UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POSGRADO

PROGRAMA ACADÉMICO DE MAESTRÍA EN DERECHO PENAL Y PROCESAL PENAL

Implicancias Jurídicas del Fraude Informático y la Protección Penal del Delito Contra el Patrimonio Distrito Fiscal de Lima Norte 2020

TESIS PARA OBTENER EL GRADO ACADÉMICO DE:

Maestro en Derecho Penal y Procesal Penal

AUTOR:

Condori Ccori, Rufino (ORCID: 0000-0001-9364-6502)

ASESOR:

Mg. Núñez Untiveros, Jesús Enrique (ORCID: 0000-0001-9069-4496)

LÍNEA DE INVESTIGACIÓN:

Derecho Penal

LIMA- PERÚ

2020

Dedicatoria:

A Dios, porque, me ha iluminado y guiado para seguir avanzando adelante con esfuerzo y dedicación, a mi adorada madre Agripina Ccori Ramos y en memoria de mi padre Ramón Condori Salazar, quienes me han inspirado para lograr este capítulo de mi vida y, a toda mi familia. Quienes han sido parte de este logro porque, me apoyaron en todo momento y espero que mi sobrino Angel Diego, Jhon Felipe y otros sigan mis pasos.

Agradecimiento:

A mi asesor Núñez Untiveros, Jesús Enrique quien me ha guiado con sus conocimientos de vasto experiencia académica y paciencia, asimismo a mi hermana Isidora Condori Ccori, Rogelio Depaz Valderrama y a las personas que me apoyaron de manera incondicional para lograr el desarrollo de la presente tesis.

Índice de contenidos

Índice de tablas

Índice de figuras

Resumen

La presente investigación tiene como objetivo determinar cuáles son las implicancias jurídicas del fraude informático y la protección penal del delito contra el patrimonio Distrito Fiscal de Lima Norte 2020. El tema del fraude electrónico y el delito contra la propiedad. En la actualidad, avanza a la par con la tecnología solo se podrá evitar y la informática es uno de los instrumentos más utilizados en las actividades diarias que realizan las personas que nos permiten interactuar a través de la plataforma virtual, del sistema informático. No obstante, este instrumento lo están usando para delinquir, teniendo como consecuencia a la afectación de los bienes patrimoniales de la propiedad privada y del propio Estado, esta situación como bien es sabido ha originado que los países adopten mecanismos legales a efectos de regular este tipo de conductas, a fin de frenar su avance con los mecanismos legales necesarias a fin de combatir este flagelo.

Así tenemos que en el primer capítulo, desarrollamos la problemática desde un enfoque descriptivo, luego fue evolucionando durante todo el proceso de investigación, así también en el segundo capítulo consideramos tanto los antecedentes nacionales e internacionales, seguido del marco teórico que permite fundamentar el estudio de la presente investigación, como tercer capítulo y desarrollamos la parte metodológica, en el cuarto capítulo se ha considerado los resultados, en el quinto capítulo se pasó a desarrollar la discusión de los resultados, mientras que en el sexto capítulo las conclusiones, para concluir el séptimo capítulo con las recomendaciones respectivas de la presente tesis.

Palabras clave: Fraude informático, delito contra la propiedad, sistema informático.

Abstract

The objective of this investigation is to determine what are the legal implications of computer fraud and the criminal protection of the crime against property. Fiscal District of Lima Norte 2020. The issue of electronic fraud and crime against property. At present, it advances in line with technology, it can only be avoided and computing is one of the most used instruments in the daily activities carried out by people that allow us to interact through the virtual platform, the computer system. However, this instrument is being used to commit a crime, having as a consequence the affectation of the patrimonial assets of private property and of the State itself, this situation, as is well known, has led countries to adopt legal mechanisms in order to regulate this type of conducts, in order to stop its advance with the necessary legal mechanisms in order to combat this scourge.

Thus we have that in the first chapter, we develop the problem from a descriptive approach, then it evolved throughout the research process, thus also in the second chapter we consider both the national and international antecedents, followed by the theoretical framework that allows to base the study of In the present investigation, as the third chapter and we develop the methodological part, in the fourth chapter the results have been considered, in the fifth chapter we went on to develop the discussion of the results, while in the sixth chapter the conclusions, to conclude the seventh chapter with the respective recommendations of this thesis.

