos estadísticos respecto a las pérdidas que se generan como consecuencia de los delitos informáticos contra el patrimonio, lo es también que el Perú es un país incipiente en la regulación de estos tipos de delitos, y como evidencia de esto son las respuestas de los entrevistados, así como la propia ley de delitos informáticos que en cuyo capítulo relativo a los delitos informáticos contra el patrimonio, existe tipificado en forma expresa únicamente el fraude informático, sin embargo, en otros países, aunque no en todas, existe regulación específica de hurto, estafa y fraude informático.

El alcance teórico de estudio en esta investigación fueron el fraude, la estafa, el sabotaje y hurto informático como modalidades de delitos informáticos contra el patrimonio, sin embargo, es necesario advertir que dicha clasificación se realiza en estricta observancia del bien jurídico patrimonio y de acuerdo a las limitaciones doctrinarias y teóricas al respecto, puesto que creemos que los delitos nombrados no son los únicos que afectan el patrimonio, pudiendo expandirse en la tipificación a otras modalidades o clasificación distinta y más amplia. En este estudio se tomó la prioridad de analizar el fraude, la estafa, el sabotaje y hurto informático debido a la evidente observación de la existencia de dichos delitos y la inexistencia de norma penal específica para una prevención, investigación y sanción efectiva de estos tipos de delitos.

La comisión de los delitos informáticos no tiene fronteras, es decir, las limitaciones espaciales para su comisión, por cuanto con la sola tenencia de un ordenador, es factible la comisión del ilícito con efectos en otros países o continentes, sobre el cual, Rincón (2015) encontró que las fronteras creadas no son solo por el territorio, sino por el concepto de jurisdicción y competencia que son los delimitantes del ejercicio punitivo de los Estados, impiden que se investigue, juzgue y sancione a quienes hayan cometido la conducta desde un

territorio pero con consecuencias en otro, es decir, el delito se cometió desde un Estado pero las víctimas o el daño se materializan en otro estado, por lo que estas limitaciones y fronteras crea impunidad en la búsqueda y persecución de los delitos informáticos.

Es en este sentido, que el Estado peruano se encuentra incapacitado para la investigación y sanción de los delitos informáticos que se cometan por personas que se encuentran en otros países, pero cuyo efecto del delito recae en el Estado Peruano, puesto que aparte de las limitaciones tecnológicas para la investigación de estos delitos, existen graves limitaciones jurisdiccionales o de competencia, más si el Perú no ha ratificado el convenio de cibercrimibnalidad de 2001 (Convenio de Budapest).

En relación a ello, González (2013) encontró que la expansión exponencial de la ciberdelincuencia es innegable, y se trata de un fenómeno novedoso que cuyas prácticas delictivas requiere la intervención de los diferentes estados, y este tipo de delitos, su aparición y su desarrollo tienen, en contradicción con el lento avance del Derecho en el tratamiento jurídico penal de los delitos informáticos, puesto que estos delitos tienen un carácter trasnacional , por lo que nunca es suficiente la regulación protectora en un único Estado, puesto que para la comisión de los delitos informáticos, no se requiere la cercanía física, puede hacerlo tan lejos como el medio de comunicación o el internet tiene alcance. Al cual agrega Piccirilli (2015) es bastante alto el nivel de la ciberdelincuencia, y que la constante evolución del delito es la que provoca generar nuevas inquietudes, siendo necesario la creación de un órgano asesor técnico informático pericial.

Por otro lado, los trabajos previos a nivel nacional muestran que existen deficiencias en la regulación de los delitos informáticos, es así que Tenorio y Tuesta (2012) encontraron que la legislación del secreto bancario en el Perú, no es acorde con el avance tecnológico y el incremento de la criminalidad cibernética, pues el secreto bancario constituye un obstáculo en la investigación del delito de hurto informático de dinero, puesto que el secreto bancario se levanta exclusivamente por orden judicial en procesos concretos, el cual influye en la impunidad de los autores del delito de hurto informático de dinero. Mientras Sequeiros (2016) encontró que debido a la naturaleza virtual de los delitos

informáticos, estos se pueden volver confusos en su tipificación, ya que a nivel general, se poseen pocos conocimientos y experiencias en el manejo de ésta área.

Sin embargo, los resultados de la investigación demuestran que el Estado Peruano ha introducido modificaciones en el 2013 en la legislación penal, es así que se aprobó la ley de delitos informáticos y modificado ésta a efectos de que la legislación especial esté de acuerdo a los parámetros del convenio de Budapest, sin embargo es notable la deficiencia normativa para sancionar los delitos informáticos, especialmente a aquellos que afectan el patrimonio, toda vez que dentro de la legislación de delitos contra el patrimonio, únicamente se tipifica como fraude informático, sin contemplar otros tipos penales como la estafa informática, hurto informático y el sabotaje informático, el cual dificulta enormemente la investigación y sanción de los delitos informáticos contra el patrimonio. Los cuales son concordantes con los supuestos específicos planteados en esta investigación, puesto que tanto de la estafa, fraude, sabotaje ni fraude informático existe una regulación eficiente, sino una regulación ambigua y deficiente, cuyo tipo penal es insuficiente para la investigación y sanción de las modalidades de los delitos informáticos contra el patrimonio.

Por otro lado, Sánchez (2017) encontró que la adopción de estrategias de ciberseguridad incide significativamente en la protección de la información, mientras Alarcón y Barrera (2017) recomendaros que se debe involucrar a los docentes y directivos de las instituciones a que implementen módulos prácticos que permita a los estudiantes alejarse de las prácticas inapropiadas con el uso de la informática. Así como Espinoza (2017) admite que los delitos informáticos son transnacionales y multidisciplinarios conforme a lo ya analizado líneas arriba.

Sin embargo, se puede advertir que no existe sola investigación en forma específica de los delitos informáticos contra el patrimonio, siendo que las investigaciones relacionadas al tema han sido genéricas o de aspectos particulares de delitos informáticos, pero no respecto a los delitos informáticos contra el patrimonio, por lo que este aspecto de los delitos informáticos es todavía bastante incipiente, pese a que por primera vez se tipificó como delito informático aquello que afectaba el patrimonio y el surgimiento de delitos informáticos en el

Perú ha sido con fines de proteger el bien jurídico patrimonio. Asimismo, los delitos informáticos que afectan el patrimonio es la que cuenta con mayor incidencia a diferencia de los demás tipos de delitos informáticos.

Por otro lado, de las teorías relacionadas al tema de estudio, existen diferentes autores nacionales y extranjeros quienes manifiestan su punto de vista sobre la regulación, sanción y tratamiento de los ilícitos en estudio.

Que los delitos informáticos son delitos emergentes que cada vez varían de acuerdo al avance de las tecnologías informáticas, por lo que es necesario que todo el aparato judicial debe ir a la altura de ésta, es decir, debe estar en la capacidad de responder con una adecuada investigación y sanción de los delitos informáticos.

Uno de los grandes problemas en la sanción de los delitos informáticos no son sino la investigación y sanción, por el carácter de internacional o global que esta tiene, pues como es de verse del contenido de la investigación, el delincuente informático puede con toda facilidad cometer el ilícito desde un continente distinto al lugar de la víctima, por lo que se hace sumamente difícil la investigación y sanción, más cuando no existen organismos internacionales o países que cooperen con la investigación y sanción de estos delitos, siendo entonces, el ámbito espacial, uno de los graves problemas para la investigación y sanción de los delitos informáticos contra el patrimonio.

En el Estado peruano si se ha preocupado en diseñar fórmulas legales para la sanción de los delitos informáticos, sin embargo dichas normas, pues quedan desfasadas con el tiempo o son inoperativas frente a la amplitud y alcance de los delitos informáticos contra el patrimonio.

VI. Conclusiones

Primero: El tratamiento jurídico penal de los delitos informáticos contra el patrimonio es deficiente, toda vez que ilógicamente se comprende dentro de fraude informático todo los tipos o modalidades de delitos informáticos contra el patrimonio, el cual genera incertidumbre en la interpretación de la norma que no permite la sanción efectiva de los delitos informáticos contra el patrimonio.

Segundo: El tratamiento jurídico penal de los delitos informáticos contra el patrimonio en su modalidad de hurto es deficiente, en la medida que en la legislación peruana no se regula en forma expresa el delito informático contra el patrimonio, por lo que dicho vacío genera dificultades en la investigación y sanción de los delitos informáticos de hurto, más cuando no se cumple con el principio de tipicidad.

Tercero: El tratamiento jurídico penal de los delitos informáticos contra el patrimonio en su modalidad de fraude es deficiente, puesto que dentro de esta modalidad directiva se ha comprendido toda las modalidades de delitos informáticos contra el patrimonio, y al ser este tipo penal muy abierto y ambiguo no permite la efectiva sanción de los delitos informáticos contra el patrimonio.

Cuarto: El tratamiento jurídico penal de los delitos informáticos contra el patrimonio en su modalidad de estafa es deficiente, toda vez que la legislación peruana no regula expresamente este ilícito penal, por lo que, al no cumplirse con el principio de tipicidad, dificulta la investigación y sanción de los delitos informáticos contra el patrimonio en su modalidad de estafa.

Quinto: El tratamiento jurídico penal de los delitos informáticos contra el patrimonio en su modalidad de sabotaje informático es deficiente, puesto que, pese a que en la vigente legislación se sanciona la destrucción de datos, no se regula en forma clara y expresa la afectación al patrimonio por medio sistemas informáticos, con o sin fines lucrativos, el cual genera impunidad de los actos de sabotaje informático contra las empresas o personas para reducir su competitividad.

VII. Recomendaciones

Primero: Congreso de la República por parte de las instituciones con iniciativa legislativa y la sociedad civil, la adhesión del Perú al convenio de Budapest, puesto que en América solo lo han ratificado: USA, Canadá, Panamá, República Dominicana y el 2017 Chile, el no existir una legislación uniforme en delitos informáticos genera dualidad de delitos y problemas de interpretación dogmática, y además, la migración de la delincuencia on line a esta parte del planeta ya que la criminalidad informática, sabe que la legislaciones diferentes en cada país latinoamericano son una ventaja para que estas nuevas conductas delictivas sigan cubiertas bajo el manto de la impunidad.

Segundo: El Congreso de la República dele legislar en forma expresa y tipificar los delitos informáticos contra el patrimonio, diferenciando las modalidades, sean éstos delitos de fraude, estafa, sabotaje o hurto informático.

Tercero: En todas las Universidades se debe incluir un curso obligatorio de derecho informático, así como a nivel de la formación primaria y secundaria se debe incluir en la malla curricular el curso de informática, con énfasis en la prevención de todo tipo de delitos informáticos.

Cuarto: Se debe**n** crear Fiscalías especializadas en delitos informáticos para que la investigación y sanción de estos delitos sea eficiente, más cuando el avance de la informática es mucho más acelerado, son delitos emergentes en aumento y la comisión suele ser cada vez más sofisticados.

Quinto: Se debe crear una Corte internacional con competencia en delitos informáticos, debido a que los diferentes delitos informáticos son cometidos de cualquier parte del mundo y los estados son limitados e imposibilitados por su jurisdicción para la investigación y sanción de actos criminales que se encuentran y cometen delitos con el uso de los medios informáticos desde otras jurisdicciones.

VIII. Propuesta

Propuesta de clasificación de delitos informáticos contra el patrimonio

En la actualidad la Ley Nº 30096 modificado por la Ley N° 30171, en su Capítulo V que regula los delitos informáticos contra el patrimonio, en el artículo 8, tipifica en forma expresa el fraude informático, donde establece como conductas típicas al diseño, introducción, borrado, alteración, supresión, clonación de datos informáticos o cualquier interferencia o manipulación en el funcionamiento de un sistema informático es sancionada penalmente, siendo el agravante la afectación del patrimonio del Estado destinado a fines asistenciales o a programas de apoyo social.

Véase que únicamente, en forma genérica, se comprende, dentro del fraude informático a cualquier delito informático contra el patrimonio, no habiendo la observancia del principio de tipicidad para sancionar la estafa, sabotaje y hurto informático que se comete utilizando los medios informáticos, por lo que la propuesta de clasificación de los delitos informáticos contra el patrimonio, de acuerdo a los bienes jurídicos protegidos, es el siguiente:

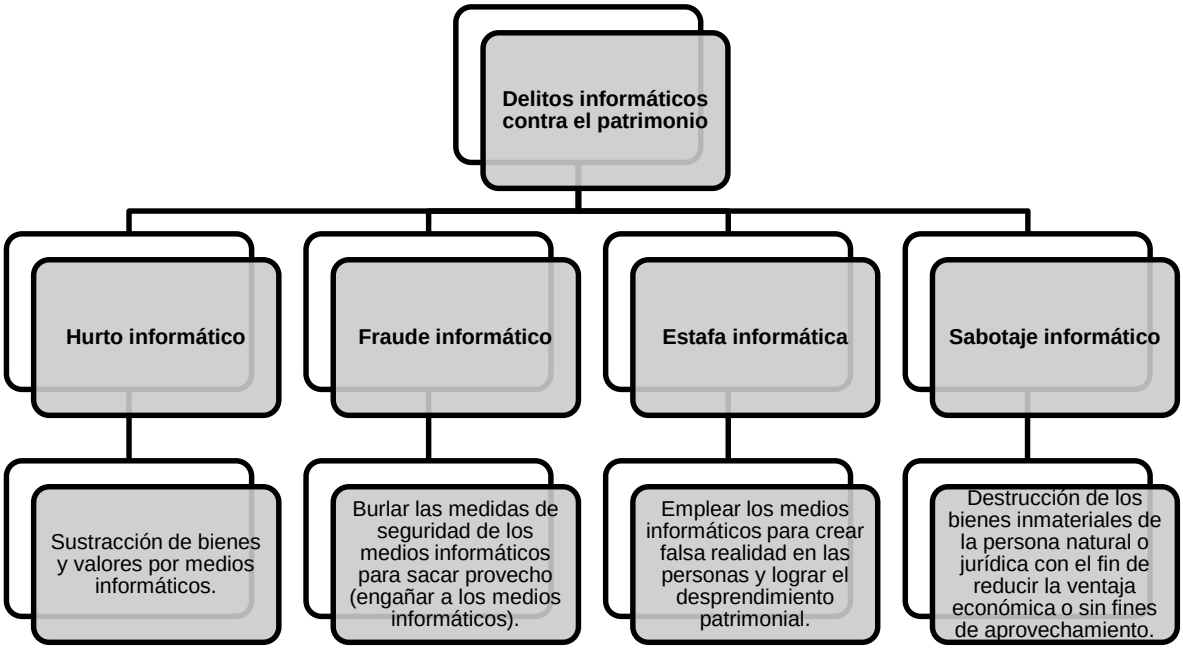


Figura 7:
Propuesta de clasificación de los delitos informáticos contra el patrimonio

Proyecto de Ley N°

Proyecto de Ley que modifica el Artículo 8 de la Ley Nº 30096 (Ley de Delitos Informáticos) e incorpora Artículos 8A, 8B, 8C y 8D.

Fórmula Legal

Artículo único.- Objeto de la ley

La presente Ley tiene por objeto modificar el Artículo 8 de la Ley Nº 30096 (Ley de Delitos Informáticos) e incorporar los Artículos 8A, 8B, 8C y 8D, los cuales quedan redactados de la siguiente manera:

Artículo 8.- fraude informático

El que deliberada e ilegítimamente procura para sí o para otro un provecho ilícito en perjuicio de tercero burlando las medidas de seguridad de los medios informáticos ya sea manipulando, sustituyendo, clonando o realizando cualquier interferencia o alteración para su acceso 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.

Artículo.- 8A.- Hurto informático

El que deliberada e ilegítimamente sustrae valores, datos, dinero y cualquier bien inmaterial con valor patrimonial usando los medios informáticos en provecho propio o de terceros 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.

Artículo.- 8B.- Estafa informática

El que empleando medios informáticos logra el desprendimiento patrimonial de la víctima para sí o para otro un provecho ilícito en perjuicio de tercero, creando falsa realidad, induciendo o manteniendo en error al agraviado mediante engaño, astucia, ardid u otra forma fraudulenta 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.

Artículo.- 8C.- Sabotaje informático

El que deliberada e ilegítimamente, en perjuicio de otro, destruye, altera, suprime, inmoviliza o introduce modificaciones de cualquier naturaleza, que haga inoperativa u obstaculice su correcto funcionamiento del sistema informático, el software o sus componentes, con el fin de lucro, reducir la ventaja económica, generar pérdidas o generar daños sin fines de aprovechamiento, 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.

Artículo.- 8D.- Agravantes

Los hechos tipificados en los Artículos 8, 8A, 8B y 8C serán sancionados con pena 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.

Comuníquese al Señor Presidente de la República para su Promulgación.

Proyecto de Resolución Legislativa que aprueba el Convenio sobre la Ciberdelincuencia

Resolución Legislativa Nº

El Congreso de la República;

Ha dado la Resolución Legislativa siguiente:

Resolución Legislativa que aprueba el Convenio sobre la Ciberdelincuencia

Artículo único. Aprobación del Convenio

Apruébese el Convenio sobre la Ciberdelincuencia, adoptado en Budapest el 23 el noviembre del año 2001.

Comuníquese al señor Presidente de la República para su promulgación.

*** Nota:** Cabe resaltar que a la fecha de la conclusión de la presente investigación existe Proyecto Resolución Legislativa N° 2807/2017-PE, por el que se propone el "Convenio sobre la Ciberdelincuencia" con algunas declaraciones y reservas, y se encuentra con dictamen de Comisión de Relaciones Exteriores.

IX. Referencias

Abdulai, Mohammed, A. (2016). *Determinantes del miedo a la victimización del crimen de cibernética: un estudio del fraude a la tarjeta de crédito / débito entre estudiantes de la Universidad de Saskatchewan*. (Tesis de Maestría, Universidad de Saskatchewan). (Acceso el 10 de julio de 2018).

Acurio, S. M. (Julio de 2018). *Entrevista de profundidad para la investigación*. Ecuador.

Aggarwal, P., Arora, P., Ghai, R. y Poonam. (2014). Revisión sobre crimen cibernético y seguridad. *Revista Internacional de Investigación en Ingeniería y Ciencias Aplicadas*, 2(1), 48-51.

Alanezi, F. (2015). *Las percepciones de fraude en línea y el impacto sobre las contramedidas para el control del fraude en línea en las instituciones financieras de Arabia Saudí*. (Tesis de Doctorado, Brunel University London). (Acceso el 10 de julio de 2018).

Alarcón, D. A. y Barrera, J. A. (2017). *Uso de internet y delitos informáticos en los estudiantes de primer semestre de la Universidad Pedagógica y Tecnológica de Colombia, Sede Seccional Sogamoso 2016*. (Tesis de Maestría, Universidad Privada Norbert Wiener). (Acceso el 10 de julio de 2018).

Alcívar, C., Domenech, G. A., y Ortiz, K. M. (2015). *La seguridad jurídica frente a los delitos informáticos.* Revista de Investigación Jurídica. 10(12), 41.

Álvarez, A. (Julio de 2018). *Entrevista de profundidad para la investigación*. España.

Álvarez-Gayou Jurgenson, J. L. (2009). *Cómo hacer investigación cualitativa*. México: PAIDÓS.

Bashir, B., & Khalique, A. (2016). *Una revisión sobre seguridad versus ética*. Revista Internacional de Aplicaciones Informáticas, 151(11), 244-249.

Besares, M. A. (2015). *Tópicos de Derecho Informático*. Texas: UNACH | Instituto De Investigaciones Jurídicas.

Bracho, C., Cuzme, F., Pupiales, C., Suárez, L., Peluffo, D., y Moreira, C. (2017). *Auditoría de seguridad informática siguiendo la metodología OSSTMMv3: caso de estudio*. Maskana, 8, 307-319.

Broadhurst, R., & Chang, L. Y. (2013). *Cibercrimen en Asia: tendencias y desafíos*. Manual de Criminología Asiática. Springer, New York, NY. 49-63.