Key words: Computer fraud, property crime, computer system

I.- INTRODUCCIÓN

En la actualidad, el constante avance de la tecnología informática es uno de los instrumentos más utilizados en las actividades cotidianas que realizan las personas para interactuar a través de la plataforma de internet por su versatilidad y automatización; sin embargo, esta herramienta viene siendo aplicado de forma incorrecta debido al incremento de las conductas delictivas por medio de las redes informáticas teniendo como consecuencia la afectación de los derechos patrimoniales de la propiedad privada y del Estado. Esta situación ha motivado que los países de cada estado adopten instrumentos legales a efectos de regular este tipo de conductas, nuestro país no es ajeno a esta problemática ya que en los últimos años se han reportado muchos casos como actos delictivos cometidos por medios informáticos, siendo los más frecuentes bajo la modalidad de fraude informático lo cual constituye el protagonismo de la ciberdelincuencia por hechos ilícitos relacionados a las transferencias electrónicas indebidas de fondos debido, al impacto económico y el auge del comercio electrónico que se viene incrementando considerablemente por los usuarios que optan en utilizar los medios informáticos por su versatilidad y la automatización.

Es por ello, que el fraude informático, transacciones ilegales y otras amenazas fueron los más frecuentes, al respecto en nuestra legislación se ha previsto en el artículo 8 de la Ley 30096 y su modificatoria conforme al artículo 01 de la Ley Nº 30171, publicada con fecha 10 de marzo del 2014, con la finalidad de proteger los derechos patrimoniales de las personas. El auge cibercriminal se presenta a la par con el avance de la tecnología informática con el aprovechamiento de la globalización de informaciones, no obstante, el Estado las empresas privadas, medios de comunicación y entidades financieras vienen promoviendo la utilización de los recursos digitales entre personas a través de plataformas informáticas que les permite acceder con mayor versatilidad y facilidad para interrelacionarse, comunicarse de manera instantánea, las tratativas de negocios nacionales e internacionales, transacciones económicas de acuerdo a sus necesidades e intereses a fin de optimizar la particularidad de vida de los ciudadanos.

Por otro lado, a pesar de los esfuerzos adoptados por el Estado y la empresa privada el uso de la tecnología informática ha tenido repercusiones negativas en nuestra sociedad, del cual algunos ciudadanos aprovechando de su conocimiento tecnológico han incursionado en la novedosa forma de delinquir a través de las redes informáticas del internet en los delitos contra el patrimonio como es el fraude informático de transacciones ilegales en beneficio propio de los ciberdelincuentes teniendo como consecuencia la afectación de los derechos patrimoniales de las personas, debido a su desconocimiento en el uso de los programas software y de las técnicas informáticas de funcionamiento para la mayoría de los usuarios.

Como consecuencia de los delitos informáticos contra el patrimonio se trae a colación el estudio previo que ha realizado el Ministerio Público, elaborado por la Oficina de Racionalización y Estadística – ORACE dentro del periodo enero a noviembre del dos mil dieciocho, fueron registrados la cantidad de 3,851 delitos sin embargo en el periodo enero a noviembre del año dos mil diecinueve, con un registro de 6,906 hechos delictuosos bajo la modalidad de delitos informáticos, cantidad que incrementa en un 79.33% al periodo anterior, asimismo se advierte según informe estadístico con mayor incidencia se presenta en los delitos informáticos contra el patrimonio con un 38.24% las mismas han sido registrados en Fiscalías Provinciales Penales y Mixtas, aunado a ello cabe mencionar la estadística de las denuncias reportadas por el INEI sobre el delito contra el patrimonio en la modalidad de Estafas y otras defraudaciones según el informe técnico de noviembre 2018 – abril 2019 asciende a 1611 casos.

Asimismo, en nuestra legislación en su tratamiento Dogmático jurídico penal a avanzado muy poco, por ello su importancia radica en la necesidad de hacer modificaciones de la normativa en la defensa de los derechos patrimoniales de las personas, teniendo en consideración el perfil del delincuente informático, en aras de garantizar la seguridad jurídica y con la finalidad de convivir en bienestar, la tranquilidad y la paz social que merecen todos los ciudadanos dentro de un estado de derecho. En consecuencia la problemática que existe en nuestro ordenamiento jurídico respecto, al fraude informático, se debe porque, no cubre de manera amplia los ámbitos en los que se comete este tipo de delitos teniendo en cuenta que la

comisión delictiva se fundamenta sobre la base los elementos fácticos, normativos y probatorios siendo ello así, si estamos frente a un evento delictivo cometido fuera de nuestro del país vale decir, la aplicación espacial y temporal frente a ello, existe el vacío normativo en los delitos informáticos específicamente en la modalidad de fraude informático que nos ocupa en el presente estudio de investigación, debido a que las transacciones informáticas de movimiento económico se pueden realizar en cualquier lugar del mundo solo basta contar con el dispositivo electrónico de computador y estar conectado a una red de plataforma virtual lo cual, se hace mucho más complejo su tratamiento normativo sobre los presupuestos fácticos más comunes, y su configuración delictiva, en la actualidad ¿cómo enfrenta el Ministerio Público del Distrito Fiscal de Lima Norte sobre este tipo de delitos? Teniendo en consideración las denuncias de víctimas del fraude informático, al respecto es importante resaltar que la mayor parte de las denuncias no prosperan durante la investigación fiscal.