Cconislla, R. (2017). *Incorporar la modalidad del delito de pedofilia en la Ley Nº 30096 capítulo III de los delitos informáticos (Propuesta legislativa)*. Puerto Maldonado: Universidad Andina de Cusco.

Chaparro, M. F. (2014). *Legislación informática y protección de datos en Colombia, comparada con otros países*. INVENTUM, 9(17), 32-37.

Conedo, A. (2013). *La informática forense y los delitos informáticos*. Revista Pensamiento Americano, 3(4). 81-88.

Das, S., y Nayak, T. (2013). *Impacto del crimen cibernético: cuestiones y desafíos*. Revista Internacional de Ciencias de la Ingeniería y Tecnologías Emergentes, 6(2), 142-153.

Espinoza, M. (2017). *Derecho penal informático: deslegitimación del poder punitivo en la sociedad de control*. (Tesis de grado, Universidad Nacional del Altiplano). (Acceso el 10 de julio de 2018).

García, C. M. (2017). *Los delitos de estafas y sus consecuencias a través de las redes sociales*. Babahoyo Ecuador: Universidad Regional Autónoma de los Andes – UNIANDES.

García, J. C. y Peña, D. E. (2017). Cibercriminalidad & postmodernidad: la cibercriminología como respuesta al escenario contemporáneo. Puebla/Lima.

González, J. A. (2013). *Delincuencia informática: daños informáticos del artículo 264 del Código Penal y propuesta de reforma*. (Tesis Doctoral, Universidad Complutense de Madrid). (Acceso el 10 de julio de 2018).

Han, C., y Dongre, R. (2014). ¿Qué motiva a los ciber-atacantes?. Revista de la gestión de la innovación tecnológica, 4(10). 40-42.

Hernández, R. M. (2014). La investigación cualitativa a través de entrevistas: su análisis mediante la teoría fundamentada. España: Universidad Internacional de la Rioja. 187-210.

Herrera, L. M. (2018). *Eficacia de la ley de delitos informáticos en el Distrito Judicial de Huánuco 2017*. Huánuco: Universidad de Huánuco.

Imbaquingo, D. E., Jacome, J. G., Pusdá, M. R., Ortega, M., y Imbaquingo, H. (2016). Informática Forense. Los delitos Informáticos en la Provincia de Imbabura. Innovación Tecnológica. Ibarra: Universidad Técnica del Norte.

INEI. (Junio de 2018). *Estadísticas de las Tecnologías de Información y Comunicación en los Hogares Enero – Febrero- Marzo 2018*. Lima: Instituto Nacional de Estadística e Informática.

Jaramillo, J. A., Valarezo, G. y Astudillo, O. B. (2014). *Rigurosidad versus flexibilidad en la investigación cualitativa*. Revista Panorama Médico. Quito. 8 (1), 06-13.

Lamperti, S. B. (2017). Aspectos Legales. Los Delitos Informáticos. *El rastro digital del delito: aspectos técnicos, legales y estratégicos de la Informática Forense*. Mar de Plata: Universidad FASTA Ediciones.

Lerma, H. D. (2011). *Presentación de informes. El documento final de investigación*. (3ra Ed.). Bogotá: Ecoe Ediciones.

Levin, A., & Ilkina, D. (2013). Comparación internacional del crimen cibernético. Toronto: Ryerson University.

López, A. J, López, L. y Jerónimo, G. (2017). *Factores que contribuyen a la prevención de los delitos informáticos en el Estado de Tabasco*. Revista Gênero & Direito, 6(3). 1-17.

Loredo, J. A., y Ramírez, A. (2013). *Delitos informáticos: su clasificación y una visión general de las medidas de acción para combatirlo*. Celerinet. 44-51.

Manjarres, I. (Julio de 2018). *Entrevista de profundidad para la investigación.* Colombia.

Mayan, M. J. (2001). *Una Introducción a los Métodos Cualitativos: Módulo de entrenamiento para Estudiantes y Profesionales*. México.

Mayer, L. (2017). *El bien jurídico protegido en los delitos informáticos*. Revista chilena de derecho, 44(1), 261-285.

Ministerio Público. (Diciembre de 2017). *Boletín Estadístico del Ministerio Público*. Lima: Ministerio Público.

Neghina, D. E., & Scarlat, E. (2013). Gestionar la seguridad de la tecnología de la información en el contexto de las tendencias del delito cibernético. *Revista internacional de comunicaciones y control de computadoras*, 8(1), 97-104.

Peña, D. (Julio de 2018). *Entrevista de profundidad para la investigación. Perú.*

Piccirilli, D. A. (2015). Protocolos a aplicar en la Forensia Informática en el marco de las nuevas tecnologías (Pericia – Forensia y Cibercrimen). (Tesis Doctoral, Universidad Nacional de La Plata). (Acceso el 10 de julio de 2018).

Rada, D. M. (s.f.). *El rigor en la investigación cualitativa: técnicas de análisis, credibilidad, transferibilidad y confirmabilidad.* Caracas: Universidad Pedagógica Experimental Libertador

Ramallo, M., y Roussos, A. (2008). *Lo cualitativo, un modelo para la comprensión de los métodos de investigación*. Buenos Aires: Universidad de Belgrano.

Ramírez, D. A., y Castro, E. F. (2018). *Análisis de la evidencia digital en Colombia como soporte judicial de delitos informáticos mediante cadena de custodia*. Villavicencio: Universidad Nacional Abierta y a Distancia “UNAD”.

Rico, M. (2013). *Los desafíos del derecho penal frente a los delitos informáticos y otras conductas fraudulentas en los medios de pago electrónicos*. Revista IUS, 7(31), 207-222.

Rincon, L. M., Taborda, D. A., & Roldan, L. M. (2017). *Clonación de tarjetas de crédito*. Medellín: Tecnológico de Antioquia Institución Universitaria.

Rincón, R. J. (2015). *El delito en la cibersociedad y la justicia penal internacional. Madrid*: (Tesis Doctoral, Universidad Complutense de Madrid). (Acceso el 10 de julio de 2018).

Rodríguez, F. (2013). *Derecho informático. El derecho en la era digital. La sociedad de información y el sistema jurídico. Contratos informáticos. Protección jurídica de los programas de computación. Delitos informáticos. La tutela jurídica del sistema informático*. UNC y FCEFyN.

Sánchez, J. J. (2017). *Adopción de estrategias de Ciberseguridad en la protección de la información en la Oficina de Economía del Ejército, San Borja- 2017*. (Tesis de Maestría, Instituto Científico Tecnológico del Ejército). (Acceso el 10 de julio de 2018).

Semprini, G. M. (Julio de 2018). *Entrevista de profundidad para la investigación.* Argentina.

Sequeiros, I. C. (2016). V*acíos legales que imposibilitan la sanción de los delitos informáticos en el nuevo código penal peruano-2015*. (Tesis de grado, Universidad de Huánuco). (Acceso el 10 de julio de 2018).

Silva, G. A. (Julio de 2018). *Entrevista de profundidad para la investigación*. Perú.

Strauss, A., y Corbin, J. (2002). *Bases de la investigación cualitativa: Técnicas y procedimientos para desarrollar la teoría fundamentada*. Medellin: Editorial Universidad de Antioquia.

Temperini, M. G. (2014). *Delitos informáticos en Latinoamérica: un estudio de derecho comparado*. In XLIII Jornadas Argentinas de Informática e Investigación Operativa. Buenos Aires: Simposio Argentino de Informática y Derecho (SID).

Tenorio, J. y Tuesta, M. (2012). Legislación del secreto bancario y su relación con el delito de hurto informático de dinero mediante la violación de claves

secretas, Iquitos- 2010. (Tesis de Maestría, Universidad Nacional de la Amazonía Peruana). (Acceso el 10 de julio de 2018).

Vásquez, C. E., Regalado, J. M., y Guadron, R. S. (2017). *Cibercrimen e informática forense: introducción y análisis en El Salvador*. Revista Tecnológica; Nº. 10. 63-68.

Villavicencio, F. (Diciembre 2014). *Delitos informáticos*. IUS ET VERITAS, 24(49), 284-304.

Wall, D. S. (2015). *Crimen desorganizado: hacia un modelo distribuido de la organización del cibercrimen*. La Revista Europea del crimen organizado. Sgocnet. 2(2), 71-90.

Wang, Q. (2016). *Estudio comparativo de la ciberdelincuencia en Derecho Penal: China, Estados Unidos, Inglaterra, Singapur y el Consejo de Europa*. (Tesis de doctorado, Universidad Erasmo de Rotterdam). (Acceso el 10 de julio de 2018).

X. Anexos

Anexo1: Artículo científico

Tratamiento jurídico penal de los delitos informáticos contra el patrimonio, Distrito Judicial de Lima, 2018

Criminal legal treatment of computer crimes against property, Judicial District of Lima, 2018

PARDO VARGAS, Alejo

Resumen

La presente investigación titulada “Tratamiento jurídico penal de los delitos informáticos contra el patrimonio, Distrito Judicial de Lima, 2018” tuvo como objetivo general Analizar el tratamiento jurídico penal de los delitos informáticos contra el patrimonio, Distrito Judicial de Lima, 2018. Para el cual se utilizó serie de métodos de investigación, propias de la investigación cualitativa, de nivel descriptico explicativo. Se utilizó como técnica la entrevista con su respectivo instrumento de recolección de datos, la guía de entrevista, con el cual se recopiló información de los expertos sobre el tema, nacionales y extranjeros, llegándose a conclusiones precisas.

En tal sentido, se concluye que el tratamiento jurídico penal de los delitos informáticos contra el patrimonio es deficiente, toda vez que ilógicamente se comprende dentro de fraude informático todo los tipos o modalidades de delitos informáticos contra el patrimonio, el cual genera incertidumbre en la interpretación de la norma que no permite la sanción efectiva de los delitos informáticos contra el patrimonio.

Finalmente se recomienda que el Congreso de la República por parte de las instituciones con iniciativa legislativa y la sociedad civil, la adhesión del Perú al convenio de Budapest, así como debe legislar en forma expresa y tipificar los

delitos informáticos contra el patrimonio, diferenciando las modalidades, sean éstos delitos de fraude, estafa, sabotaje o hurto informático, y en todas las Universidades se debe incluir un curso obligatorio de derecho informático, así como a nivel de la formación primaria y secundaria se debe incluir en la malla curricular el curso de informática, con énfasis en la prevención de todo tipo de delitos informáticos.

Palabras claves: Informática, delito informático, delitos informáticos contra el patrimonio hurto informático, estafa informática, fraude informático y sabotaje informático.

Abstract

This research entitled "Criminal legal treatment of computer crimes against property, Judicial District of Lima, 2018" had as its general objective Analyze the criminal legal treatment of computer crimes against property, Judicial District of Lima, 2018. For which a series of research methods was used, typical of qualitative research, descriptive descriptive level. The interview with its respective instrument of data collection, the interview guide, was used as a technique, with which information of the experts on the national and foreign subject was collected, reaching conclusions.

It is concluded that the criminal legal treatment of computer crimes against the heritage is deficient, since illogically it is understood within computer fraud all the types or modalities of computer crimes against the patrimony, which generates uncertainty in the interpretation of the norm that does not allow the effective sanction of computer crimes against the patrimony.

Finally, it is recommended that the Congress of the Republic by institutions with legislative initiative and civil society, Peru's accession to the Budapest Convention, as well as expressly legislate and criminalize computer crimes against heritage, differentiating the modalities , be these crimes of fraud, fraud, sabotage or computer theft, and in all universities must include a mandatory computer law course, as well as at the level of primary and secondary education should be included in the curriculum the computer course , with emphasis on the prevention of all types of computer crimes.

Key words: Computing, computer crime, computer crimes against computer theft, computer fraud, computer fraud and computer sabotage.

Introducción

En la actualidad se observa que cada vez más las nueves sistemas de información, nuevas tecnologías, sistemas informáticos y en específico las nuevas tecnologías informáticas ha ido avanzando, donde existen muchos expertos en la materia, quienes hacen y desasen diversos software.

Estas tecnologías informáticas definitivamente se pueden usar para muchas y buenas cosas, pero también para causar perjuicio a terceros, sustraer patrimonios, bienes, alterar sistemas de seguridad, extraer, modificar y eliminar datos, realizar un sin número de fraudes e incluso acceder a los datos de las entidades públicas y privadas rompiendo sistemas de seguridad.

En este orden de ideas, el problema de la ciberdelincuencia ha aumentado y desarrollados nuevos sofisticados modos de operación, donde nadie lo descubre, frente a este realidad el derecho penal de muchos países de hecho ha quedado en el tiempo, la peruana no es la excepción, a pesar de las modificatorias introducidas en forma genérica en relación a la ciberdelincuencia no basta, por lo que el derecho penal ya queda y lo es aparente frente a esta situación.

En tal sentido, existen sin número de modalidades en las que el ciberdelincuente pueda cometer delitos contra el sistema informático ya sea mediante acceso o alteración de los sistemas informáticos, así como cometer delitos contra el patrimonio, ya sea mediante cualquier tipo de fraude informático, pero también se puede cometer delitos contra la privacidad de las personas, instituciones y el Estado mismo, en este aspecto, las pequeñas y medianas empresas son las más vulnerables debido a que no cuentan con un sistema de ciberseguridad, en las plataformas o nubes que usan, pues todo los datos que se almacenan en la nube pueden estar siendo objeto de intercepción.

Este último toma relevancia en la medida que los datos que se guardan son de carácter confidencial como documentos oficiales, historias clínicas entre otros que por su carácter, impotencia o naturaleza sea objeto de protección y confidencialidad.

Los delitos informáticos contra el patrimonio se realizan en afectación de las personas naturales y jurídicas, en la modalidad de hurto, fraude, estafa y sabotaje informático, los mismos que a todas luces pasa desapercibido debido a la debilidad del tratamiento jurídico penal que los países le dan a estas conductas ilícitas, también por las especiales características que distinguen a estas conductas, como la condición cualificada de los sujetos activos quienes tienen un alto grado de expertís en la informática, es así como los nuevos delitos informáticos que pasan desapercibidos y difíciles de descubrir aunque son denunciadas.

Que los avances tecnológicos son utilizados para beneficiarse ilícitamente del patrimonio de terceros por medio de clonación de tarjeras bancarias, alteración o vulneración de sistemas informáticos con el objetivo de beneficiarse de servicios, así como las trasferencia de fondos ajenos por medio de manipulación de sistemas informáticos de seguridad.

Las empresas o instituciones que no estén en la red simplemente no existen y mantienen desventaja frente a los que están disponibles en el internet, en este sentido, las transacciones comerciales de diversa naturaleza cada vez más va en aumento y mucho más consolidado, sin embargo, la contra que pone en duda y por consiguiente la limitación de realizar operaciones por medios electrónicos es justamente el fraude, estafa o hurtos informáticos que puedan afectar a los usuarios como consecuencia de que por las plataformas virtuales, para concretar transacciones es necesario proporcionar los datos y claves de la tarjeta electrónica, pudiendo ser utilizadas los datos para hurtos sistemáticos del fondo de la tarjeta, si opere el cobro del monto pero nunca pueda recibir el bien adquirido o el servicio contratado, siendo el usuario víctima de estafa, puesto que se le indujo en error al ofrecer un bien o servicio y logrando que se desprenda del patrimonio, el cual de hecho genera desconfianza

En el derecho penal informático, la legislación penal (derecho penal) cumple el rol de simbólico, que carece de sistematicidad y exhaustividad en la calificación de las conductas que afectan bienes jurídicos penalmente tutelables, como es el patrimonio.

De acuerdo a la estadística proporcionada por el Instituto Nacional de Estadística e Informática, en el Perú, las denuncias realizadas por los delitos informáticos en los periodos 2008 al 2011 no existe una sola denuncia o caso registrado sobre delitos informáticos, cabe preguntarse entonces ¿Por qué es que no existe una sala denuncia?

Posteriormente a ello, con las modificaciones introducidas en el 2013 y 2014 se observa que el aumento de los casos registrados de los delitos informáticos, conforme a los informes estadísticos del Ministerio Públicos, ha aumentado considerablemente y se está multiplicando, entonces, las denuncias presentadas o los casos registrados, si no se tiene una regulación adecuada para sancionarlos penalmente, es evidente que va quedar impune, puesto que en la legislación peruana no existe una regulación expresa de hurto, estafa y sabotaje informático, más por el contrario, se ha introducido fraude informático como un delito genérico, pues éste genera más ambigüedades y vaguedad en su interpretación que bridar soluciones y permitir una sanción que corresponda a la conducta penalmente relevante y reprochada por la sociedad.

El artículo 8 de la “ley de delitos informáticos” tipifica una sola modalidad de delitos informáticos contra el patrimonio, al cual se rotula con el nomen iuris de “fraude informático”, dicha regulación genérica que no permite delimitar e identificar plenamente las conductas en el tipo penal, esto es, la subsunción de la conducta con el tipo penal (tipificación).

Material y métodos

El problema general de estudio fue ¿Cómo es el tratamiento jurídico penal de los delitos informáticos contra el patrimonio, Distrito Judicial de Lima, 2018? Cuyo

objetivo fue analizar el tratamiento jurídico penal de los delitos informáticos contra el patrimonio, Distrito Judicial de Lima, 2018.

El diseño de estudio fue teoría fundamentada, enfoque cualitativo, nivel de estudio descriptivo explicativo, y se emplearon métodos comparativo, descriptivos, analíticos, dogmáticos y hermenéuticos; como técnica de recolección de datos se utilizó a la entrevista con su respectivo instrumentos, el cual fue la guía de preguntas de entrevista.

Resultados

Los entrevistados coinciden que la criminalidad informática va de la mano con el acelerado avance de las tecnologías informáticas, permitiendo nuevas modalidades de comisión de delitos cada vez más sofisticados, difíciles de identificar, por lo que es necesario contar con organismos y funcionarios especializados para llevar adelante las investigaciones con resultados favorables.

En Ecuador y en España se han realizado buenas reformas respecto a los delitos informáticos, ampliándose la redacción de los tipos penales no contemplados, actualizándose la legislación penal. Por otro lado, los entrevistados de Colombia y Argentina consideran que la legislación sobre delitos informáticos es insuficiente para sancionar en forma eficaz las nuevas formas delictivas con el uso de las tecnologías informáticas. Con esta última respuesta coinciden los entrevistados nacionales señalando que la legislación es insuficiente y esto va acompañado de la falta de difusión de la criminalidad informática.

Se concluye que los entrevistados de España y uno de Perú manifiestan que es adecuado comprender a la estafa, hurto y sabotaje informático dentro del *nomen iuris* “fraude informático, sin embargo, Acurio (2018) entrevistado de Ecuador, Manjarres (2018) entrevistado de Colombia y Silva (2018) entrevistado de Perú discrepan con dicha postura, puesto que el primero considera que el los fraudes informáticos son específicos, pertenecen a las defraudaciones en genérico, es un delito de carácter patrimonial, pero diferente del hurto y sabotaje, y no da para que se les nomine solo como fraude, y finalmente, se señala que el fraude se refiere a cualquier tipo de manipulación por lo que la estafa no

corresponde ser comprendida, pero el sabotaje podría cuadrar dentro del fraude por tratarse de alteración de datos, pero sobre el hurto no existe un verbo rector.

Casi todo los entrevistados coinciden que los bancos no están dispuestos a denunciar penalmente delitos de hurto sistemáticos de cuentas bancarias y otros por la protección de su imagen corporativo, para mantener la clientela, para evitar su propio desprestigio y no hacer denotar la inseguridad, por no perder la confianza de sus clientes y futuros clientes y evitar el pánico financiero, sin embargo, Álvarez (2018) entrevistado de España señala que los bancos Españolas si están dispuestos a colaborar en la denuncia e investigación criminal.

En la legislación penal ecuatoriana no existe regulación expresa del hurto informático, mientras en la legislación Española, tampoco existe regulación expresa, pero está comprendido dentro de fraudes informáticos, en el caso peruano si había una regulación en el artículo 186 del código Penal, sin embargo fue derogada por la Ley 30096 modificada por la Ley 30171. A diferencia de las demás legislaciones, en Colombia si existe regulación expresa del delito de hurto informático, el cual está tipificada en la Ley 1273.

Al cual, en el ámbito nacional, Silva (2018) señala que interceptación ilegitima de datos informáticos, el cual podría entenderse como hurto al apoderarse de datos de manera ilegal pertenecientes a un tercero, sin embargo, admite que la legislación peruana es incipiente y tiene ciertas falencias.

Todo los entrevistados coinciden que tanto las personas como las empresas están expuestos a ser víctimas de fraudes informáticos, los atacantes informáticos se aprovechan de la falta de conocimiento y cultura de ciberseguridad de sus víctimas, nunca de puede estar de todo seguro y siempre se estará expuesto a potenciales fraudes, y últimamente se viene practicando nuevas modalidades como la “CRYPTOLOCKER” y Ramsomware, modalidad, mediante el cual se encripta o restringe el acceso a archivos de la víctima, pidiendo grandes cantidades de dinero para desincriptarlos, es decir, para que su propietario pueda obtener la clave y acceder a los archivos “secuestrados”.

A diferencia de Ecuador, Colombia, España y Argentina, en el Perú no existen estrategias claras para la prevención y sanción de delitos de fraude informático.

En ecuador existe ISO 27000 sobre la Seguridad de la Información por parte de las entidades públicas y privadas, en España aparte de la legislación, existen campañas de información para detectar estos delitos y saber actuar ante ellos y en Argentina existe el protocolo de grooming que lo difunde a la sociedad sobre los fraudes informáticos.

Del cual se desprende que en el Perú no se ha tomado en cuenta la real dimensión de los delitos informáticos, puesto que se actúa únicamente en forma reactiva, no existe legislación adecuada ni políticas de prevención de delitos informáticos contra el patrimonio.

Las plataformas informáticas generarán confianza para realizar compras y contratar servicios a través de internet siempre que cumplan estándares de seguridad que garanticen realizar las transacciones sin riesgo, o que la compañía sea uno conocido de renombre, puesto las compañías extranjeras que no tengas los certificados de seguridad mínimos genera desconfianza para realizar cualquier tipo de transacción. Al cual agrega Silva (2018) al decir que la legislación penal peruana resulta insuficiente dado la creciente actividad criminal, pese a que considera que se cumple con el principio de tipicidad en la sanción de la estafa informática.

Acurio (2018) entrevistado de Ecuador señala que la estafa es un delito computacional que consiste en lograr engañar a la víctima, es decir, generar error psicológico en la víctima que le conduzca al desprendimiento patrimonial, por otro lado, Manjarres (2018) entrevistado de Colombia señala que en su país si existe la regulación específica de la estafa informática, el cual se encuentra en la Ley 1273 de 2009, por el contrario, Álvarez (2018) advierte que en la legislación Española no existe en concreto la regulación específica de estafa informática, pero el artículo 148 referente a la estafa es de gran utilidad para tratar el delito de estafa.

Por otro lado, Peña (2018) entrevistado peruano, señala que en el Perú no se sancionan correctamente los delitos informáticos como la estafa informática. En este sentido, se puede concluir que en el Perú no se ha tipificado en forma expresa la estafa informática.

Los entrevistados consideran que cuando un pirata informático destruye información y softwares en la red afecta el patrimonio de la víctima, puesto que como señala Acurio (2018) ahora la información puede tener una valor económico para la víctima y eso puede causarle un perjuicio patrimonial, con ello concuerda Manjarres (2018) al decir que la víctima ha dedicado tiempo, estudio e investigación en la información destruida.

Se debe tener en cuenta que el perjuicio patrimonial no solo es en razón a la destrucción de la información en sí, sino que, además, la empresa o persona, a efectos de recuperar la información destruida suele contratar profesionales o empresas externar, cuya contratación se traduce en un desprendimiento patrimonial como consecuencia de la destrucción de la información. El patrimonio no solo es material, sino también inmaterial. Agrega Silva (2018), que la legislación penal peruana es insuficiente para la sanción de sabotaje informático.

Conforme señala Acurio (2018) en Ecuadro existe un delito símil al sabotaje informático, el cual es el delito de daños, asimismo, en la Legislación colombiana también existe regulado en la Ley 1273 de 2009, sin embargo, en el Código Penal Español no se encuentra tipificado como tal, pero el Artículo 264 del Código Penal Español, al igual que de Ecuador, regula como Daños informáticos, tipo penal en la que se puede cuadrar correctamente el sabotaje informático. A diferencia de los países antes nombrados, en la legislación penal peruana no existe en forma expresa la tipificación de delito de sabotaje informático, pero es posible que se puede encuadrar como atentado contra la integridad de datos informáticos conforme al artículo 3 de la Ley 30171 que modificó a la Ley 300096, sin embargo, se puede advertir que no se estaría cumpliendo con el principio de tipicidad para sancionar los delitos de sabotaje informático.

Álvarez (2018), señala que leyes Españolas, previenen los delitos informáticos contra el patrimonio, pero advierte que debería ser más concreta y

una legislación Global, ya que en el momento que esos delitos, provienen de fuera de nuestras fronteras, la investigación se hace más difícil, concordante a ello Acurio (2018) señala que el limitante puede ser que al ser delitos de tipo transnacional las evidencias o pruebas estén en otra jurisdicción. Por otro lado, Manjarres (2018) señala que la regulación por sí sola no contribuye con la prevención de estos delitos. Se necesitan campañas educativas eficaces.

La legislación peruana no previene los delitos informáticos contra el patrimonio, dado que la norma es una sola y genérica para todas las modalidades de delitos contra el patrimonio, por lo que se está lejos de la prevención.

La mayoría de los entrevistados consideran que es necesario una reforma legislativa para prevenir y sancionar los delitos informáticos contra el patrimonio, y se hace énfasis que no solo debe ser respecto a los delitos informáticos contra el patrimonio, sino, sobre las demás modalidades de delitos informáticos, puesto que de acuerdo a las nuevas tecnologías informáticas existen nuevas modalidades de comisión de delitos y la legislación penal debe estar a la altura para prevenir y sancionar.

Finalmente, entre los principales aportes u opiniones de los expertos, claridad terminológica en el tema de los delitos informáticos en especial sobre los fraudes informáticos desde el punto de vista de la tipicidad objetiva, los delitos informáticos son muy desconocidos por la población en general, el Perú se debe adherir al convenio de Budapest y que en el Perú se debe ampliar el radio de acción de División de Delitos Informáticos de la PNP e implementar las herramientas necesarias.

Discusión

Respecto a la discusión de los resultados de la investigación, Lerma (2011) señala que el objetivo de la discusión es “(…) mostrar las concordancias y diferencias de los propios resultados con los encontrados por otros investigadores, y que ya fueron mencionados en el marco de referencia del estudio (…)” (p. 70). En este orden de ideas, tomando en cuenta que la discusión

es el contraste crítico de los resultados de la investigación con los antecedentes o trabajos previos respecto al problema de estudio, así como con las teorías relacionadas al tema, el cual, en la presente investigación se presenta de la siguiente manera.

En el supuesto general de la presente investigación se enfatizó que el tratamiento jurídico penal de los delitos informáticos contra el patrimonio es deficiente por comprender dentro de fraude informático todo los tipos o modalidades de delitos informáticos contra el patrimonio, generando éste incertidumbre en la interpretación de la norma, no permitiendo la sanción efectiva de los delitos informáticos contra el patrimonio.

En el ámbito extranjero, citado como trabajos previos, Wang (2016) encontró que China tiene un sistema de regulación de niveles múltiples en malas acciones cibernéticos, sin embargo, los EE.UU. pese a que logra penalizar las malas acciones cibernéticos no está exenta de problemas puesto que la legislación de los Estados Unidos sobre la ciberdelincuencia menos consistente, y esa incompatibilidad conduce a problemas en la práctica judicial. Por otro lado, encontró que Singapur ha sido activo en la promulgación y modificación de su Ley sobre Abusos Informáticos.

Es así que se pudo advertir que los países como China, los Estados Unidos, Inglaterra y Singapur han experimentado reformas significativas para adaptar su legislación penal. Mientras a nivel internacional, el Consejo de Europa ha lanzado seminarios y proyectos que analizan el cibercrimen y exploran soluciones, y ha redactado la Convención sobre Ciberdelincuencia, sin embargo, estas contramedidas son insuficientes todavía para el cibercrimen, por la naturaleza de delitos y limitación en la cobertura de la ley penal.

En este sentido, si bien en la legislación peruana existen legislaciones, modificaciones normativas con fines investigación y sanción de los delitos informáticos, como se encontró en los resultados del estudio, la legislación es insuficiente para sancionar las diversas modalidades de los delitos informáticos contra el patrimonio, mucho menos se logra con la prevención de dichos ilícitos.

Del censo llevado a cabo en el año 2018, conforme al informe del Instituto Nacional de Estadística e Informática, el 99.7% de los hogares donde el jefe del hogar es con instrucción superior universitaria, tienen acceso a las Tecnologías de Información y Comunicación, 99.2% superior no universitaria y 96.6% secundaria, siendo entonces un alto índice de acceso a las Tecnologías de Información y Comunicación en los hogares peruanos, el cual constituye una oportunidad bastante grande para los ciberdelincuentes, toda vez que mientras mayor población tenga acceso a las tecnologías informáticas y menos sea el conocimiento de las medidas de seguridad, la posibilidad de comisión de diversos delitos informáticos contra el patrimonio aumenta, es decir, el riesgo de ser víctima de ciberdelito aumenta.

Uno de los delitos informáticos más notables y comunes es el hurto sistemático de los fondos de las cuentas bancarias, al respecto Abdulai (2016) encontró que la experiencia de victimización y los comportamientos de uso de internet están asociados positivamente con el temor de los estudiantes y su riesgo de convertirse en víctimas de fraude con tarjetas de crédito / débito. El cual implica que es todavía riesgosa la realización de transacciones por medios informáticos, en la medida que se exige revelación de los datos secretos de la tarjeta.

El uso masificado de internet ha aumentado la posibilidad de ser víctimas de cualquier tipo de delitos que se pueden concretar por dicho medio, es así que Alanzi (2015) en el estudio que realizó respecto a las percepciones de fraude en línea y el impacto sobre las contramedidas para el control del fraude en línea en las instituciones financieras de Arabia Saudí encontró que las personas son dependientes de Internet; la posibilidad de ser violado por los hackers y estafadores está creciendo, especialmente en lo que la socialización, compras en línea y la banca se llevan a cabo a través de computadoras personales o dispositivos móviles, siendo que el fraude en línea ha sido descrito como una epidemia que se ha extendido a la mayoría de las actividades en línea.

Dicho estudio encontró que expansión de las actividades en línea y uso de información tecnologías en las transacciones bancarias crean oportunidades y lagunas explotadas por algunos estafadores en línea, lo que generó pérdida de

más de 20 millones de dólares en 2010 y 2012 para Arabia Saudí. A diferencia de este estudio, si bien en el Perú no existen datos estadísticos respecto a las pérdidas que se generan como consecuencia de los delitos informáticos contra el patrimonio, lo es también que el Perú es un país incipiente en la regulación de estos tipos de delitos, y como evidencia de esto son las respuestas de los entrevistados, así como la propia ley de delitos informáticos que en cuyo capítulo relativo a los delitos informáticos contra el patrimonio, existe tipificado en forma expresa únicamente el fraude informático, sin embargo, en otros países, aunque no en todas, existe regulación específica de hurto, estafa y fraude informático.

El alcance teórico de estudio en esta investigación fueron el fraude, la estafa, el sabotaje y hurto informático como modalidades de delitos informáticos contra el patrimonio, sin embargo, es necesario advertir que dicha clasificación se realiza en estricta observancia del bien jurídico patrimonio y de acuerdo a las limitaciones doctrinarias y teóricas al respecto, puesto que creemos que los delitos nombrados no son los únicos que afectan el patrimonio, pudiendo expandirse en la tipificación a otras modalidades o clasificación distinta y más amplia. En este estudio se tomó la prioridad de analizar el fraude, la estafa, el sabotaje y hurto informático debido a la evidente observación de la existencia de dichos delitos y la inexistencia de norma penal específica para una prevención, investigación y sanción efectiva de estos tipos de delitos.

La comisión de los delitos informáticos no tiene fronteras, es decir, las limitaciones espaciales para su comisión, por cuanto con la sola tenencia de un ordenador, es factible la comisión del ilícito con efectos en otros países o continentes, sobre el cual, Rincón (2015) encontró que las fronteras creadas no son solo por el territorio, sino por el concepto de jurisdicción y competencia que son los delimitantes del ejercicio punitivo de los Estados, impiden que se investigue, juzgue y sancione a quienes hayan cometido la conducta desde un territorio pero con consecuencias en otro, es decir, el delito se cometió desde un Estado pero las víctimas o el daño se materializan en otro estado, por lo que estas limitaciones y fronteras crea impunidad en la búsqueda y persecución de los delitos informáticos.

Es en este sentido, que el Estado peruano se encuentra incapacitado para la investigación y sanción de los delitos informáticos que se cometan por personas que se encuentran en otros países, pero cuyo efecto del delito recae en el Estado Peruano, puesto que aparte de las limitaciones tecnológicas para la investigación de estos delitos, existen graves limitaciones jurisdiccionales o de competencia, más si el Perú no ha ratificado el convenio de cibercrimibnalidad de 2001 (Convenio de Budapest).

En relación a ello, González (2013) encontró que la expansión exponencial de la ciberdelincuencia es innegable, y se trata de un fenómeno novedoso que cuyas prácticas delictivas requiere la intervención de los diferentes estados, y este tipo de delitos, su aparición y su desarrollo tienen, en contradicción con el lento avance del Derecho en el tratamiento jurídico penal de los delitos informáticos, puesto que estos delitos tienen un carácter trasnacional , por lo que nunca es suficiente la regulación protectora en un único Estado, puesto que para la comisión de los delitos informáticos, no se requiere la cercanía física, puede hacerlo tan lejos como el medio de comunicación o el internet tiene alcance. Al cual agrega Piccirilli (2015) es bastante alto el nivel de la ciberdelincuencia, y que la constante evolución del delito es la que provoca generar nuevas inquietudes, siendo necesario la creación de un órgano asesor técnico informático pericial.

Por otro lado, los trabajos previos a nivel nacional muestran que existen deficiencias en la regulación de los delitos informáticos, es así que Tenorio y Tuesta (2012) encontraron que la legislación del secreto bancario en el Perú, no es acorde con el avance tecnológico y el incremento de la criminalidad cibernética, pues el secreto bancario constituye un obstáculo en la investigación del delito de hurto informático de dinero, puesto que el secreto bancario se levanta exclusivamente por orden judicial en procesos concretos, el cual influye en la impunidad de los autores del delito de hurto informático de dinero. Mientras Sequeiros (2016) encontró que debido a la naturaleza virtual de los delitos informáticos, estos se pueden volver confusos en su tipificación, ya que a nivel general, se poseen pocos conocimientos y experiencias en el manejo de ésta área.

Sin embargo, los resultados de la investigación demuestran que el Estado Peruano ha introducido modificaciones en el 2013 en la legislación penal, es así que se aprobó la ley de delitos informáticos y modificado ésta a efectos de que la legislación especial esté de acuerdo a los parámetros del convenio de Budapest, sin embargo es notable la deficiencia normativa para sancionar los delitos informáticos, especialmente a aquellos que afectan el patrimonio, toda vez que dentro de la legislación de delitos contra el patrimonio, únicamente se tipifica como fraude informático, sin contemplar otros tipos penales como la estafa informática, hurto informático y el sabotaje informático, el cual dificulta enormemente la investigación y sanción de los delitos informáticos contra el patrimonio. Los cuales son concordantes con los supuestos específicos planteados en esta investigación, puesto que tanto de la estafa, fraude, sabotaje ni fraude informático existe una regulación eficiente, sino una regulación ambigua y deficiente, cuyo tipo penal es insuficiente para la investigación y sanción de las modalidades de los delitos informáticos contra el patrimonio.

Por otro lado, Sánchez (2017) encontró que la adopción de estrategias de ciberseguridad incide significativamente en la protección de la información, mientras Alarcón y Barrera (2017) recomendaros que se debe involucrar a los docentes y directivos de las instituciones a que implementen módulos prácticos que permita a los estudiantes alejarse de las prácticas inapropiadas con el uso de la informática. Así como Espinoza (2017) admite que los delitos informáticos son transnacionales y multidisciplinarios conforme a lo ya analizado líneas arriba.

Sin embargo, se puede advertir que no existe sola investigación en forma específica de los delitos informáticos contra el patrimonio, siendo que las investigaciones relacionadas al tema han sido genéricas o de aspectos particulares de delitos informáticos, pero no respecto a los delitos informáticos contra el patrimonio, por lo que este aspecto de los delitos informáticos es todavía bastante incipiente, pese a que por primera vez se tipificó como delito informático aquello que afectaba el patrimonio y el surgimiento de delitos informáticos en el Perú ha sido con fines de proteger el bien jurídico patrimonio. Asimismo, los delitos informáticos que afectan el patrimonio es la que cuenta con mayor incidencia a diferencia de los demás tipos de delitos informáticos.

Por otro lado, de las teorías relacionadas al tema de estudio, existen diferentes autores nacionales y extranjeros quienes manifiestan su punto de vista sobre la regulación, sanción y tratamiento de los ilícitos en estudio.

Que los delitos informáticos son delitos emergentes que cada vez varían de acuerdo al avance de las tecnologías informáticas, por lo que es necesario que todo el aparato judicial debe ir a la altura de ésta, es decir, debe estar en la capacidad de responder con una adecuada investigación y sanción de los delitos informáticos.

Uno de los grandes problemas en la sanción de los delitos informáticos no son sino la investigación y sanción, por el carácter de internacional o global que esta tiene, pues como es de verse del contenido de la investigación, el delincuente informático puede con toda facilidad cometer el ilícito desde un continente distinto al lugar de la víctima, por lo que se hace sumamente difícil la investigación y sanción, más cuando no existen organismos internacionales o países que cooperen con la investigación y sanción de estos delitos, siendo entonces, el ámbito espacial, uno de los graves problemas para la investigación y sanción de los delitos informáticos contra el patrimonio.

En el Estado peruano si se ha preocupado en diseñar fórmulas legales para la sanción de los delitos informáticos, sin embargo dichas normas, pues quedan desfasadas con el tiempo o son inoperativas frente a la amplitud y alcance de los delitos informáticos contra el patrimonio.

Conclusiones

Primero: El tratamiento jurídico penal de los delitos informáticos contra el patrimonio es deficiente, toda vez que ilógicamente se comprende dentro de fraude informático todo los tipos o modalidades de delitos informáticos contra el patrimonio, el cual genera incertidumbre en la interpretación de la norma que no permite la sanción efectiva de los delitos informáticos contra el patrimonio.

Segundo: El tratamiento jurídico penal de los delitos informáticos contra el patrimonio en su modalidad de hurto es deficiente, en la medida que en la legislación peruana no se regula en forma expresa el delito informático contra el

patrimonio, por lo que dicho vacío genera dificultades en la investigación y sanción de los delitos informáticos de hurto, más cuando no se cumple con el principio de tipicidad.

Tercero: El tratamiento jurídico penal de los delitos informáticos contra el patrimonio en su modalidad de fraude es deficiente, puesto que dentro de esta modalidad directiva se ha comprendido toda las modalidades de delitos informáticos contra el patrimonio, y al ser este tipo penal muy abierto y ambiguo no permite la efectiva sanción de los delitos informáticos contra el patrimonio.