El Ministerio Público, en muchos casos de investigación no logran identificar al presunto autor de la conducta incriminatoria, tampoco se logra establecer el lugar y el tiempo donde y cuando se han perpetrado los hechos, teniendo como consecuencia no ha lugar para continuar con la investigación preparatoria archivándose la misma finalmente queda impune la denuncia, sobre el particular, mediante la presente investigación nos permitirá determinar ¿cuáles son las implicancias jurídicas del fraude informático y la protección penal del delito contra el patrimonio?, para finalmente llegar a una conclusión y efectuar las recomendaciones que debe tomarse en cuenta a fin de contribuir para dar la solución a este problema de investigación.

La presente investigación cualitativa tiene como finalidad proponer el mecanismo normativo que permita orientar sobre los alcances y su tratamiento jurídico penal para su aplicación práctica y teórica en las investigaciones del delito de fraude informático que se tramitan por parte del Ministerio Público, frente a los hechos que afectan los derechos patrimoniales de los ciudadanos que han sido víctimas en distrito de Lima Norte.

Por lo abordado, precedentemente en el presente estudio se formuló como planteamiento general: ¿cuáles son las implicancias jurídicas del fraude informático y la protección penal del delito contra el patrimonio Distrito fiscal de Lima Norte 2020?, seguido de tres interrogantes específicos: i) ¿De qué manera repercute el fraude informático en la protección penal del delito contra el patrimonio Distrito fiscal de Lima Norte 2020?; ii) ¿Cómo se relaciona el fraude informático en el delito contra el patrimonio Distrito Fiscal de Lima Norte 2020? y iii) ¿De qué manera afecta el fraude informático en el derecho patrimonial del agraviado Distrito fiscal de Lima Norte 2020?.

En este sentido, la investigación se justifica convenientemente porque contribuye a los alcances que debe tener la norma jurídica respecto a las deficiencias de su aplicación espacial y temporal en los delitos informáticos específicamente en la modalidad de fraude informático sobre las transacciones informáticas de movimiento económico mediante dispositivos electrónicos en el fraude informático de los delitos patrimoniales con la finalidad de proteger el patrimonio de las personas. Asimismo, el estudio se justifica teóricamente porque, se aplica la recopilación de informaciones a través de múltiples fuentes e instrumentos normativos los cuales posibilita adquirir basta información sobre las dos clases.

En el presente, trabajo de investigación a fin de fundamentar las categorías y subcategorías, ha sido necesario tener en cuenta recurrir a los trabajos previos de carácter internacional y nacional, así como de distintas teorías o doctrinas relacionados al tema, aunado de los enfoques conceptuales. En este sentido como trabajos previos internacionales tenemos a Mayer y Oliver (2020) opinaron que existe la necesidad de regular el delito de fraude informático, acerca de tres exigencias copulativos esto es la comprobación de la gestión representativa consistente en operar antecedentes o programas de métodos de proceso computarizado de la información; el reto de un resultado y su disposición típica con el perjuicio patrimonial impropio y, la representación de lucro en el agente de su conducta incriminada, en esa misma línea, Utreras (2017) en su trabajo de investigación concluyó el fraude informático compone los elementos engaño y disposición patrimonial que se asemejan precisamente a la estafa, pues el arreglo

de estos injustos exige matices diferenciadores impidiendo promediarlos en cuanto a presupuestos típicos. Por lo tanto, la estafa y el fraude informático muestran una estructura parecida, sin embargo, las particularidades de ambos injustos los alejan diametralmente. En ese sentido, Mesa (2017) sostuvo que la cibercriminalidad, se encuentra en constante incremento evolucionando a un ritmo considerable el delito el fraude informático, no obstante la respuesta represiva del Estado Español frente a este fenómeno, interviene el Derecho Penal, adoptando las medidas de seguridad de información, que evite caer tan fácilmente en las técnicas de ingeniería informática aplicada por ciberdelincuentes a través de las redes sociales aportando los usuarios información que posteriormente puede ser empleado para actividades ilícitas.

En esa misma línea, Chungata (2015) manifestó que el delito del fraude informático se lo vincula con la estafa, ya que el objetivo del ciberdelincuente es beneficiarse económicamente, lo cual se efectúa por medio de la tecnología o sistemas informáticos, en procura de la satisfacción personal o a favor de un tercero, los fraudes más usuales son el phishing y pharming, que se lleva a cabo con la finalidad de extraer información confidencial del usuario por vías fraudulentas, a través de una página web falsa, con el objetivo de usar dicha información para obtener ganancias económicas, que favorecen al ciberdelincuente.

En ese sentido Acurio (2015) en su trabajo de investigación concluyó que el delito de fraude informático entiende cuatro modalidades, que vienen a ser los datos falsos o engañosos, manejo de programas o los caballos de troya, la técnica del salami, adulteración informática, maniobra de los datos de salida y por último el Fishing, las cuatro modalidades delictivas están encaminadas a un solo objetivo, el de burlar la seguridad informática, en la misma línea Gómez (2016) sostuvo que, la tipicidad del fraude informático conserva varios elementos para su configuración típica sustancial teniendo en cuenta que el esencia material en el que reincide la gestión puede ser cualquier cosa, con carácter de beneficio ilícito de modo tal que no restrinja la tipicidad a la apropiación de una “cosa mueble extraña adecuada del robo.

En ese orden de ideas, Cevallos et al. (2020) en su artículo científico señalaron que los delitos más comunes como fraudes son: La falsificación de la firma en instrumento y variación de caracteres magnéticos de tarjetas de crédito: clonación de tarjeta, robadas que no tienen ningún tipo de revelo o bloqueo, falsificación alteración de la banda magnética de la tarjeta, acrecentamiento fraudulento de porción, lavado de dinero mediante el uso de estas tarjetas, con el accionar dolosa del ciberdelincuente se cometen a diario por medios informáticos de forma online el robo de identidad, el phishing, el vishing y el smishing.

Por su parte, Alcívar B., y Calderón (2018) en su revista científica opinaron que los representantes del Ministerio Público que examinen los delitos informáticos deben capacitarse con procedimiento técnicos de averiguación, para preservar la cadena de custodia de la certeza digital, Identificación de IP internacionales a fin de presentar los elementos de convicción en las fases del proceso penal que corresponda, dado que los delitos informáticos se acrecientan a la par con el progreso tecnológico, formándose en un fenómeno progresivo muy compleja, en todo el mundo debido a la impericia de técnicas de investigación y la falta de coordinación interinstitucional del sector a cargo de las telecomunicaciones.

Por otro lado, Temitayo y Olaniyan (2018) en su revista científica en inglés señalaron que la magnitud de la pérdida derivada de los fraudes bancarios ha crecido como resultado del mal hábito para otorgar préstamos y descubiertos sin consentimiento y/o retiros fraudulentos de la cuenta de ahorros del cliente, lo cual tiene la consecuencia adversa de calmar la confianza de los depositantes, disminuyendo el depósito total de la entidad financiera. En esa misma línea, Kavipriya y Geetha (2018) en su revista científica en inglés concluyeron que en el transcurso de cotejo se utiliza la técnica del tipo de pronóstico de la clasificación SVM que revela e identifica con claridad y exactitud las transacciones fraudulentas y también sobre el avance el rendimiento de la afirmación. Lograr una alta cobertura de fraude concertada con una baja tasa de falsas alarmas. Es decir, da un menor número de falsos positivos en cotejo con el técnico existente. En general, el sistema logra sus propósitos y de esta manera puede esgrimirse para la procedencia, la manifestación y el reconocimiento automáticos de los servicios fraudulentos con tarjetas de crédito.

Asimismo, Habirovs A. (2018) en su trabajo de investigación en inglés manifestó que la población general del Reino Unido es acostumbrarse y sentirse más agradable con la Internet y el uso de la Internet entre la gente en el Reino Unido está desarrollando rápidamente. Sin embargo, la desconfianza al cibercriminal está también prosperando a medida que la gente confía en Internet con más de su información personal como la banca referencias en el caso de que se metan aplicaciones de banca móvil, o indagación personal. Sin embargo, las tasas de agraviados están reduciendo significativamente a lo largo de los años y el uso de medidas de prevención está acrecentando también,

Tobias (2018) en su trabajo de investigación en inglés concluyó que el adelanto perenne de las estrategias para implicar el fraude requiere un desarrollo incesante de esos sistemas, solo cuando los sistemas de descubrimiento de fraudes son capaces de resaltar incluso a la mayoría de los fraudes de los delincuentes transformadores pueden prevenirse con éxito. Para conseguirlo, se encomienda llevar a cabo más indagaciones en tres áreas principales que brotan de: primero, la diferenciación del medio contextual, indagando las diferencias de la prevención del fraude a través de varias formas del comercio.