Cuarto: El tratamiento jurídico penal de los delitos informáticos contra el patrimonio en su modalidad de estafa es deficiente, toda vez que la legislación peruana no regula expresamente este ilícito penal, por lo que, al no cumplirse con el principio de tipicidad, dificulta la investigación y sanción de los delitos informáticos contra el patrimonio en su modalidad de estafa.

Quinto: El tratamiento jurídico penal de los delitos informáticos contra el patrimonio en su modalidad de sabotaje informático es deficiente, puesto que, pese a que en la vigente legislación se sanciona la destrucción de datos, no se regula en forma clara y expresa la afectación al patrimonio por medio sistemas informáticos, con o sin fines lucrativos, el cual genera impunidad de los actos de sabotaje informático contra las empresas o personas para reducir su competitividad.

Recomendaciones

Primero: Congreso de la República por parte de las instituciones con iniciativa legislativa y la sociedad civil, la adhesión del Perú al convenio de Budapest, puesto que en América solo lo han ratificado: USA, Canadá, Panamá, República Dominicana y el 2017 Chile, el no existir una legislación uniforme en delitos informáticos genera dualidad de delitos y problemas de interpretación dogmática, y además, la migración de la delincuencia on line a esta parte del planeta ya que la criminalidad informática, sabe que la legislaciones diferentes en cada país latinoamericano son una ventaja para que estas nuevas conductas delictivas sigan cubiertas bajo el manto de la impunidad.

Segundo: El Congreso de la República dele legislar en forma expresa y tipificar los delitos informáticos contra el patrimonio, diferenciando las modalidades, sean éstos delitos de fraude, estafa, sabotaje o hurto informático.

Tercero: En todas las Universidades se debe incluir un curso obligatorio de derecho informático, así como a nivel de la formación primaria y secundaria se debe incluir en la malla curricular el curso de informática, con énfasis en la prevención de todo tipo de delitos informáticos.

Cuarto: Se deben crear Fiscalías especializadas en delitos informáticos para que la investigación y sanción de estos delitos sea eficiente, más cuando el avance de la informática es mucho más acelerado, son delitos emergentes en aumento y la comisión suele ser cada vez más sofisticados.

Quinto: Se debe crear una Corte internacional con competencia en delitos informáticos, debido a que los diferentes delitos informáticos son cometidos de cualquier parte del mundo y los estados son limitados e imposibilitados por su jurisdicción para la investigación y sanción de actos criminales que se encuentran y cometen delitos con el uso de los medios informáticos desde otras jurisdicciones.

Referencias bibliográficas

Acurio, S. M. (Julio de 2018). *Entrevista de profundidad para la investigación*. Ecuador.

Álvarez, A. (Julio de 2018). *Entrevista de profundidad para la investigación*. España.

Manjarres, I. (Julio de 2018). *Entrevista de profundidad para la investigación.* Colombia.

Peña, D. (Julio de 2018). *Entrevista de profundidad para la investigación. Perú.*

Semprini, G. M. (Julio de 2018). *Entrevista de profundidad para la investigación.* Argentina.

Silva, G. A. (Julio de 2018). *Entrevista de profundidad para la investigación*. Perú.

Anexo 2: Instrumentos de recolección de datos

GUÍA DE ENTREVISTA

Dirigido a expertos nacionales y extranjeros

ESCUELA DE POSGRADO
UNIVERSIDAD CÉSAR VALLEJO

TRATAMIENTO JURÍDICO PENAL DE LOS DELITOS INFORMÁTICOS CONTRA EL PATRIMONIO

La presente investigación tiene como finalidad recoger su opinión para analizar el tratamiento jurídico penal de los delitos informáticos contra el patrimonio.

Entrevistado :……

Cargo :……

Institución :……

Breve resumen curricular:……...

1. ¿Qué opina respecto al acelerado avance de tecnologías informáticas y las modalidades de comisión de delitos?

   ……
   ……..……
   ……
   ……..……
   ……
   ……..

2. ¿Considera usted que la legislación sobre delitos informáticos es eficiente para sancionar las nuevas formas delictivas con el uso de las tecnologías informáticas? ¿Por qué?

   ……
   ……..……
   ……
   ……..……
   ……
   ……..

3. ¿Considera usted adecuado comprender a la estafa, hurto y sabotaje informático dentro del *nomen iuris* “fraude informático”? ¿Por qué?

……
……
……
……
……
……

4. ¿Considera usted que los bancos están dispuestos a denunciar penalmente delitos de hurto sistemáticos de cuentas bancarias y otros? ¿Por qué?

……
……
……
……
……
……

5. Explique ¿En la legislación penal existe regulación específica del delito de hurto informático?

……
……
……
……
……
……

6. ¿Considera usted que tanto las personas como las empresas están expuestos a ser víctimas de fraudes informáticos? ¿Por qué?

……
……
……
……
……
……

7. ¿En la actualidad existen estrategias claras para la prevención y sanción de delitos de fraude informático? Si fuera afirmativa ¿Cuáles?

……
……
……
……
……
……

8. ¿Le genera confianza las plataformas informáticas para realizar compras y contratar servicios a través de internet? ¿Por qué?

……
……
……
……

……
……..

9. Explique ¿En la legislación penal existe regulación específica del delito de estafa informática?

……
……..……
……
……..……
……
……..

10. ¿Considera usted que cuando un pirata informático destruye información y *softwares* en la red afecta el patrimonio de la víctima? ¿Por qué?

……
……..……
……
……..……
……
……..

11. Explique ¿En la legislación penal existe regulación específica del delito de sabotaje informático?

……
……..……
……
……..……
……
……..

12. ¿Considera usted que la vigente regulación contribuye con la efectiva prevención de los delitos informáticos contra el patrimonio? ¿Por qué?

……
……..……
……
……..……
……
……..

13. ¿Considera usted necesario una reforma legislativa para prevenir y sancionar los delitos informáticos contra el patrimonio? ¿Por qué?

……
……..……
……
……..……
……
……..

14. ¿Tiene usted alguna opinión adicional sobre la presente investigación? Si fuera afirmativa ¿Cuál?

……
……..……
……
……..

……………………………………………………………………………………………
……………………………………………………………………..

Muchas gracias por su valiosa opinión

GUÍA DE ENTREVISTA

Dirigido a expertos nacionales

ESCUELA DE POSGRADO
UNIVERSIDAD CÉSAR VALLEJO

TRATAMIENTO JURÍDICO PENAL DE LOS DELITOS INFORMÁTICOS CONTRA EL PATRIMONIO, DISTRITO JUDICIAL DE LIMA, 2018

La presente investigación tiene como finalidad recoger su opinión para analizar el tratamiento jurídico penal de los delitos informáticos contra el patrimonio, Distrito Judicial de Lima, 2018.

Entrevistado :……

Cargo :……

Institución :……

Breve resumen curricular:……..

1. ¿Qué opina respecto al acelerado avance de tecnologías informáticas y las modalidades de comisión de delitos?

   ……
   ……..……
   ……
   ……..……
   ……
   ……..

2. ¿Considera usted que la legislación sobre delitos informáticos es eficiente para sancionar las nuevas formas delictivas con el uso de las tecnologías informáticas? ¿Por qué?

   ……
   ……..……
   ……
   ……..……
   ……
   ……..

3. ¿Considera usted adecuado comprender a la estafa, hurto y sabotaje informático dentro del *nomen iuris* “fraude informático”? ¿Por qué?

……
……
……
……
……
……..

4. ¿Considera usted que los bancos están dispuestos a denunciar penalmente delitos de hurto sistemáticos de cuentas bancarias y otros? ¿Por qué?

……
……
……
……
……
……..

5. Explique ¿En la legislación penal existe regulación específica del delito de hurto informático?

……
……
……
……
……
……..

6. ¿Qué opinión le merece la vigente regulación sobre la prevención y sanción del hurto informático?

……
……
……
……
……
……..

7. ¿Considera usted que la ley de delitos informáticos cumple con el principio de tipicidad para sancionar el hurto informático? ¿Por qué?

……
……
……
……
……
……..

8. ¿Considera usted que tanto las personas como las empresas están expuestos a ser víctimas de fraudes informáticos? ¿Por qué?

……
……
……
……
……
……

9. ¿Cree usted adecuado que la regulación de delitos informáticos contra el patrimonio se traduzca únicamente en fraude informático? ¿Por qué?

……
……
……
……
……
……

10. ¿En la actualidad existen estrategias claras para la prevención y sanción de delitos de fraude informático? Si fuera afirmativa ¿Cuáles?

……
……
……
……
……
……

11. ¿Le genera confianza las plataformas informáticas para realizar compras y contratar servicios a través de internet? ¿Por qué?

……
……
……
……
……
……

12. Explique ¿En la legislación penal existe regulación específica del delito de estafa informática?

……
……
……
……
……
……

13. ¿Considera usted que la ley de delitos informáticos cumple con el principio de tipicidad para sancionar la estafa informática? ¿Por qué?

……
……
……
……
……
……

14. ¿Considera usted que cuando un pirata informático destruye información y *softwares* en la red afecta el patrimonio de la víctima? ¿Por qué?

……
……
……
……
……
……

15. Explique ¿En la legislación penal existe regulación específica del delito de sabotaje informático?

……
……
……
……
……
……

16. ¿Considera usted que la ley de delitos informáticos cumple con el principio de tipicidad para sancionar el sabotaje informático? ¿Por qué?

……
……
……
……
……
……

17. ¿Considera usted que la vigente regulación contribuye con la efectiva prevención de los delitos informáticos contra el patrimonio? ¿Por qué?

……
……
……
……
……
……

18. ¿Considera usted necesario una reforma legislativa para prevenir y sancionar los delitos informáticos contra el patrimonio? ¿Por qué?

……
……
……
……
……
……

19. ¿Tiene usted alguna opinión adicional sobre la presente investigación? Si fuera afirmativa ¿Cuál?

……
……
……
……
……
……

Muchas gracias por su valiosa opinión

Anexo 3: Certificados de validación de instrumentos

ESCUELA DE POSGRADO
UNIVERSIDAD CÉSAR VALLEJO

CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO POR DE JUICIO DE EXPERTOS

Nº	CATEGORÍAS/ ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
	Categoría: Tratamiento jurídico penal	**Si**	**No**	**Si**	**No**	**Si**	**No**	
1	¿Qué opina respecto al acelerado avance de tecnologías informáticas y las modalidades de comisión de delitos?							
2	¿Considera usted que la legislación sobre delitos informáticos es eficiente para sancionar las nuevas formas delictivas con el uso de las tecnologías informáticas? ¿Por qué?							
3	¿Considera usted adecuado comprender a la estafa, hurto y sabotaje informático dentro del *nomen iuris* "fraude informático"? ¿Por qué?							
	Categoría: Hurto informático	**Si**	**No**	**Si**	**No**	**Si**	**No**	
4	¿Considera usted que los bancos están dispuestos a denunciar penalmente delitos de hurto sistemáticos							

	de cuentas bancarias y otros? ¿Por qué?							
5	Explique ¿En la legislación penal existe regulación específica del delito de hurto informático?							
6	¿Qué opinión le merece la vigente regulación sobre la prevención y sanción del hurto informático?							
7	¿Considera usted que la ley de delitos informáticos cumple con el principio de tipicidad para sancionar el hurto informático? ¿Por qué?							
	Categoría: Fraude informático	**Si**	**No**	**Si**	**No**	**Si**	**No**	
8	¿Considera usted que tanto las personas como las empresas están expuestos a ser víctimas de fraudes informáticos? ¿Por qué?							
9	¿Cree usted adecuado que la regulación de delitos informáticos contra el patrimonio se traduzca únicamente en fraude informático? ¿Por qué?							
10	¿En la actualidad existen estrategias claras para la prevención y sanción de delitos de fraude informático? Si fuera afirmativa ¿Cuáles?							
	Categoría: Estafa informática	**Si**	**No**	**Si**	**No**	**Si**	**No**	
11	¿Le genera confianza las plataformas informáticas para realizar compras y contratar servicios a través de							

	internet? ¿Por qué?							
12	¿Considera usted que la ley de delitos informáticos cumple con el principio de tipicidad para sancionar la estafa informática? ¿Por qué?							
13	Explique ¿En la legislación penal existe regulación específica del delito de estafa informática?							
	Categoría: Sabotaje informático	**Si**	**No**	**Si**	**No**	**Si**	**No**	
14	¿Considera usted que cuando un pirata informático destruye información y softwares en la red afecta el patrimonio de la víctima? ¿Por qué?							
15	¿Considera usted que la ley de delitos informáticos cumple con el principio de tipicidad para sancionar el sabotaje informático? ¿Por qué?							
16	Explique ¿En la legislación penal existe regulación específica del delito de sabotaje informático?							
17	¿Considera usted que la vigente regulación contribuye con la efectiva prevención de los delitos informáticos contra el patrimonio? ¿Por qué?							
18	¿Considera usted necesario una reforma legislativa para prevenir y sancionar los delitos informáticos contra el patrimonio? ¿Por qué?							

19	¿Tiene usted alguna opinión adicional sobre la presente investigación? Si fuera afirmativa ¿Cuál?							

Observaciones (precisar si hay suficiencia):_____

Opinión de aplicabilidad: **Aplicable [ ]** **Aplicable después de corregir [ ]** **No aplicable [ ]**

Apellidos y nombres del juez validador. **DNI:……**

Especialidad del validador:……

…….de……..del 20…..

[1]**Pertinencia:**El ítem corresponde al concepto teórico formulado.
[2]**Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo
[3]**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión

---

Firma del Experto Informante.

Anexo 4: Matriz de categorización

Título: Tratamiento jurídico penal de los delitos informáticos contra el patrimonio, Distrito Judicial de Lima, 2018

Problema	Problema de investigación	Objetivos de investigación	Categoría	Sub categoría	Fuente (informante)	Técnica	Instrumento
En la actualidad se observa que cada vez más las nueves sistemas de información, nuevas tecnologías, sistemas informáticos y en específico las nuevas tecnologías informáticas ha ido avanzando, donde existen muchos expertos en la materia, quienes hacen y desasen diversos software. En uso de estas nuevas tecnologías informáticas se cometen un sin número de delitos sin que siquiera se perciba, toda vez que la consumación de dichos ilícitos es en la red informática, difícil de	¿Cómo es el tratamiento jurídico penal de los delitos informáticos contra el patrimonio, Distrito Judicial de Lima, 2018?	Analizar el tratamiento jurídico penal de los delitos informáticos contra el patrimonio, Distrito Judicial de Lima, 2018.	Tratamiento jurídico penal	• Tratamiento procesal. • Tratamiento legislativa	Expertos en informática y delitos informáticos	Entrevista Análisis de fuentes documentales	Guía de entrevista Ficha de análisis de fuentes documentarias
	¿Cómo es el tratamiento jurídico penal de los delitos informáticos contra el patrimonio en su modalidad de hurto?	Analizar el tratamiento jurídico penal de los delitos informáticos contra el patrimonio en su modalidad de hurto.	Hurto	• Hurto sistemático • Hurto de valores			
	¿Cómo es el tratamiento jurídico penal de los delitos informáticos contra el patrimonio en su modalidad de fraude?	Analizar el tratamiento jurídico penal de los delitos informáticos contra el patrimonio en su modalidad de fraude.	Fraude	• Fraude al sistema • Fraude en los datos			
	¿Cómo es el	Analizar el	Estafa	• Estafa			

identificar muchas veces, sin embargo, existen también actos ilícitos y a pesar que no lo fueran, vulneran bienes jurídicos penalmente relevantes en forma virtual, los mismos que no son sancionados debido a que existe deficiente regulación sobre la sanción de los delitos informáticos, toda vez que existen vacíos legales frente al desarrollo de las nuevas tecnologías informáticas e incremento de la ciberdelincuencia.	tratamiento jurídico penal de los delitos informáticos contra el patrimonio en su modalidad de estafa?	tratamiento jurídico penal de los delitos informáticos contra el patrimonio en su modalidad de estafa.		informática • Modalidades de estafa			
	¿Cómo es el tratamiento jurídico penal de los delitos informáticos contra el patrimonio en su modalidad de sabotaje informático?	Analizar el tratamiento jurídico penal de los delitos informáticos contra el patrimonio en su modalidad de sabotaje informático.	Sabotaje informático	• Destrucción de datos • Alteración de sistemas			

Anexo 5: Matriz de triangulación

Nº de pregunta	Entrevistado 1 Dr. Santiago Martín Acurio Del Pino (Ecuador)	Entrevistado 2 Abg. Ivan Manjarres Bolaño (Colombia)	Entrevistado 3 Dr. Andrés Álvarez Pérez (España)	Entrevistado 4 Ing. Gaston Miguel Semprini (Argentina)	Entrevistado 5 Mg. Daniel Peña Labrin (Perú)	Entrevistado 6 Dr. Gustavo Adolfo Silva Huamán (Perú)	Conclusión
1. ¿Qué opina respecto al acelerado avance de tecnologías informáticas y las modalidades de comisión de delitos?	El uso y masificación de las Tecnologías de la Información y la Comunicación, a supuesto varios avances en la ciencia y la tecnología, pero también se ha convertido en un factor criminógeno que ha permitido la comisión de nuevas modalidades de delitos, los cuales dependiendo de la legislación podrían no encontrarse tipificados, lo cual es una problema al momento de su persecución, desde la perspectiva del principio de legalidad.	Pareciera que van al mismo ritmo, sobre todo en lo que concierne al robo de datos. Las diferentes entidades, sean de comercio o de servicios, en su afán de captar más usuarios, incitan en un momento dado, a que las personas para hacer uso de estos ofrecimientos, exponen sus datos personales, exponiéndolos con esto a que sean víctimas potenciales para la comisión de este tipo de delitos.	Hoy en día, el avance de las tecnologías y el fácil uso de las mismas, han proporcionado herramientas a los delincuentes, con los que cometer delitos más sofisticados y mucho más difícil de identificar.	Creo que la el avance tecnológico va de la mano de los distintos delitos cometidos con dispositivos tecnológicos. Pero más allá de eso, considero que es necesario que los organismos de investigación especializados, cuenten con personal capacitado y formado para llevar adelante esas investigaciones y así obtener resultados favorables en la investigación.	La tecnología, no solo ha traído la mejora de la calidad de vida de la población global, sino también las actividades delictivas se han modernizado en su actuar delincuencial mejorando obstenciblemente su performance criminal.	Que el aumento de la criminalidad en el ámbito de tecnologías informáticas obedece al propio avance de la criminalidad en nuestro País, atendiendo a que dicho fenómeno no solo se encuentra relacionado con este tipo de delitos sino con la delincuencia en general, que al no ser contrarrestadas oportunamente por el Estado su incremento crece exponencialmente, más aún si se tiene presente el creciente avance y permanente innovación del sector tecnológico.	Los entrevistados coinciden que la criminalidad informática va de la mano con el acelerado avance de las tecnologías informáticas, permitiendo nuevas modalidades de comisión de delitos cada vez más sofisticados, difíciles de identificar, por lo que es necesario contar con organismos y funcionarios especializados para llevar adelante las investigaciones con resultados favorables.
2. ¿Considera usted que la legislación sobre delitos informáticos es eficiente para sancionar las nuevas formas delictivas con el uso de las tecnologías informáticas? ¿Por qué?	En el Ecuador con la expedición del Código Orgánico Integral Penal, se amplió el espectro de los delitos informáticos, mejorando la redacción y ampliando tipos que no existían contemplados antes en el Código Penal anterior, eso fue un avance en la legislación.	La intangibilidad de estos delitos hacen parecer o dan la sensación, en un momento dado, que la legislación existente no es capaz de enmarcar estos delitos y sancionarlos de una forma eficaz.	Cada día es más eficiente y efectiva la legislación referente a los Delitos Informáticos. En España se ha realizado un gran avance en legislar en referencia en esta clase de delitos, con la actualización del Código Penal en el año 2015, se dio un gran paso en este asunto.	No creo que sea eficiente nunca, porque siempre la tecnología y las nuevas formas delictivas, va más rápido que el derecho. Pero si considero que es necesario ir trabajando para mejorar la legislación y/o adherirse a distintos convenios internacionales para ir combatiendo dichos delitos.	Aun falta no solo legislar sobre las nuevas actividades delictivas, sino también difundir y explicar la nueva criminalidad informática en su connotación holística.	La legislación existente resulta insuficiente, toda vez que continuamente se renuevan las modalidades delictivas en el ámbito informatice, asimismo si se tiene presente que en nuestro país las herramientas existentes para contrarrestar dichos ilícitos no resultan ser suficientes, y que poco es el efecto disuasivo en la proliferación del mismo.	En Ecuador y en España se han realizado buenas reformas respecto a los delitos informáticos, ampliándose la redacción de los tipos penales no contemplados, actualizándose la legislación penal. Por otro lado, los entrevistados de Colombia y Argentina consideran que la legislación sobre delitos informáticos es insuficiente para sancionar en forma eficaz las nuevas formas delictivas con el uso de las

Nº de pregunta	Entrevistado 1 Dr. Santiago Martín Acurio Del Pino (Ecuador)	Entrevistado 2 Abg. Ivan Manjarres Bolaño (Colombia)	Entrevistado 3 Dr. Andrés Álvarez Pérez (España)	Entrevistado 4 Ing. Gaston Miguel Semprini (Argentina)	Entrevistado 5 Mg. Daniel Peña Labrin (Perú)	Entrevistado 6 Dr. Gustavo Adolfo Silva Huamán (Perú)	Conclusión
							tecnologías informáticas. Con esta última respuesta coinciden los entrevistados nacionales señalando que la legislación es insuficiente y esto va acompañado de la falta de difusión de la criminalidad informática.
3. ¿Considera usted adecuado comprender a la estafa, hurto y sabotaje informático dentro del *nomen iuris* "fraude informático"? ¿Por qué?	No me parece, los fraudes informáticos son específicos, pertenecen a las defraudaciones en genérico, es un delito de carácter patrimonial, pero diferente del hurto y sabotaje.	La comisión de estos delitos en lo que respecta a espacio, tiempo y forma, no da para que se les nomine de esta forma.	Si claro, El Modus Operandi actual de este tipo de delitos, está basado en el uso de las nuevas tecnologías, en especial, el uso de Internet, es por ello que el encajarlo en "Fraude Informático", es totalmente correcto.	Si por supuesto, siempre en todos los casos debiéndose demostrar con las distintas pericias que sean necesarias el fraude cometido.	Si, porque todo los delitos tienen un componente de dañosidad de engaño, de allí que esta circunscritos en el fraude informático, para que guarde relación con el convenio de Budapest, pero a mi punto de vista no es suficiente.	Al respecto el delito de fraude informatice se encuentra previsto y sancionado en el artículo 8 de la Ley N° 30096, que sanciona la alteración, supresión, borrado de datos informáticos o cualquier interferencia o manipulación en el funcionamiento de un sistema informático, por lo que en estricto se refiere a cualquier tipo de manipulación de datos o el funcionamiento de un sistema, por lo que la estafa, no corresponde ser comprendidas dentro del mismo, sin embargo respecto al sabotaje, se entiende que ello corresponde a la alteración en cualquier modalidad de datos en un sistema informático, por lo que puede entenderse dentro del mismo, empero respecto al hurto no existe un verbo rector que incluya dicha modalidad, lo cual más bien podría ser contemplada dentro del tipo penal Interceptación de Datos	Se concluye que los entrevistados de España y uno de Perú manifiestan que es adecuado comprender a la estafa, hurto y sabotaje informático dentro del *nomen iuris* "fraude informático, sin embargo, Acurio (2018) entrevistado de Ecuador, Manjarres (2018) entrevistado de Colombia y Silva (2018) entrevistado de Perú discrepan con dicha postura, puesto que el primero considera que el los fraudes informáticos son específicos, pertenecen a las defraudaciones en genérico, es un delito de carácter patrimonial, pero diferente del hurto y sabotaje, y no da para que se les nomine solo como fraude, y finalmente, se señala que el fraude se refiere a cualquier tipo de manipulación por lo que la estafa no corresponde ser comprendida, pero el sabotaje podría cuadrar dentro del fraude por tratarse de alteración de datos, pero sobre el hurto no existe un verbo rector.

Nº de pregunta	Entrevistado 1 Dr. Santiago Martín Acurio Del Pino (Ecuador)	Entrevistado 2 Abg. Ivan Manjarres Bolaño (Colombia)	Entrevistado 3 Dr. Andrés Álvarez Pérez (España)	Entrevistado 4 Ing. Gaston Miguel Semprini (Argentina)	Entrevistado 5 Mg. Daniel Peña Labrin (Perú)	Entrevistado 6 Dr. Gustavo Adolfo Silva Huamán (Perú)	Conclusión
						informáticos previsto en el artículo 7 de la citada ley.	
4. ¿Considera usted que los bancos están dispuestos a denunciar penalmente delitos de hurto sistemáticos de cuentas bancarias y otros? ¿Por qué?	Bueno el hurto sistemático, hay que aclararlo, ya que por principio de legalidad en el Ecuador no existe el hurto informático, lo que existe es el Fraude Informático o puede ser Peculado Bancario, dependiendo de los hechos. En cuanto a si los Bancos denuncian esos tipos penales, hay que recordar que muchos de ellos quedan como cifra negra, debido a que podrían constituir un atentado a la imagen corporativa del Banco, y por ello en muchos casos buscan solucionar esos problemas de forma interna. Sin acudir a la Administración de Justicia o a la Fiscalía General del Estado.	Si lo deben hacer tanto por el bien de los clientes como el de su misma imagen, aunque en algunos casos tratan de minimizar el daño que les han causado para, precisamente, mantener su clientela.	Si, Por supuesto, mi experiencia en la investigación relacionadas con entidades bancarias, me ha proporcionado la evidencia de total colaboración y disposición, no solo a la denuncia de los mismos, si no a prestar total colaboración en las investigaciones que se llevan a cabo.	No, porque en realidad sería un desprestigio como institución y haría denotar que no cuenta con la seguridad necesaria, y haría perder la confianza de sus clientes o posibles nuevos clientes.	Solo cuando estos son significativos, ya que no lo hacen públicos con frecuencia, por el tema de no provocar "pánico financiero" y de eso se aprovecha la criminalidad informática.	Considero que en la mayoría de casos no, por la imagen de su entidad, dado que ello pone en evidencia las falencias de su seguridad, y que también implica un resarcimiento económico, de verificarse que la falla fue del sistema de la propia entidad, sin embargo en los casos que fuere por descuido y negligencia del propio cliente lo común es que lo pongan en conocimiento de los usuarios o la autoridad competente, pero ello es cuando existe una significativa cantidad de casos similares.	Casi todo los entrevistados coinciden que los bancos no están dispuestos a denunciar penalmente delitos de hurto sistemáticos de cuentas bancarias y otros por la protección de su imagen corporativo, para mantener la clientela, para evitar su propio desprestigio y no hacer denotar la inseguridad, por no perder la confianza de sus clientes y futuros clientes y evitar el pánico financiero, sin embargo, Álvarez (2018) entrevistado de España señala que los bancos Españolas si están dispuestos a colaborar en la denuncia e investigación criminal.
5. Explique ¿En la legislación penal existe regulación específica del delito de hurto informático?	No existe en la legislación penal del Ecuador, doctrinalmente puede existir el hurto de servicios de telecomunicaciones.	Si. En nuestro código penal con la expedición de la ley 1273 de 2009 allí se tipifica el delito de Hurto informático en el artículo 13.	Como tal no existe, pero está incluido en el artículo 248 del Código Penal Español, con el concepto "Fraudes Informáticos".	Contamos en la Argentina con la ley 26388 de delitos informáticos, pero no está especificado el hurto informático.	Existió en el artículo 186 del C.P., segundo párrafo numeral 3, modificado por la ley 26319, que disponía además "la pena será no menor de 4 años ni mayor de 8 años, "si el hurto es cometido mediante la utilización de sistemas de transferencia electrónica de fondos de la telemática en	==========	En la legislación penal ecuatoriana no existe regulación expresa del hurto informático, mientras en la legislación Española, tampoco existe regulación expresa, pero está comprendido dentro de fraudes informáticos, en el caso peruano si había una regulación en el artículo 186 del código Penal, sin embargo fue derogada por la Ley 30096 modificada por la Ley 30171. A diferencia de las demás legislaciones, en Colombia si existe

Nº de pregunta	Entrevistado 1 Dr. Santiago Martín Acurio Del Pino (Ecuador)	Entrevistado 2 Abg. Ivan Manjarres Bolaño (Colombia)	Entrevistado 3 Dr. Andrés Álvarez Pérez (España)	Entrevistado 4 Ing. Gaston Miguel Semprini (Argentina)	Entrevistado 5 Mg. Daniel Peña Labrin (Perú)	Entrevistado 6 Dr. Gustavo Adolfo Silva Huamán (Perú)	Conclusión
					general o la violación del empleo de claves secretas", y fue derogado por la DCD única de la ley 30096, modificada por la ley 30171.		regulación expresa del delito de hurto informático, el cual está tipificada en la Ley 1273.
6. ¿Considera usted que tanto las personas como las empresas están expuestos a ser víctimas de fraudes informáticos? ¿Por qué?	Los atacantes informáticos, buscan aprovechar la falta de conocimiento y previsión de las víctimas. Falta una cultura de Ciberseguridad que es aprovechada por los atacantes para cometer este tipo de delitos. En especial la llamada ingeniería social.	Totalmente. En esta época el uso masificado de los elementos para comunicación y la aparición de las llamadas redes sociales nos exponen a que nuestros datos personales estén expuestos para que de allí sean utilizados por este tipo de delincuentes para iniciar su accionar delictivo.	Por supuesto, En las ponencias que de vez en cuando hago, es un tema en la hago especial insistencia. Nunca se puede estar completamente seguro en este mundo en el que vivimos, siempre hay que estar en alerta y preparados ante cualquier fraude. El más común en estos últimos tiempos es el que se comete a través de "CRYPTOLOCKER", consistente en encriptar todos los archivos del disco duro y a continuación solicitar una elevada cantidad de dinero, para desencriptarlos.	Si y siempre lo estarán, porque la seguridad absoluta no existe, si se deben tomar todos los recaudos de seguridad pertinentes, pero siempre hay acciones delictivas nuevas que el usuario común o personal de empresas no está al tanto o capacitados, permitiendo accesos indebidos a datos valiosos personales o de la empresa por ejemplo los casos de Ramsomware.	Si, por la naturaleza de sus actividades donde el factor económico es determinante para la delincuencia online.	Todas las personas, naturales o jurídicas, son susceptibles de ser agraviados en este tipo de delitos, por cuantos ello implica el aprovechamiento a través de tecnologías en un sistema determinado, o los datos que se transfieren a través de medios tecnológicos.	Todo los entrevistados coinciden que tanto las personas como las empresas están expuestos a ser víctimas de fraudes informáticos, los atacantes informáticos se aprovechan de la falta de conocimiento y cultura de ciberseguridad de sus víctimas, nunca de puede estar de todo seguro y siempre se estará expuesto a potenciales fraudes, y últimamente se viene practicando nuevas modalidades como la "CRYPTOLOCKER" y Ramsomware, modalidad, mediante el cual se encripta o restringe el acceso a archivos de la víctima, pidiendo grandes cantidades de dinero para desincriptarlos, es decir, para que su propietario pueda obtener la clave y acceder a los archivos "secuestrados".
7. ¿En la actualidad existen estrategias claras para la prevención y sanción de delitos de fraude informático? Si	Para la sanción de los Fraudes existen las normas del Código Orgánico Integral Penal. En el campo de la prevención, falta la aplicación de normas como	Si, sobre todo en las entidades bancarias y en las dependencias del gobierno, el tratamiento de y uso de los datos personales están	Si, efectivamente, en España existe claras estrategias para la lucha y prevención de este tipo de fraudes,	Creo que el convenio de Budapest lo considera.	No las hay, el estado no formula una cultura de prevención de criminalidad informática. En	Tengo entendido que a través de la SBS se realizan campañas de información a las personas respecto a las actividades delictivas en	A diferencia de Ecuador, Colombia, España y Argentina, en el Perú no existen estrategias claras para la prevención y sanción de delitos de fraude

Nº de pregunta	Entrevistado 1 Dr. Santiago Martín Acurio Del Pino (Ecuador)	Entrevistado 2 Abg. Ivan Manjarres Bolaño (Colombia)	Entrevistado 3 Dr. Andrés Álvarez Pérez (España)	Entrevistado 4 Ing. Gaston Miguel Semprini (Argentina)	Entrevistado 5 Mg. Daniel Peña Labrin (Perú)	Entrevistado 6 Dr. Gustavo Adolfo Silva Huamán (Perú)	Conclusión
fuera afirmativa ¿Cuáles?	la ISO 27000 sobre la Seguridad de la Información por parte de las entidades públicas y privadas. Las instituciones financieras deben emprender campañas de información sobre las modalidades de fraudes informáticos, tales como el pishing o el pharming a fin de que los usuarios de la banca virtual no sean perjudicados. Al igual sobre las tarjetas de crédito y débito que pueden ser clonadas fácilmente y así perjudicar a sus tenedores.	protejidos por ley.	entre otras el refuerzo en las leyes que tratan de estos temas, como también una campaña de información para detectar estos delitos y saber actuar ante ellos.		Argentina, el estado tiene un protocolo de grooming que lo difunde a la sociedad igualmente en chile, acá no existe nada parecido, tampoco existe el delito de sexting (muy común en la posmodenidad).	entidades financieras, y que por intermedio de la Policía Nacional del Perú también se informa preventivamente sobre diversos ilícitos en este área, sin embargo, resulta insuficiente, puesto que at igual que los delitos de Lavado de Activos o Trafico de Drogas es necesario una política criminal especifica.	informático. En ecuador existe ISO 27000 sobre la Seguridad de la Información por parte de las entidades públicas y privadas, en España aparte de la legislación, existen campañas de información para detectar estos delitos y saber actuar ante ellos y en Argentina existe el protocolo de grooming que lo difunde a la sociedad sobre los fraudes informáticos. Del cual se desprende que en el Perú no se ha tomado en cuenta la real dimensión de los delitos informáticos, puesto que se actúa únicamente en forma reactiva, no existe legislación adecuada ni políticas de prevención de delitos informáticos contra el patrimonio.
8. ¿Le genera confianza las plataformas informáticas para realizar compras y contratar servicios a través de internet? ¿Por qué?	Todo depende de la plataforma, si esta cumple con los estándares como: ◦ ISO 27001:2013: Buenas prácticas para el manejo de sistemas de información y proceso de datos. ◦ PCI DSS: Transacciones y pagos con tarjetas de crédito. ◦ OWASP ASVS: Seguridad de aplicaciones web Si el sitio o página web tiene estas seguridades se puede realizar transacciones seguras.	Personalmente no realizó ningún tipo de compras por internet. Tramites si, donde este seguro que la información suministrada va a tener un tratamiento adecuado.	Soy una persona que compra a menudo por Internet, y me generan mucha confianza, claro está, que siempre realizo estas comprar en plataformas de compañías de confianza y de renombre. Los problemas pueden surgir, cuando se realizan en páginas web extranjeras que no tienen los	Sí, siempre tomando las precauciones pertinentes.	No genera confianza, y principalmente por la brecha digital, el Perú tiene el porcentaje más bajo de comercio electrónico en la Región.	Al respecto existen ciertas medidas de seguridad a seguir, tales como la fiabilidad de las páginas web de compra, y seguir las políticas de seguridad de dichas entidades.	Se concluye que las plataformas informáticas generarán confianza para realizar compras y contratar servicios a través de internet siempre que cumplan estándares de seguridad que garanticen realizar las transacciones sin riesgo, o que la compañía sea uno conocido de renombre, puesto las compañías extranjeras que no tengas los certificados de seguridad mínimos genera desconfianza para realizar cualquier tipo de transacción.

Nº de pregunta	Entrevistado 1 Dr. Santiago Martín Acurio Del Pino (Ecuador)	Entrevistado 2 Abg. Ivan Manjarres Bolaño (Colombia)	Entrevistado 3 Dr. Andrés Álvarez Pérez (España)	Entrevistado 4 Ing. Gaston Miguel Semprini (Argentina)	Entrevistado 5 Mg. Daniel Peña Labrin (Perú)	Entrevistado 6 Dr. Gustavo Adolfo Silva Huamán (Perú)	Conclusión
			certificados de seguridad mínimos, ni con un nombre conocido.				
9. Explique ¿En la legislación penal existe regulación específica del delito de estafa informática?	La estafa informática es básicamente un delito computacional, más no informático. Es decir que para lograr el engaño del sujeto pasivo se lo hace a través por ejemplo de un anuncio en la página web, donde se vende un producto a menor precio que el que se puede conseguir en una tienda, por ejemplo un reloj ROLEX en USD. 1.000 dólares. El sujeto pasivo ve ese anuncio, se contacta con el sujeto activo, quien le dice que debe hacer una transferencia a una cuenta, o a través de Western Union o Money Gram, luego el sujeto activo, recibe la transferencia y envía el paquete al sujeto pasivo, quien al recibirlo encuentra una foto del ROLEX, por tanto se da cuenta que ha sido estafado, siendo medio fraudulento el engaño o abuso de confianza que generó el error sicológico en el sujeto pasivo que le llevo a la disposición patrimonial lesiva.	Si está regulado. (ver Ley 1273 de 2009 Colombia)	En nuestra legislación, en concreto en el artículo 248 del Código Penal, referente a La Estafa, aunque no se especifica la estafa informática, el desarrollo de dicho artículo, es de gran utilidad para poder tratar estos delitos.	Desconozco.	En el Perú no se sancionan correctamente los delitos informáticos como la estafa informática: solo el acceso ilícito; atentados contra la integridad de datos; delitos contra la indemnidad sexual; delitos contra la intimidad y secreto de las comunicaciones y contra la fe pública. (copia del convenio de budapest).	==========	Acurio (2018) entrevistado de Ecuador señala que la estafa es un delito computacional que consiste en lograr engañar a la víctima, es decir, generar error psicológico en la víctima que le conduzca al desprendimiento patrimonial, por otro lado, Manjarres (2018) entrevistado de Colombia señala que en su país si existe la regulación específica de la estafa informática, el cual se encuentra en la Ley 1273 de 2009, por el contrario, Álvarez (2018) advierte que en la legislación Española no existe en concreto la regulación específica de estafa informática, pero el artículo 148 referente a la estafa es de gran utilidad para tratar el delito de estafa. Por otro lado, Peña (2018) entrevistado peruano, señala que en el Perú no se sancionan correctamente los delitos informáticos como la estafa informática. En este sentido, se puede concluir que en el Perú no se ha tipificado en forma expresa la estafa informática.
10. ¿Considera usted que cuando un	Depende de la información, si esa información está en la	Si claro sobre todo el llamado patrimonio	En muchos casos, si, efectivamente, a	Si porque esa información y/o datos	Si ya que el patrimonio de la	Si, dado que resulta un bien no tangible de la	Los entrevistados consideran que cuando un