Finalmente, You lu y Cynthia (2016) en su trabajo de investigación en inglés manifestaron que el delito informático, es un tipo de delito procedente últimamente con computadoras utilizadas por algunas personas a realizar diversos tipos de actos ilícitos, se ha transformado en uno de los problemas del mundo y ahora es el fondo de estudio más importante en criminología. La razón se ve facilitada por su pujante función de Internet. El computador se ha convertido en una herramienta tan útil que casi todas las sociedades del mundo moderno confían en él para realizar sus servicios o ceder, procesar y almacenar las informaciones. Con una correspondencia tan estrecha entre humanos y computadoras, no es difícil conjeturar la dificultad de la pérdida o el daño si se causa en un delito informático

Por otro lado, como antecedente nacional tenemos a Mori (2019) en su indagación concluyó el amparo penal de la privacidad en las violaciones informáticas con la intervención de los operadores de justicia tanto en la investigación, juzgamiento y la defensa penal de la intimidad, se determinó la

usencia de alineación tecnológica y desconocimiento informático, asimismo se logró evidenciar que la deontología tecnológica daña la competitividad de los operadores de justicia que intervienen en la inexacta determinación del tipo penal y en la competencia en la indagación y juzgamiento de los contravenciones informáticos, en ese mismo sentido Pardo (2018) en su investigación informó que el método jurídico del derecho penal de los delitos informáticos que transgreden el patrimonio en su vertiente de fraude es incompleta, debido a que en todas sus modalidades delictivas de los delitos informáticos contra el patrimonio, se ha demostrado que son muy complejas abiertas y ambiguas logrando rechazar la efectiva sanción penal en dichos ilícito contra el patrimonio. En esa línea de ideas Romero (2017) en su trabajo de investigación concluyó que el fraude por intermedio de computadoras, estas gestiones abarcan en la manipulación ilícita, mediante la creación de datos falsos o la transformación y manipulación de datos o procedimiento que se enlace en sistemas informáticos, elaborada con la finalidad de conseguir ganancias ilegítimas.

En la misma línea Blossiers (2018) refirió que los delitos informáticos, en la modalidad de fraudes y/o delitos que se rigen contra estas protege los ahorros que se encuentran depositadas en las empresas bancarias que puedan administrar y manipular fuertes capitales, no obstante, con ello los llamados hackers, han logrado acceder y violentar estos sistemas de seguridad, haciendo el uso ilegal de su conocimiento informático, con el fin de obtener dichosas ganancias, que no solo burlan y afectan a las empresas bancarias, de igual modo a todos sus usuarios. Asimismo, Florentina (2016) en su trabajo de investigación concluyó que los delitos cometidos por medio del Internet se vienen incrementando, subrayando el fraude por ser el más habitual, por tanto, esta estafa resplandece por ser una incierta en la sociedad actual ya que los malhechores no paran de hallar nuevas particularidades de realizar esta infracción penal.

Por su parte Villavicencio (2014) en su artículo científico informó que la imagen penal de dolo informático, normativizada en el artículo 8, del instrumento normativo de delitos informáticos lo clasifica e indica como un crimen de consecuencia, ya que su tipificación no abarca con realizar dicha comportamiento

exigida en el ejemplo legal (diseño, prólogo, variación, tachado, pérdida, clonación de fichas informáticos o cualquier interrupción o manejo en el desenvolvimiento de un método informático), siendo así que, es necesario establecer la consecuencia ulterior que radica en ocasionar el daño o perjuicio a tercero.

En relación a la protección penal Muñoz (2018) en su trabajo de indagación concluyó que se ha determinado que el resguardo y protección penal de la intimidad personal en las redes sociales en el Perú es insuficiente y deficiente dado que, no se ha tomado en consideración el redimensionamiento que posee este bien jurídico protegido en el ámbito del conocimiento y el desarrollo de la informática. Asimismo, por la relación y redacción de los ejemplos penales alusivos a la intimidad personal, se finaliza que no resguardan al bien jurídico protegido y no prevén la dimensión del daño producido.