Nº de pregunta	Entrevistado 1 Dr. Santiago Martín Acurio Del Pino (Ecuador)	Entrevistado 2 Abg. Ivan Manjarres Bolaño (Colombia)	Entrevistado 3 Dr. Andrés Álvarez Pérez (España)	Entrevistado 4 Ing. Gaston Miguel Semprini (Argentina)	Entrevistado 5 Mg. Daniel Peña Labrin (Perú)	Entrevistado 6 Dr. Gustavo Adolfo Silva Huamán (Perú)	Conclusión
pirata informático destruye información y softwares en la red afecta el patrimonio de la víctima? ¿Por qué?	nube o almacenada en un dispositivo de almacenamiento. Ya que esta puede tener respaldo. También depende del tipo de información que ha sido destruida, ya que ahora la información puede tener una valor económico para la víctima y eso puede causarle un perjuicio patrimonial, pero como esta clase de delitos son de tipo pluriofensivo también puede afectar a la disponibilidad de la información y a su integridad.	intelectual porque la victima ha dedicado tiempo, estudio e investigación en la elaboración de estos.	nivel particular, muchas personas que han sufrido algún caso de destrucción de información, han tenido que recurrir a empresas externas, que se dedican a recuperar datos perdidos, con el consecuente gasto monetario. A nivel de empresas, la destrucción de datos, aparte del gasto en su recuperación, también está el descredito ante sus clientes, los cuales pueden optar por cambiar de empresa.	que se encuentran dentro de un software o sistema es información personal, es por ello que la ley 26388 prevé condenas para esos casos.	víctima no solo es material sino también inmaterial, en esta posmodernidad de la dictadura de la NTICS.	víctima, más aún, si la misma puede ser susceptible para la obtención de bien económico, tales como códigos de seguridad que permitan el acceso cuentas bancarias u otros.	pirata informático destruye información y softwares en la red afecta el patrimonio de la víctima, puesto que como señala Acurio (2018) ahora la información puede tener una valor económico para la víctima y eso puede causarle un perjuicio patrimonial, con ello concuerda Manjarres (2018) al decir que la víctima ha dedicado tiempo, estudio e investigación en la información destruida. Se debe tener en cuenta que el perjuicio patrimonial no solo es en razón a la destrucción de la información en sí, sino que, además, la empresa o persona, a efectos de recuperar la información destruida suele contratar profesionales o empresas externar, cuya contratación se traduce en un desprendimiento patrimonial como consecuencia de la destrucción de la información. El patrimonio no solo es material, sino también inmaterial.
11. Explique ¿En la legislación penal existe regulación específica del delito de sabotaje informático?	En el caso ecuatoriano existe el delito de daños informáticos. Art. 232 COIP.	Si existe este tipo penal (ver Ley 1273 de 2009).	En el Código Penal Español, como tal, no está reflejado, pero concretamente en el Artículo 264, viene especificado como Daños Informáticos y en cual, entra ese delito.	Desconozco	Estuvo en el artículo 207-b del Código Penal, y ahora en la Ley 30096 y modificada por la ley 30171, en el artículo 3: atentado contra la integridad de datos informáticos.	==========	Conforme señala Acurio (2018) en Ecuadro existe un delito símil al sabotaje informático, el cual es el delito de daños, asimismo, en la Legislación colombiana también existe regulado en la Ley 1273 de 2009, sin embargo, en el Código Penal Español no se

Nº de pregunta	Entrevistado 1 Dr. Santiago Martín Acurio Del Pino (Ecuador)	Entrevistado 2 Abg. Ivan Manjarres Bolaño (Colombia)	Entrevistado 3 Dr. Andrés Álvarez Pérez (España)	Entrevistado 4 Ing. Gaston Miguel Semprini (Argentina)	Entrevistado 5 Mg. Daniel Peña Labrin (Perú)	Entrevistado 6 Dr. Gustavo Adolfo Silva Huamán (Perú)	Conclusión
							encuentra tipificado como tal, pero el Artículo 264 del Código Penal Español, al igual que de Ecuador, regula como Daños informáticos, tipo penal en la que se puede cuadrar correctamente el sabotaje informático. A diferencia de los países antes nombrados, en la legislación penal peruana no existe en forma expresa la tipificación de delito de sabotaje informático, pero es posible que se puede encuadrar como atentado contra la integridad de datos informáticos conforme al artículo 3 de la Ley 30171 que modificó a la Ley 300096, sin embargo, se puede advertir que no se estaría cumpliendo con el principio de tipicidad para sancionar los delitos de sabotaje informático.
12. ¿Considera usted que la vigente regulación contribuye con la efectiva prevención de los delitos informáticos contra el patrimonio? ¿Por qué?	En la legislación ecuatoriana están comprendidas viarias modalidades de fraudes informáticos que permite su persecución, la única limitante puede ser que al ser delitos de tipo transnacional las evidencias o pruebas estén en otra jurisdicción, por ello la necesidad se suscribir el Convenio del Cibercrimen de la Comunidad Europea que permitiría una mejor cooperación internacional en el caso de los delitos	La regulación por sí sola no contribuye con la prevención de estos delitos. Se necesitan campañas educativas eficaces que alerten a las personas cuando utilicen cualquier medio informático del riesgo de ser víctima de estos delitos y la forma de evitarlos.	Las leyes Españolas, previenen los delitos informáticos contra el patrimonio, existe una extensa jurisprudencia al respecto. Pero si es verdad, que debería ser más concreta y una legislación Global, ya que en el momento que esos delitos, provienen de fuera de nuestras fronteras, la	Desconozco.	No completamente, se tiene que incluir: la estafa informática de manera indubitable, asimismo, la usurpación de identidad (la suplantacion no basta).	Es insuficiente, dado que solo se prevee un solo tipo penal contra el patrimonio.	Álvarez (2018), señala que leyes Españolas, previenen los delitos informáticos contra el patrimonio, pero advierte que debería ser más concreta y una legislación Global, ya que en el momento que esos delitos, provienen de fuera de nuestras fronteras, la investigación se hace más difícil, concordante a ello Acurio (2018) señala que el limitante puede ser que al ser delitos de tipo transnacional las evidencias

Nº de pregunta	Entrevistado 1 Dr. Santiago Martín Acurio Del Pino (Ecuador)	Entrevistado 2 Abg. Ivan Manjarres Bolaño (Colombia)	Entrevistado 3 Dr. Andrés Álvarez Pérez (España)	Entrevistado 4 Ing. Gaston Miguel Semprini (Argentina)	Entrevistado 5 Mg. Daniel Peña Labrin (Perú)	Entrevistado 6 Dr. Gustavo Adolfo Silva Huamán (Perú)	Conclusión
	informáticos y cibernéticos.		investigación se hace más difícil.				o pruebas estén en otra jurisdicción. Por otro lado, Manjarres (2018) señala que la regulación por sí sola no contribuye con la prevención de estos delitos. Se necesitan campañas educativas eficaces. La legislación peruana no previene los delitos informáticos contra el patrimonio, dado que la norma es una sola y genérica para todas las modalidades de delitos contra el patrimonio, por lo que se está lejos de la prevención.
13. ¿Considera usted necesario una reforma legislativa para prevenir y sancionar los delitos informáticos contra el patrimonio? ¿Por qué?	En el caso ecuatoriano no es necesario, con el actual COIP	La legislación debe ir a la par de los diferentes cambios tecnológicos y sobre todo en lo que respecta a la seguridad cuando se manejan datos personales o corporativos.	Considero, que siempre es necesario mejorar las leyes y reformarlas, los delincuentes siempre están actualizando sus métodos y procedimientos para la realización de delitos, es por ello, que la reforma legislativa para la lucha del Delito Informático, y no solo, el referente al Patrimonio, si no, a todos lo que abarcan este tipo de Delitos Informáticos.	Desconozco.	Si para perfeccionar los delitos informáticos contra el patrimonio de manera específica: estafa informática y usurpación de identidad.	Considero que debe extenderse los tipos penales en esta ley especial.	La mayoría de los entrevistados consideran que es necesario una reforma legislativa para prevenir y sancionar los delitos informáticos contra el patrimonio, y se hace énfasis que no solo debe ser respecto a los delitos informáticos contra el patrimonio, sino, sobre las demás modalidades de delitos informáticos, puesto que de acuerdo a las nuevas tecnologías informáticas existen nuevas modalidades de comisión de delitos y la legislación penal debe estar a la altura para prevenir y sancionar.
14. ¿Tiene usted alguna opinión adicional sobre la presente	Debe haber claridad terminológica en el tema de los delitos informáticos en especial sobre los fraudes	Este tipo de investigación contribuye a que se tenga una mayor y mejor	Este tipo de asuntos, son desgraciadamente muy desconocidos	No	Si entre muchas, que se proponga al Congreso de la República por parte	Que para la resolución de estos tipos de delitos, es necesario el apoyo técnico del área encargada, esto	Entre los principales aportes u opiniones de los expertos, claridad terminológica en el tema de los delitos

Nº de pregunta	Entrevistado 1 Dr. Santiago Martín Acurio Del Pino (Ecuador)	Entrevistado 2 Abg. Ivan Manjarres Bolaño (Colombia)	Entrevistado 3 Dr. Andrés Álvarez Pérez (España)	Entrevistado 4 Ing. Gaston Miguel Semprini (Argentina)	Entrevistado 5 Mg. Daniel Peña Labrin (Perú)	Entrevistado 6 Dr. Gustavo Adolfo Silva Huamán (Perú)	Conclusión
investigación? Si fuera afirmativa ¿Cuál?	informáticos desde el punto de vista de la tipicidad objetiva.	información sobre los delitos informáticos y su legislación lo cual sirve para prevenir a las personas que la consultan, ser víctima de este tipo de delitos.	por la población en general, y es interesante que se dé información al respecto, para no caer en esta clase de delitos.		de las instituciones con iniciativa legislativa y la sociedad civil, la adhesión del Perú al convenio de Budapest. En América solo lo han ratificado: USA, Canadá, Panamá, República Dominicana y el 2017 Chile, el no existir una legislación uniforme en delitos informáticos genera dualidad de delitos y problemas de interpretación dogmática, y además, la migración de la delincuencia on line a esta parte del planeta ya que la criminalidad informática, sabe que la legislaciones diferentes en cada país latinoamericano son una ventaja para que estas nuevas conductas delictivas sigan cubiertas bajo el manto de la impunidad.	es, la División de Delitos Informáticos de la PNP la cual no se abastece debido a la carga delictiva, más aun si se encuentra centralizada en la DIRINCRI en Lima, y que tampoco cuenta con todas las herramientas necesarias para encontrarse a la par con la delincuencia que se innova a diario.	informáticos en especial sobre los fraudes informáticos desde el punto de vista de la tipicidad objetiva, los delitos informáticos son muy desconocidos por la población en general, el Perú se debe adherir al convenio de Budapest y que en el Perú se debe ampliar el radio de acción de División de Delitos Informáticos de la PNP e implementar las herramientas necesarias.

Anexo 6: Matriz de desgravación de entrevista

Categoría	Subcategoría	Codificación
Tratamiento jurídico penal de los delitos informáticos	Tratamiento procesal.	Hoy en día, el avance de las tecnologías y el fácil uso de las mismas, han proporcionado herramientas a los delincuentes, con los que cometer delitos más sofisticados y mucho más difícil de identificar (Álvarez, 2018).
	Tratamiento legislativa	Acurio (2018) (…) en la legislación podrían no encontrarse tipificados, lo cual es una problema al momento de su persecución, desde la perspectiva del principio de legalidad. (…) que la legislación existente no es capaz de enmarcar estos delitos y sancionarlos de una forma eficaz (Manjarres, 2018).
Hurto informático	Hurto sistemático	(…) el hurto sistemático, hay que aclararlo, ya que por principio de legalidad en el Ecuador no existe el hurto informático (Acurio, 2018).
	Hurto de valores	(…) la Ley N° 30096, que sanciona la interceptación ilegitima de datos informáticos, el cual podría entenderse como hurto al apoderarse de datos de manera ilegal pertenecientes a un tercero, y que si bien de alguna manera se protege los datos informáticos, nuestra regulación resulta incipiente en este aspecto

		(Silva., 2018).
Fraude informático	Fraude al sistema	(…) los fraudes informáticos son específicos, pertenecen a las defraudaciones en genérico, es un delito de carácter patrimonial, pero diferente del hurto y sabotaje (Acurio, 2018).
	Fraude en los datos	(…) todo los delitos tienen un componente de dañosidad de engaño, de allí que esta circunscritos en el fraude informático (Peña, 2018).
Estafa informática	Estafa informática	En el Perú no se sancionan correctamente los delitos informáticos como la estafa informática (…) (Labrin, 2018).
	Modalidades de estafa	La estafa informática es básicamente un delito computacional, más no informático. (Acurio, 2018).
Sabotaje informático	Destrucción de datos	(…) muchas personas que han sufrido algún caso de destrucción de información, han tenido que recurrir a empresas externas, que se dedican a recuperar datos perdidos, con el consecuente gasto monetario (Álvarez, 2018).
	Alteración de sistemas	Lo que se tipifica es la manipulación de datos en diversas modalidades, lo cual se traduce en la alteración de los datos informáticos (Silva, 2018).

Anexo 7: Transcripción de los resultados de las entrevistas

Respecto al objetivo general.

Analizar el tratamiento jurídico penal de los delitos informáticos contra el patrimonio, Distrito Judicial de Lima, 2018.

1.- ¿Qué opina respecto al acelerado avance de tecnologías informáticas y las modalidades de comisión de delitos?

Dr. Santiago Martín Acurio Del Pino (Ecuador): *El uso y masificación de las Tecnologías de la Información y la Comunicación, a supuesto varios avances en la ciencia y la tecnología, pero también se ha convertido en un factor criminógeno que ha permitido la comisión de nuevas modalidades de delitos, los cuales dependiendo de la legislación podrían no encontrarse tipificados, lo cual es una problema al momento de su persecución, desde la perspectiva del principio de legalidad.*

Abg. Ivan Manjarres Bolaño (Colombia): *Pareciera que van al mismo ritmo, sobre todo en lo que concierne al robo de datos.*

Las diferentes entidades, sean de comercio o de servicios, en su afán de captar más usuarios, incitan en un momento dado, a que las personas para hacer uso de estos ofrecimientos, exponen sus datos personales, exponiéndolos con esto a que sean víctimas potenciales para la comisión de este tipo de delitos.

Dr. Andrés Álvarez Pérez (España): *Hoy en día, el avance de las tecnologías y el fácil uso de las mismas, han proporcionado herramientas a los delincuentes, con los que cometer delitos más sofisticados y mucho más difícil de identificar.*

Ing. Gaston Miguel Semprini (Argentina): *Creo que la el avance tecnológico va de la mano de los distintos delitos cometidos con dispositivos tecnológicos. Pero más allá de eso, considero que es necesario que los organismos de investigación especializados, cuenten con personal capacitado y formado para llevar adelante esas investigaciones y así obtener resultados favorables en la investigación.*

Mg. Daniel Peña Labrin (Perú): *La tecnología, no solo ha traído la mejora de la calidad de vida de la población global, sino también las actividades delictivas se han modernizado en su actuar delincuencial mejorando obstenciblemente su performance criminal.*

Dr. Gustavo Adolfo Silva Huamán (Perú): Que el aumento de Ia criminalidad en el ámbito de tecnologías informáticas obedece al propio avance de la criminalidad en nuestro País, atendiendo a que dicho fen6meno no solo se encuentra relacionado con este tipo de delitos sino con la delincuencia en general, que al no ser contrarrestadas oportunamente por el Estado su incremento crece exponencialmente, mas aún si se tiene presente el creciente avance y permanente innovación del sector tecnológico.

2.- ¿Considera usted que la legislación sobre delitos informáticos es eficiente para sancionar las nuevas formas delictivas con el uso de las tecnologías informáticas? ¿Por qué?

Dr. Santiago Martín Acurio Del Pino (Ecuador): *En el Ecuador con la expedición del Código Orgánico Integral Penal, se amplió el espectro de los delitos informáticos, mejorando la redacción y ampliando tipos que no existían contemplados antes en el Código Penal anterior, eso fue un avance en la legislación.*

Abg. Ivan Manjarres Bolaño (Colombia): *La intangibilidad de estos delitos hacen parecer o dan la sensación, en un momento dado, que la legislación existente no es capaz de enmarcar estos delitos y sancionarlos de una forma eficaz.*

Dr. Andrés Álvarez Pérez (España): *Cada día es más eficiente y efectiva la legislación referente a los Delitos Informáticos. En España se ha realizado un gran avance en legislar en referencia en esta clase de delitos, con la actualización del Código Penal en el año 2015, se dio un gran paso en este asunto.*

Ing. Gaston Miguel Semprini (Argentina): *No creo que sea eficiente nunca, porque siempre la tecnología y las nuevas formas delictivas, va más rápido*

que el derecho. Pero si considero que es necesario ir trabajando para mejorar la legislación y/o adherirse a distintos convenios internacionales para ir combatiendo dichos delitos.

Mg. Daniel Peña Labrin (Perú): *Aun falta no solo legislar sobre las nuevas actividades delictivas, sino también difundir y explicar la nueva criminalidad informática en su connotación holística.*

Dr. Gustavo Adolfo Silva Huamán (Perú): La legislación existente resulta insuficiente, toda vez que continuamente se renuevan las modalidades delictivas en el ámbito informatice, asimismo si se tiene presente que en nuestro país las herramientas existentes para contrarrestar dichos ilícitos no resultan ser suficientes, y que poco es el efecto disuasivo en la proliferación del mismo.

3.- ¿Considera usted adecuado comprender a la estafa, hurto y sabotaje informático dentro del *nomen iuris* "fraude informático"? ¿Por qué?

Dr. Santiago Martín Acurio Del Pino (Ecuador): *No me parece, los fraudes informáticos son específicos, pertenecen a las defraudaciones en genérico, es un delito de carácter patrimonial, pero diferente del hurto y sabotaje.*

Abg. Ivan Manjarres Bolaño (Colombia): *La comisión de estos delitos en lo que respecta a espacio, tiempo y forma, no da para que se les nomine de esta forma.*

Dr. Andrés Álvarez Pérez (España): *Si claro, El Modus Operandi actual de este tipo de delitos, está basado en el uso de las nuevas tecnologías, en especial, el uso de Internet, es por ello que el encajarlo en "Fraude Informático", es totalmente correcto.*

Ing. Gaston Miguel Semprini (Argentina): *Si por supuesto, siempre en todos los casos debiéndose demostrar con las distintas pericias que sean necesarias el fraude cometido.*

Mg. Daniel Peña Labrin (Perú): *Si, porque todo los delitos tienen un componente de dañosidad de engaño, de allí que esta circunscritos en el*

fraude informático, para que guarde relación con el convenio de Budapest, pero a mi punto de vista no es suficiente.

Dr. Gustavo Adolfo Silva Huamán (Perú): Al respecto el delito de fraude informatice se encuentra previsto y sancionado en el artículo 8 de la Ley N° 30096, que sanciona la alteración, supresión, borrado de datos informáticos o cualquier interferencia o manipulación en el funcionamiento de un sistema informático, por lo que en estricto se refiere a cualquier tipo de manipulación de datos o el funcionamiento de un sistema, por lo que la estafa, no corresponde ser comprendidas dentro del mismo, sin embargo respecto al sabotaje, se entiende que ello corresponde a la alteración en cualquier modalidad de datos en un sistema informático, por lo que puede entenderse dentro del mismo, empero respecto al hurto no existe un verbo rector que incluya dicha modalidad, lo cual más bien podría ser contemplada dentro del tipo penal Interceptación de Datos informáticos previsto en el artículo 7 de la citada ley.

Respecto al primer objetivo específico

Analizar el tratamiento jurídico penal de los delitos informáticos contra el patrimonio en su modalidad de hurto.

4.- ¿Considera usted que los bancos están dispuestos a denunciar penalmente delitos de hurto sistemáticos de cuentas bancarias y otros? ¿Por qué?

Dr. Santiago Martín Acurio Del Pino (Ecuador): *Bueno el hurto sistemático, hay que aclararlo, ya que por principio de legalidad en el Ecuador no existe el hurto informático, lo que existe es el Fraude Informático o puede ser Peculado Bancario, dependiendo de los hechos.*

En cuanto a si los Bancos denuncian esos tipos penales, hay que recordar que muchos de ellos quedan como cifra negra, debido a que podrían constituir un atentado a la imagen corporativa del Banco, y por ello en

muchos casos buscan solucionar esos problemas de forma interna. Sin acudir a la Administración de Justicia o a la Fiscalía General del Estado.