En la misma línea Tirado (2015) refirió que el derecho penal es un derecho suplementario, fragmentario y posteriormente basado en el principio de intervención minúscula. La protección penal de la pertenencia intelectual no respecta, por ello, autoritariamente equivalente a la tutela civil o administrativa. En realidad, no lo es, pero los puntos de concurrencia y las zonas de confluencia entre los diferentes ámbitos de tutela son indudables y es obligatorio efectuar un esfuerzo interpretativo invariable para delimitar los confines de las adecuadas esferas de protección, en su labor de investigación De las Heras (2017) manifestó que el derecho penal resguarda los intereses jurídicos y que la sanción penal termina siendo la herramienta más eficiente y eficaz, con el fin de enmendar las conductas humanas que son socialmente reprochadas e inaceptables en los delitos de apoderamiento, incautación o interceptación interponiendo artificios técnicos para vulnerar y quebrantar la intimidad.

II.- MARCO TEÓRICO

A nivel de doctrina en primer orden pasaremos a definir el delito informático del cual se deriva el fraude informático materia de estudio de la presente investigación teniendo en cuenta las distintas opiniones doctrinarias, la regulación normativa tanto en la legislación nacional, comparada y la jurisprudencia de carácter nacional e internacional, en ese orden de ideas el Primer tratado

Internacional fue el convenio sobre la Ciberdelincuencia Budapest con fecha 23 de noviembre del 2001, habiendo ingresado en vigencia internacionalmente el 01 de julio del 2004 tratado internacional creado por los países miembros del Consejo de Europa, no obstante en nuestro país el Poder Legislativo recién dio por aprobado mediante Resolución Legislativa Nº 30913 con fecha 12 de febrero del 2019, el mismo fue ratificado por el Poder Ejecutivo mediante Decreto Supremo Nº 010-2019-RE, con fecha 10 de marzo del mismo año.

Según, la Real Academia Española define el fraude como aquella acción inversa a la realidad y a la rectitud, que perjudica a la persona contra quien se comete acto tendente a evitar una soltura legal en daño del Estado o de intermediarios, por su parte Jiménez (2017) señaló que el fraude es una forma de conseguir beneficios utilizando la creatividad, con la inteligencia y la habilidad del ser humano, dicho acto puede conllevar consecuencias muy graves para las personas que la realizan o para los que son víctimas.

Seguidamente en la doctrina nacional el fraude informático Villavicencio (2014) sostuvo que estas gestiones delictivas son convenientes del ilícito dañoso se cataloga como delito de consecuencia porque la conducta no basta que se configure en el delito de fraude informático, además de ello es menester que la acción tenga una consecuencia distante de la misma gestión el que resulte en causar el perjuicio a un tercero, en esa misma línea Mata y Martín (2003) consideran que la computación y en general, el procesamiento computado de investigación se muestra como factores criminógenos, pues consienten el acceso y el manejo de bases de datos y programas de cualquier género, en ocasiones de forma lesiva para los intereses básicos de las personas.

Asimismo, Sáenz (2013) opinó que el ilícito penal engloba, la amenaza a la esfera privada de las personas, lo cual implica la acumulación, archivo, asociación y propagación de datos obtenidos por medios informáticos y por otros delitos patrimoniales por la extralimitación de datos informáticos procesados de manera automáticamente. Aunado a ello, Prias (2016) señaló que los medios especiales empleados a fin de obtener el resultado tienen la virtud de transformar estas conductas en delitos que se caracterizan por la ausencia de presencia física del

sujeto activo para los ojos de la víctima, además para realizar las maniobras engañosas a través de la información contenida en una base de datos se difirieren en la producción de sus efectos en el tiempo.

En esa misma línea, Jiménez (2017) informó que el fraude informático es cualquier acción u omisión encaminada a eludir las disposiciones legales, penales o civiles, teniendo en cuenta que con ello se produzcan perjuicio contra el Estado o terceros, asimismo los clasifica de la siguiente forma: 1) Alterar el ingreso de datos de manera ilegal, ello requiere que el ciberdelincuente posea un alto nivel de técnica en redes informáticas para alterar datos como generar información adulterada que los permita beneficiar, crear instrucciones y procesos no autorizados o dañar los sistemas, 2) Alterar, destruir suprimir o robar datos, señala que es un evento difícil de detectar, 3) Alterar o borrar archivos, 4) Alterar o dar mal uso a sistemas o software consiste en alterar o reescribir códigos con propósitos fraudulentos, dichos eventos requieren de un alto nivel de conocimiento informático.