Abg. Ivan Manjarres Bolaño (Colombia): *Si lo deben hacer tanto por el bien de los clientes como el de su misma imagen, aunque en algunos casos tratan de minimizar el daño que les han causado para, precisamente, mantener su clientela.*

Dr. Andrés Álvarez Pérez (España): *Si, Por supuesto, mi experiencia en la investigación relacionadas con entidades bancarias, me ha proporcionado la evidencia de total colaboración y disposición, no solo a la denuncia de los mismos, si no a prestar total colaboración en las investigaciones que se llevan a cabo.*

Ing. Gaston Miguel Semprini (Argentina): *No, porque en realidad sería un desprestigio como institución y haría denotar que no cuenta con la seguridad necesaria, y haría perder la confianza de sus clientes o posibles nuevos clientes.*

Mg. Daniel Peña Labrin (Perú): *Solo cuando estos son significativos, ya que no lo hacen públicos con frecuencia, por el tema de no provocar "pánico financiero" y de eso se aprovecha la criminalidad informática.*

Dr. Gustavo Adolfo Silva Huamán (Perú): Considero que en la mayoría de casos no, por la imagen de su entidad, dado que ello pone en evidencia las falencias de su seguridad, y que también implica un resarcimiento econ6mico, de verificarse que la falla fue del sistema de la propia entidad, sin embargo en los casos que fuere por descuido y negligencia del propio cliente lo común es que lo pongan en conocimiento de los usuarios o la autoridad competente, pero ello es cuando existe una significativa cantidad de casos similares.

5.- Explique ¿En la legislación penal existe regulación específica del delito de hurto informático?

Dr. Santiago Martín Acurio Del Pino (Ecuador): *No existe en la legislación penal del Ecuador, doctrinalmente puede existir el hurto de servicios de telecomunicaciones.*

Abg. Ivan Manjarres Bolaño (Colombia): *Si. En nuestro código penal con la expedixción de la ley 1273 de 2009 alli se tipifica el delito de Hurto informático en el artículo 13.*

Dr. Andrés Álvarez Pérez (España): *Como tal no existe, pero está incluido en el artículo 248 del Código Penal Español, con el concepto "Fraudes Informáticos".*

Ing. Gaston Miguel Semprini (Argentina): *Contamos en la Argentina con la ley 26388 de delitos informáticos, pero no está especificado el hurto informático.*

Mg. Daniel Peña Labrin (Perú): *Existió en el artículo 186 del c.p., segundo párrafo numeral 3, modificado por la ley 26319, que disponía además "la pena será no menor de 4 años ni mayor de 8 años, "si el hurto es cometido mediante la utilización de sistemas de transferencia electrónica de fondos de la telemática en general o la violación del empleo de claves secretas", y fue derogado por la DCD única de la ley 30096, modificada por la ley 30171.*

Dr. Gustavo Adolfo Silva Huamán (Perú):

¿Qué opinión le merece la vigente regulación sobre la prevención y sanción del hurto informático?

Al respecto existe la Ley N° 30096, que sanciona la interceptación ilegitima de datos informáticos, el cual podría entenderse como hurto al apoderarse de datos de manera ilegal pertenecientes a un tercero, y que si bien de alguna manera se protege los datos informáticos, nuestra regulación resulta incipiente en este aspecto.

¿Considera usted que la ley de delitos informáticos cumple con el principio de tipicidad para sancionar el hurto informático? ¿Por qué?

Al resultar incipiente la regulación de los delitos informáticos, ello implica ciertas falencias tales como la tipificación, y que de acuerdo a nuestra

legislación el hurto informático como tal no se encuentra previsto, sino a través del apoderamiento de datos informáticos, o la manipulación, supresión, clonación de los mismos.

Respecto al segundo objetivo específico

Analizar el tratamiento jurídico penal de los delitos informáticos contra el patrimonio en su modalidad de fraude.

6.- ¿Considera usted que tanto las personas como las empresas están expuestos a ser víctimas de fraudes informáticos? ¿Por qué?

Dr. Santiago Martín Acurio Del Pino (Ecuador): *Los atacantes informáticos, buscan aprovechar la falta de conocimiento y previsión de las víctimas. Falta una cultura de Ciberseguridad que es aprovechada por los atacantes para cometer este tipo de delitos. En especial la llamada ingeniería social*.

Abg. Ivan Manjarres Bolaño (Colombia): *Totalmente. En esta época el uso masificado de los elementos para comunicación y la aparición de las llamadas redes sociales nos exponen a que nuestros datos personales estén expuestos para que de allí sean utilizados por este tipo de delincuentes para iniciar su accionar delictivo.*

Dr. Andrés Álvarez Pérez (España): *Por supuesto, En las ponencias que de vez en cuando hago, es un tema en la hago especial insistencia. Nunca se puede estar completamente seguro en este mundo en el que vivimos, siempre hay que estar en alerta y preparados ante cualquier fraude. El más común en estos últimos tiempos es el que se comete a través de "CRYPTOLOCKER", consistente en encriptar todos los archivos del disco duro y a continuación solicitar una elevada cantidad de dinero, para desencriptarlos.*

Ing. Gaston Miguel Semprini (Argentina): *Si y siempre lo estarán, porque la seguridad absoluta no existe, si se deben tomar todos los recaudos de seguridad pertinentes, pero siempre hay acciones delictivas nuevas que el*

usuario común o personal de empresas no está al tanto o capacitados, permitiendo accesos indebidos a datos valiosos personales o de la empresa por ejemplo los casos de Ramsomware.

Mg. Daniel Peña Labrin (Perú): *Si, por la naturaleza de sus actividades donde el factor económico es determinante para la delincuencia online.*

Dr. Gustavo Adolfo Silva Huamán (Perú): Todas las personas, naturales o jurídicas, son susceptibles de ser agraviados en este tipo de delitos, por cuantos ello implica el aprovechamiento a través de tecnologías en un sistema determinado, o los datos que se transfieren a través de medios tecnológicos.

¿Cree usted adecuado que la regulación de delitos informáticos contra el patrimonio se traduzca únicamente en fraude informático? ¿Por qué?

Considero que es el punto de partida para el desarrollo de una legislación contra este tipo de delitos, puesto que resulta insuficiente un solo tipo penal para dicha tipificación, pero ello ya es un avance, teniendo presente, que con anterioridad a la presente legislación especial, existía solo unos artículos dentro del Código Penal, y que debido al avance de la actividad criminal en este ámbito el legislador tuvo a bien la dación de la referida norma.

7.- ¿En la actualidad existen estrategias claras para la prevención y sanción de delitos de fraude informático? Si fuera afirmativa ¿Cuáles?

Dr. Santiago Martín Acurio Del Pino (Ecuador): *Para la sanción de los Fraudes existen las normas del Código Orgánico Integral Penal. En el campo de la prevención, falta la aplicación de normas como la ISO 27000 sobre la Seguridad de la Información por parte de las entidades públicas y privadas. Las instituciones financieras deben emprender campañas de información sobre las modalidades de fraudes informáticos, tales como el pishing o el pharming a fin de que los usuarios de la banca virtual no sean perjudicados. Al igual sobre las tarjetas de crédito y débito que pueden ser clonadas fácilmente y así perjudicar a sus tenedores.*

Abg. Ivan Manjarres Bolaño (Colombia): *Si, sobre todo en las entidades bancarias y en las dependencias del gobierno, el tratamiento de y uso de los datos personales están protejidos por ley.*

Dr. Andrés Álvarez Pérez (España): *Si, efectivamente, en España existe claras estrategias para la lucha y prevención de este tipo de fraudes, entre otras el refuerzo en las leyes que tratan de estos temas, como también una campaña de información para detectar estos delitos y saber actuar ante ellos.*

Ing. Gaston Miguel Semprini (Argentina): *Creo que el convenio de Budapest lo considera.*

Mg. Daniel Peña Labrin (Perú): *No las hay, el estado no formula una cultura de prevención de criminalidad informática. En Argentina, el estado tiene un protocolo de grooming que lo difunde a la sociedad igualmente en chile, aca no existe nada parecido, tampoco existe el delito de sexting (muy comun en la posmodenidad).*

Dr. Gustavo Adolfo Silva Huamán (Perú): Tengo entendido que a través de la SBS se realizan campanas de información a las personas respecto a las actividades delictivas en entidades financieras, y que por intermedio de la Policía Nacional del Perú también se informa preventivamente sobre diversos ilícitos en este área, sin embargo, resulta insuficiente, puesto que at igual que los delitos de Lavado de Activos o Trafico de Drogas es necesario una política criminal especifica.

Respecto al tercer objetivo específico

Analizar el tratamiento jurídico penal de los delitos informáticos contra el patrimonio en su modalidad de estafa.

8.- ¿Le genera confianza las plataformas informáticas para realizar compras y contratar servicios a través de internet? ¿Por qué?

Dr. Santiago Martín Acurio Del Pino (Ecuador): *Todo depende de la plataforma, si esta cumple con los estándares como:*

- ***ISO 27001:2013:*** *Buenas prácticas para el manejo de sistemas de información y proceso de datos.*
- ***PCI DSS:*** *Transacciones y pagos con tarjetas de crédito.*
- ***OWASP ASVS:*** *Seguridad de aplicaciones web*

Si el sitio o página web tiene estas seguridades se puede realizar transacciones seguras.

Abg. Ivan Manjarres Bolaño (Colombia): *Personalmente no realizó ningún tipo de compras por internet. Tramites si, donde este seguro que la información suministrada va a tener un tratamiento adecuado.*

Dr. Andrés Álvarez Pérez (España): *Soy una persona que compra a menudo por Internet, y me generan mucha confianza, claro está, que siempre realizo estas comprar en plataformas de compañías de confianza y de renombre. Los problemas pueden surgir, cuando se realizan en páginas web extranjeras que no tienen los certificados de seguridad mínimos, ni con un nombre conocido.*

Ing. Gaston Miguel Semprini (Argentina): *Sí, siempre tomando las precauciones pertinentes.*

Mg. Daniel Peña Labrin (Perú): No genera confianza, y principalmente por la brecha digital, el Perú tiene el porcentaje más bajo de comercio electrónico en la Región.

Dr. Gustavo Adolfo Silva Huamán (Perú): Al respecto existen ciertas medidas de seguridad a seguir, tales como la fiabilidad de las páginas web de compra, y seguir las políticas de seguridad de dichas entidades.

¿Considera usted que la ley de delitos informáticos cumple con el principio de tipicidad para sancionar la estafa informática? ¿Por qué?

Si, dado que las modalidades más frecuentes se encuentran tipificadas, sin embargo aún es insuficiente dado la creciente actividad criminal en dicho ámbito.

9.- Explique ¿En la legislación penal existe regulación específica del delito de estafa informática?

Dr. Santiago Martín Acurio Del Pino (Ecuador): *La estafa informática es básicamente un delito computacional, más no informático. Es decir que para lograr el engaño del sujeto pasivo se lo hace a través por ejemplo de un anuncio en la página web, donde se vende un producto a menor precio que el que se puede conseguir en una tienda, por ejemplo un reloj ROLEX en USD. 1.000 dólares. El sujeto pasivo ve ese anuncio, se contacta con el sujeto activo, quien le dice que debe hacer una transferencia a una cuenta, o a través de Western Union o Money Gram, luego el sujeto activo, recibe la transferencia y envía el paquete al sujeto pasivo, quien al recibirlo encuentra una foto del ROLEX, por tanto se da cuenta que ha sido estafado, siendo medio fraudulento el engaño o abuso de confianza que generó el error sicológico en el sujeto pasivo que le llevo a la disposición patrimonial lesiva.*

Abg. Ivan Manjarres Bolaño (Colombia): Si está regulado. (ver Ley 1273 de 2009 Colombia)

Dr. Andrés Álvarez Pérez (España): *En nuestra legislación, en concreto en el artículo 248 del Código Penal, referente a La Estafa, aunque no se especifica la estafa informática, el desarrollo de dicho artículo, es de gran utilidad para poder tratar estos delitos.*

Ing. Gaston Miguel Semprini (Argentina): *Desconozco.*

Mg. Daniel Peña Labrin (Perú): *En el Perú no se sancionan correctamente los delitos informáticos como la estafa informática: solo el acceso ilícito; atentados contra la integridad de datos; delitos contra la indemnidad sexual; delitos contra la intimidad y secreto de las comunicaciones y contra la fe pública. (copia del convenio de budapest).*

Dr. Gustavo Adolfo Silva Huamán (Perú):

Respecto al cuarto objetivo específico

Analizar el tratamiento jurídico penal de los delitos informáticos contra el patrimonio en su modalidad de sabotaje informático.

10.- ¿Considera usted que cuando un pirata informático destruye información y *softwares* en la red afecta el patrimonio de la víctima? ¿Por qué?

Dr. Santiago Martín Acurio Del Pino (Ecuador): *Depende de la información, si esa información está en la nube o almacenada en un dispositivo de almacenamiento. Ya que esta puede tener respaldo. También depende del tipo de información que ha sido destruida, ya que ahora la información puede tener una valor económico para la víctima y eso puede causarle un perjuicio patrimonial, pero como esta clase de delitos son de tipo pluriofensivo también puede afectar a la disponibilidad de la información y a su integridad.*

Abg. Ivan Manjarres Bolaño (Colombia): *Si claro sobre todo el llamado patrimonio intelectual porque la victima ha dedicado tiempo, estudio e investigación en la elaboración de estos.*

Dr. Andrés Álvarez Pérez (España): *En muchos casos, si, efectivamente, a nivel particular, muchas personas que han sufrido algún caso de destrucción de información, han tenido que recurrir a empresas externas, que se dedican a recuperar datos perdidos, con el consecuente gasto monetario. A nivel de empresas, la destrucción de datos, aparte del gasto en su recuperación, también esta el descredito ante sus clientes, los cuales pueden optar por cambiar de empresa.*

Ing. Gaston Miguel Semprini (Argentina): *Si porque esa información y/o datos que se encuentran dentro de un software o sistema es información personal, es por ello que la ley 26388 prevé condenas para esos casos.*

Mg. Daniel Peña Labrin (Perú): Si ya que el patrimonio de la víctima no solo es material sino también inmaterial, en esta posmodernidad de la dictadura de la NTICS.

Dr. Gustavo Adolfo Silva Huamán (Perú): Si, dado que resulta un bien no tangible de la víctima, más aún, si la misma puede ser susceptible para la obtención de bien económico, tales como códigos de seguridad que permitan el acceso cuentas bancarias u otros.

¿Considera usted que la ley de delitos informáticos cumple con el principio de tipicidad para sancionar el sabotaje informático? ¿Por qué?

Lo que se tipifica es la manipulación de datos en diversas modalidades, lo cual se traduce en la alteración de los datos informáticos, por lo que si bien es cierto se señala cuáles son los hechos sancionados, estos aún resultan insuficientes para todas las modalidades existentes.

11.- Explique ¿En la legislación penal existe regulación específica del delito de sabotaje informático?

Dr. Santiago Martín Acurio Del Pino (Ecuador): *En el caso ecuatoriano existe el delito de daños informáticos. Art. 232 COIP.*

Abg. Ivan Manjarres Bolaño (Colombia): *Si existe este tipo penal (ver Ley 1273 de 2009).*

Dr. Andrés Álvarez Pérez (España): *En el Código Penal Español, como tal, no está reflejado, pero concretamente en el Artículo 264, viene especificado como Daños Informáticos y en cual, entra ese delito.*

Ing. Gaston Miguel Semprini (Argentina): *Desconozco*

Mg. Daniel Peña Labrin (Perú): Estuvo en el artículo 207-b del Código Penal, y ahora en la Ley 30096 y modificada por la ley 30171, en el artículo 3: atentado contra la integridad de datos informáticos.

Dr. Gustavo Adolfo Silva Huamán (Perú):

12.- ¿Considera usted que la vigente regulación contribuye con la efectiva prevención de los delitos informáticos contra el patrimonio? ¿Por qué?

Dr. Santiago Martín Acurio Del Pino (Ecuador): *En la legislación ecuatoriana están comprendidas viarias modalidades de fraudes informáticos que permite su persecución, la única limitante puede ser que al ser delitos de tipo transnacional las evidencias o pruebas estén en otra jurisdicción, por ello la necesidad se suscribir el Convenio del Cibercrimen de la Comunidad Europea que permitiría una mejor cooperación internacional en el caso de los delitos informáticos y cibernéticos.*

Abg. Ivan Manjarres Bolaño (Colombia): *La regulación por sí sola no contribuye con la prevención de estos delitos. Se necesitan campañas educativas eficaces que alerten a las personas cuando utilicen cualquier medio informático del riesgo de ser víctima de estos delitos y la forma de evitarlos.*

Dr. Andrés Álvarez Pérez (España): *Las leyes Españolas, previenen los delitos informáticos contra el patrimonio, existe una extensa jurisprudencia al respecto. Pero si es verdad, que debería ser más concreta y una legislación Global, ya que en el momento que esos delitos, provienen de fuera de nuestras fronteras, la investigación se hace más difícil.*

Ing. Gaston Miguel Semprini (Argentina): *Desconozco.*

Mg. Daniel Peña Labrin (Perú): No completamente, se tiene que incluir: la estafa informática de manera indubitable, asimismo, la usurpación de identidad (la suplantacion no basta).

Dr. Gustavo Adolfo Silva Huamán (Perú): Es insuficiente, dado que solo se prevee un solo tipo penal contra el patrimonio.

13.- ¿Considera usted necesario una reforma legislativa para prevenir y sancionar los delitos informáticos contra el patrimonio? ¿Por qué?

Dr. Santiago Martín Acurio Del Pino (Ecuador): *En el caso ecuatoriano no es necesario, con el actual COIP*

Abg. Ivan Manjarres Bolaño (Colombia): *La legislación debe ir a la par de los diferentes cambios tecnológicos y sobre todo en lo que respecta a la seguridad cuando se manejan datos personales o corporativos.*

Dr. Andrés Álvarez Pérez (España): *Considero, que siempre es necesario mejorar las leyes y reformarlas, los delincuentes siempre están actualizando sus métodos y procedimientos para la realización de delitos, es por ello, que la reforma legislativa para la lucha del Delito Informático, y no solo, el referente al Patrimonio, si no, a todos lo que abarcan este tipo de Delitos Informáticos.*

Ing. Gaston Miguel Semprini (Argentina): Desconozco.

Mg. Daniel Peña Labrin (Perú): Si para perfeccionar los delitos informáticos contra el patrimonio de manera específica: estafa informática y usurpación de identidad.

Dr. Gustavo Adolfo Silva Huamán (Perú): Considero que debe extenderse los tipos penales en esta ley especial.

14.- ¿Tiene usted alguna opinión adicional sobre la presente investigación? Si fuera afirmativa ¿Cuál?

Dr. Santiago Martín Acurio Del Pino (Ecuador): *Debe haber claridad terminológica en el tema de los delitos informáticos en especial sobre los fraudes informáticos desde el punto de vista de la tipicidad objetiva.*

Abg. Ivan Manjarres Bolaño (Colombia): *Este tipo de investigación contribuye a que se tenga una mayor y mejor información sobre los delitos informáticos y su legislación lo cual sirve para prevenir a las personas que la consultan, ser víctima de este tipo de delitos*.

Dr. Andrés Álvarez Pérez (España): *Este tipo de asuntos, son desgraciadamente muy desconocidos por la población en general, y es interesante que se dé información al respecto, para no caer en esta clase de delitos.*

Ing. Gaston Miguel Semprini (Argentina): No

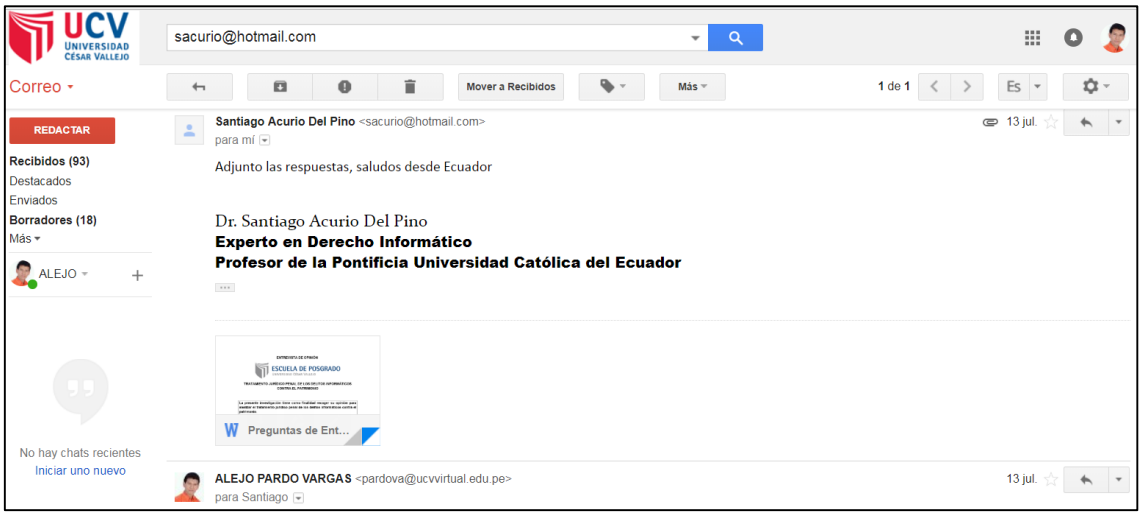
Mg. Daniel Peña Labrin (Perú): *Si entre muchas, que se proponga al Congreso de la República por parte de las instituciones con iniciativa legislativa y la sociedad civil, la adhesión del Perú al convenio de Budapest.*

En América solo lo han ratificado: USA, Canadá, Panamá, República Dominicana y el 2017 Chile, el no existir una legislación uniforme en delitos informáticos genera dualidad de delitos y problemas de interpretación dogmática, y además, la migración de la delincuencia on line a esta parte del planeta ya que la criminalidad informática, sabe que la legislaciones diferentes en cada país latinoamericano son una ventaja para que estas nuevas conductas delictivas sigan cubiertas bajo el manto de la impunidad.

Dr. Gustavo Adolfo Silva Huamán (Perú): Que para la resolución de estos tipos de delitos, es necesario el apoyo técnico del área encargada, esto es, la División de Delitos Informáticos de la PNP la cual no se abastece debido a la carga delictiva, más aun si se encuentra centralizada en la DIRINCRI en Lima, y que tampoco cuenta con todas las herramientas necesarias para encontrarse a la par con la delincuencia que se innova a diario.

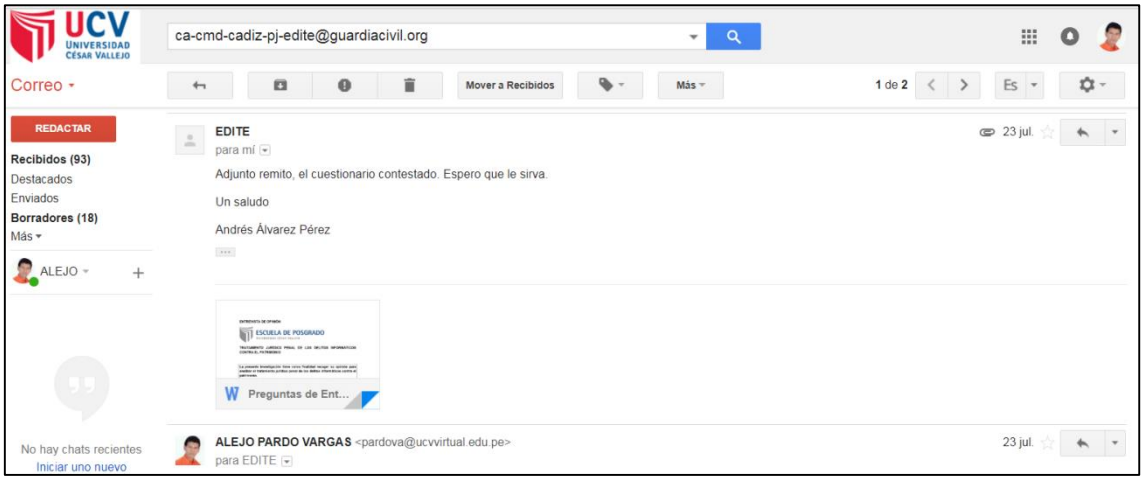
Anexo 8: Evidencias del trabajo de campo

Dr. Santiago Martín Acurio Del Pino (Ecuador)

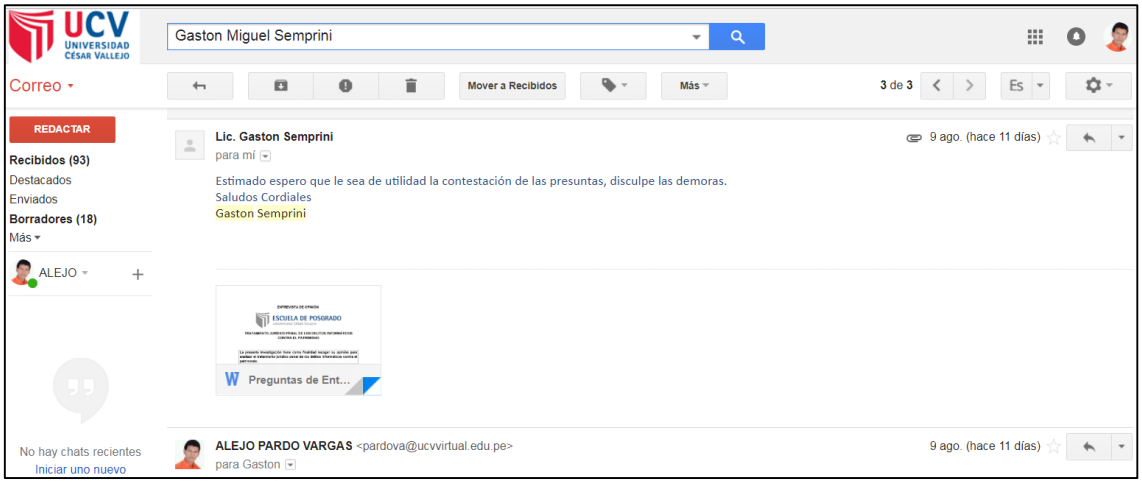


Abg. Ivan Manjarres Bolaño (Colombia)

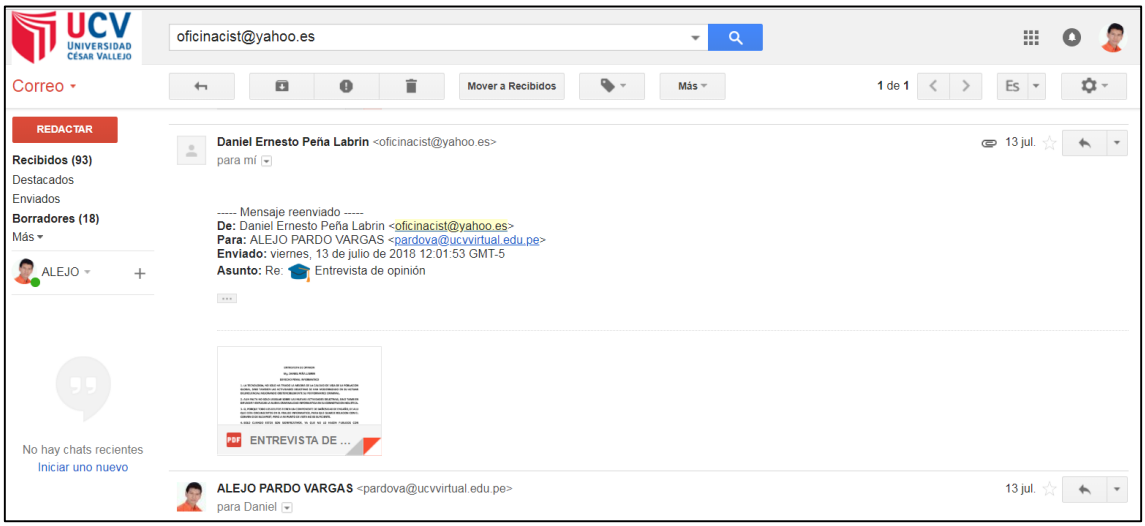
Dr. Andrés Álvarez Pérez (España)



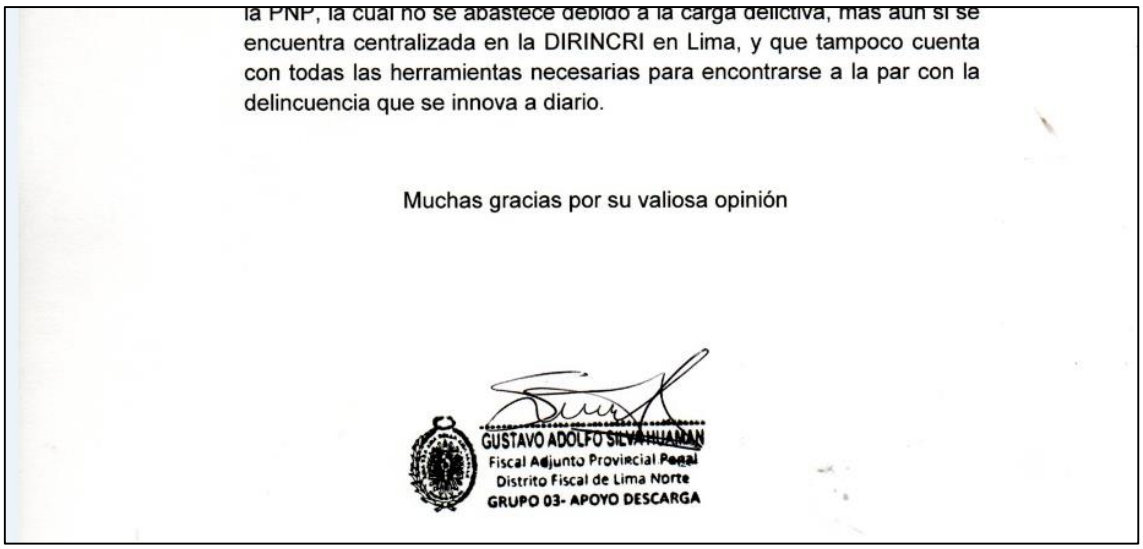
Ing. Gaston Miguel Semprini (Argentina)



Mg. Daniel Peña Labrin (Perú)



Dr. Gustavo Adolfo Silva Huamán (Perú)


la PNP, la cual no se abastece debido a la carga delictiva, más aún si se encuentra centralizada en la DIRINCRI en Lima, y que tampoco cuenta con todas las herramientas necesarias para encontrarse a la par con la delincuencia que se innova a diario.

Muchas gracias por su valiosa opinión

GUSTAVO ADOLFO SILVA HUAMAN
Fiscal Adjunto Provincial Penal
Distrito Fiscal de Lima Norte
GRUPO 03- APOYO DESCARGA

ESCUELA DE POSGRADO
UNIVERSIDAD CÉSAR VALLEJO

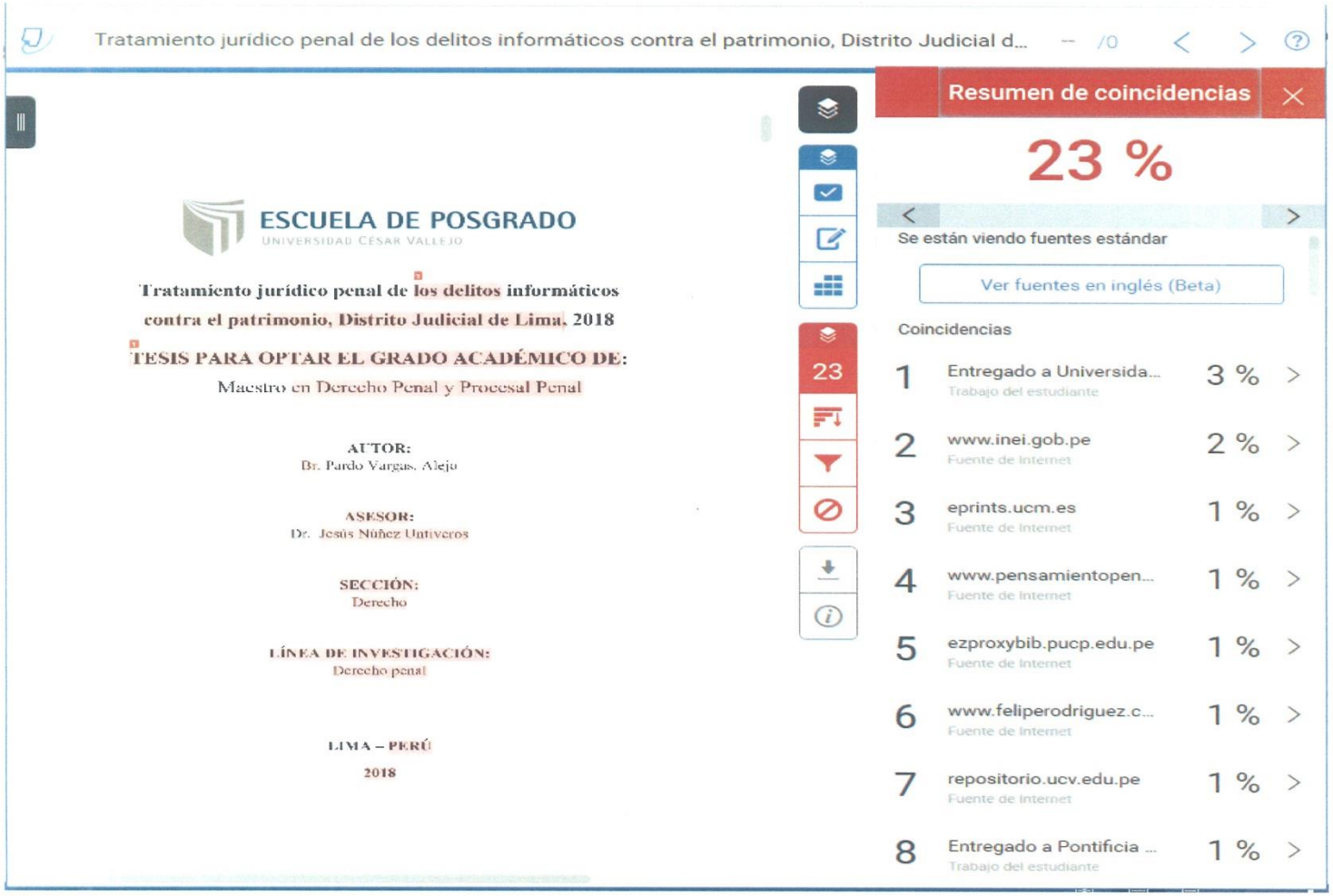
Acta de Aprobación de originalidad de Tesis

Yo, Angel Salvatierra Melgar, docente de la Escuela de Posgrado de la Universidad César Vallejo filial Lima Norte, revisor de la tesis titulada "**Tratamiento jurídico penal de los delitos informáticos contra el patrimonio, Distrito Judicial de Lima, 2018**" del (de la) estudiante **Alejo Pardo Vargas**, constato que la investigación tiene un índice de similitud de **23**% verificable en el reporte de originalidad del programa Turnitin.

El/la suscrito(a) analizo dicho reporte y concluyo que cada una de las coincidencias detectadas no constituye plagio. A mi leal saber y entender la tesis cumple con todas las normas para el uso de citas y referencias establecidas por la Universidad César Vallejo.

Lima, 18 de agosto del 2018

Angel Salvatierra Melgar
DNI: 19873533


Tratamiento jurídico penal de los delitos informáticos contra el patrimonio, Distrito Judicial d...
/0
ESCUELA DE POSGRADO
UNIVERSIDAD CÉSAR VALLEJO
Tratamiento jurídico penal de los delitos informáticos contra el patrimonio, Distrito Judicial de Lima, 2018
TESIS PARA OPTAR EL GRADO ACADÉMICO DE:
Maestro en Derecho Penal y Procesal Penal
AUTOR:
Br. Pardo Vargas, Alejo
ASESOR:
Dr. Jesús Núñez Untiveros
SECCIÓN:
Derecho
LÍNEA DE INVESTIGACIÓN:
Derecho penal
LIMA – PERÚ
2018
23
Resumen de coincidencias
23 %
Se están viendo fuentes estándar
Ver fuentes en inglés (Beta)
Coincidencias
1 Entregado a Universida... 3 %
Trabajo del estudiante
2 www.inei.gob.pe 2 %
Fuente de Internet
3 eprints.ucm.es 1 %
Fuente de Internet
4 www.pensamientopen... 1 %
Fuente de Internet
5 ezproxybib.pucp.edu.pe 1 %
Fuente de Internet
6 www.feliperodriguez.c... 1 %
Fuente de Internet
7 repositorio.ucv.edu.pe 1 %
Fuente de Internet
8 Entregado a Pontificia ... 1 %
Trabajo del estudiante

UNIVERSIDAD CÉSAR VALLEJO

Centro de Recursos para el Aprendizaje y la Investigación (CRAI)
"César Acuña Peralta"

FORMULARIO DE AUTORIZACIÓN PARA LA PUBLICACIÓN ELECTRÓNICA DE LAS TESIS

1. **DATOS PERSONALES**
Apellidos y Nombres: (solo los datos del que autoriza)
Pardo Vargas Alejo
D.N.I. : 70197606
Domicilio : Urb. San Diego Mz. G1 Lote 22 San Martín de Porres
Teléfono : Fijo : ..... Móvil : 980429676
E-mail : pardomundo.18@gmail.com

2. **IDENTIFICACIÓN DE LA TESIS**
Modalidad:
☐ Tesis de Pregrado
Facultad : .....
Escuela : .....
Carrera : .....
Título : .....

☐ Tesis de Posgrado
☒ Maestría ☐ Doctorado
Grado : Maestro
Mención : Derecho Penal y Procesal Penal

3. **DATOS DE LA TESIS**
Autor (es) Apellidos y Nombres:
Pardo Vargas Alejo

Título de la tesis:
Tratamiento Jurídico Penal De Los Delitos Informáticos Contra El Patrimonio, Distrito Judicial De Lima, 2018

Año de publicación : 2018

4. **AUTORIZACIÓN DE PUBLICACIÓN DE LA TESIS EN VERSIÓN ELECTRÓNICA:**
A través del presente documento,
Si autorizo a publicar en texto completo mi tesis. ☒
No autorizo a publicar en texto completo mi tesis. ☐

Firma : ..... Fecha : 24/09/18

UNIVERSIDAD CÉSAR VALLEJO

AUTORIZACIÓN DE LA VERSIÓN FINAL DEL TRABAJO DE INVESTIGACIÓN

CONSTE POR EL PRESENTE EL VISTO BUENO QUE OTORGA EL ENCARGADO DE INVESTIGACIÓN DE

ESCUECA DE POSGRADO

A LA VERSIÓN FINAL DEL TRABAJO DE INVESTIGACIÓN QUE PRESENTA:

PARDO JARGAS ALEJO

INFORME TÍTULADO:

TRATAMIENTO JURÍDICO PENAL DE LOS DELITOS INFORMÁTICOS CONTRA EL PATRIMONIO; DISTRITO JUDICIAL DE LIMA; 2018

PARA OBTENER EL TÍTULO O GRADO DE:

MAESTRO EN DERECHO PENAL Y PROCESAL PENAL

SUSTENTADO EN FECHA: 28 DE AGOSTO DE 2018

NOTA O MENCIÓN: APROBADO POR UNANIMIDAD

ESCUELA DE POSGRADO UCV INVESTIGACIÓN CAMPUS LIMA NORTE

FIRMA DEL ENCARGADO DE INVESTIGACIÓN