En relación al bien jurídico defendido de los delitos informáticos según Pérez (2017) informó que el bien jurídico protegido en el delito de fraude informático es el patrimonio, desde la perspectiva del derecho a la propiedad que tiene el sujeto pasivo correspondencia a su base de datos informáticos y/o al adecuado funcionamiento del sistema informático. Asimismo, Prias (2016) manifestó que se debe mantener la tutela del patrimonio económico de la persona por el daño que sucede sobre las mismas con la apropiación ilícita, más que la transgresión en la protección por el desmedro patrimonial que se afecte a su titular. Por su parte, Pérez (2017) refirió que la Ley de los delitos informáticos exceptúa del argumento patrimonial la simple intrusión, reflexionar como ilícito penal contra los datos y sistemas informáticos es decir sobre el acceso indebido y moderado contra la rectitud de datos informáticos y sistemas informáticos señalados en el artículo 2 y 3 del instrumento legal 30096. Respecto a la tipicidad objetiva la afectación con fines fraudulentos del sistema informático o de transmisión de datos para lograr una preeminencia económica constituye el contenido de lo ilícito este engaño puede residir tanto en la introducción de datos falsos como la eliminación de datos verdaderos, respecto a la particularidad típica del dolo informáticos.

Seguidamente, Pérez (2017) señaló que el delito nombrado fraude informático demanda en su aspecto que el agente, por medio de métodos informáticos encamine para sí o para otro un beneficio ilícito en agravio de un tercero mediante el diseño, introducción, variación, supresión, duplicación de los datos informáticos o manejo en el trabajo del método informático, la tipicidad requiere la necesaria maniobra de un sistema informático con el intención de lograr un ilegitimo favor económico por lo general las conductas se conciernen con la seguida maniobra del método informático entre otros, sin otra restricción que no sea provenida de la ley, la dirección de justicia o el contrato.

En ese orden de ideas, Gonzáles (2014) en su trabajo de indagación, concluyó que el elemento diferenciador del fraude informático reside en que la trasmisión patrimonial se realiza sin que la víctima ceda en su engaño, siendo el propio sujeto activo es quien lo hace a través de medios informáticos en este tipo hechos ilícitos no están presente los presupuesto de estafa, el accionar del defraudador se produce mediante un ordenador informático u otra máquina como por ejemplo el cajero automático de los bancos. Por un lado, Aboso (2011) indicó que se realiza esta especie de fraude el que traslada fondos ajenos a una cuenta propia o a favor de un tercero, o bien el que destruye fichas económicas que acaban por trastornar el cambio financiero personal, asimismo, quien maneja el sistema informático de la empresa en donde labora, alterándose la cuantía de encargos de mercancía usual expresados, con el objetivo de enviar el excedente de mercadería pedida a un tercero en complicidad con la ardid fraudulenta.

Aunado a ello, Mazuelos (2001) manifestó que el fraude informático presenta peculiaridad de no requerir que el dolo marche antecedida de una eliminación patrimonial incitado por un error humano, de ahí que resulte conveniente hacer referencia el fraude informático, como una modalidad de engaño a través de la red que no está sujeta a los requisitos exigidos por el clásico ilícito del ilícito penal cuya característica seria derivar de las relaciones interpersonales en un contexto social. Sin embargo, algunas manipulaciones informáticas podrían quedar comprendidas dentro del delito de estafa en la medida que se trate del engaño de la persona física que se encuentra del otro lado de la red.

Por su parte, De la Mata y Hernández (2011) opinaron que las conductas del fraude informático, consisten en lograr las traspasos no son consentidos de fondos través de disposiciones fingidas o de la alteración del funcionamiento de sistemas informáticos de las prácticas contables, las mismas pueden realizarse en el mismo programa en cualquier instante del proceso o método autorizado de datos, ya sea en la entrada input o escapatoria output, ya en la traspaso a distancia, mediante modem, red y otros.

Respecto al sujeto activo y pasivo del fraude informático Pérez (2017) sostuvo que es un delito común, el tipo que no exige condición y/o cualidad especifica la determinación del sujeto activo del ilícito penal es genérico, las operaciones del mercado financiero, de valores y tras actividades económicas, se trasladan a extremo sobre patrimonios no materializados, es decir, sobre escuetos informes contables electromagnéticas, sujetadas en base de datos, los cuales pueden ser motivo de codicia de personas que a través de medios informáticos buscan aprovecharse fraudulentamente perjudicando patrimonialmente a determinadas personas naturales o jurídicas.

Asimismo, Vizcardo y Silfredo (2014) señalaron que la conducta sitúa a cualquier persona natural o jurídica como sujeto activo, mientras que el tipo agravado coloca al Estado en tal situación, cuando se perturba su patrimonio, en analogía con los recursos económicos consignados a fines asistenciales o programas de apoyo social.

Según, Pérez (2017) indicó que el sujeto activo es el titular o autor de la gestión extraviada que tiene las situaciones técnicas bastantes para realizar un dolo esto es para trastornar trazar destruir etcétera algún dato método informático con el fin de obtener un beneficio ilícito para él o para otro sin interesar el perjuicio que pueda producir a un tercero como consecuencia de estafa en el fraude informático se puede imaginar tres tipos de sujeto según el argumento donde se halla, los que realizan el Estafa Interno; causado por dispositivos y personas de la propia formación puede ser muy grave ya que es ejecutado por persona que saben bien el contexto informático.

En la misma línea, Miró (2013) en su artículo científico señaló que el objetivo final en la mayoría los conflictos por medio de la red informática viene a ser el fraude patrimonial de un sujeto que maniobra en el mismo asimismo, ejecute o no movimientos económicos a través de la plataforma de Internet, esgrime servicios por medio del computador personal o de empresa utilizando correos electrónicos, ello es un riesgo que pueda verse latentemente vulnerado su pertenencia la protección penal del patrimonio frente a las distintas modalidades de ciberfraude.

Seguidamente, Oxman (2013) en su artículo científico concluyó que la sanción de las conductas delictivas no solo debería restringirse en el asunto sobre la concurrencia de la estafa, porque, en la actual de la legislación chilena está en las condiciones de sostener que el estado en esta materia requiere de un ajuste forzosa y urgente que acceda hacer frente a la insuficiencia de imponer la sanción penal que reclaman los fraudes bancarios de la comisión delictiva por medio de la banca informática, en todas sus dimensiones.

Por su parte, Pérez (2017) refirió que en algunos asuntos la computadora y las aplicaciones forman como centro material del delito, sobre el que reincide materialmente la acción para realizar el hecho plasmado en la norma, asimismo el ejercicio material no reincide sobre el orden o automatizado nombrado hardware que, como aparato físico, ya se encuentra preferido en otras figuras criminales: hurto, robo, apropiación ilícita, daños y otros.

En esa misma línea, Sáenz (2013) señaló que las conductas delictivas se ejecutan a través de sistemas informáticos que surgen como la herramienta empleada en la ejecución del ilícito penal patrimonial o socio económico, la esencia del ataque puede ser un dispositivo patrimonial de carácter económico por medios electrónicas de fondos en el uso de cajeros automáticos, también el propio sistema informático con la entrada de virus, camino ilícito a ordenadores y redes informáticos. En cuanto a la tipicidad subjetiva Pérez (2017) opinó que el delito de fraude informático es un delito preferentemente doloso (dolo directo) se exceptúa la particularidad de culposa que trascendería siendo diferente.

En correlación a la tipicidad objetiva Aboso (2011) sostuvo que la simulación con fines fraudulentos del sistema informático o de traspaso de datos reside en lograr una ventaja económica ilegítima que constituye el contenido de lo ilícito, esta presunción puede alcanzar tanto en el prólogo de datos falsos como la eliminación de datos verdaderos. Respecto a la modalidad típica de la estafa informática Pérez (2017) señaló que el delito nombrado dolo informático exige en su apariencia que el agente, a través de la plataforma informática o medios informativos encamine para sí o para otro un beneficio ilícito en provecho de tercero aplicando el diseño, preámbulo, transformación, borrado, eliminación, duplicación de fuentes informáticos o manejo en la marcha de un sistema informático. Por su parte Aboso (2011) refirió que la comisión de fraude informático reside en trasladar caudales ajenos a una cuenta propia o de un tercero o el que suprime datos económicos que acaban por perturbar el estado financiero personal.

Por un lado, Villavicencio (2014) opinó que las conductas impropias como “diseñar, meter, trastornar, borrar y suprimir” que han sido previstas en el artículo 8 del delito informático no incluyen en la modalidad de fraude informático; ya que dichas conductas son característicos del delito de daño son considerados como ilícitos de resultado porque, no basta que el evento delictivo de configure en el tipo penal para su consumación del delito de fraude informático, sino que además, es necesario que la acción de la conducta desplegada vaya acorde de un resultado apartado de la misma conducta que implique causar el perjuicio a un tercero, de lo contrario el delito quedaría en tentativa.

Bajo la misma línea en la doctrina Española según, Costa (2014) señaló que el fraude informático es aquella acción u omisión tendente a soslayar las normas de ordenamiento jurídico, previstas para regular las conductas humanas siempre que a través de ella tenga como resultado el perjuicio económico contra el Estado o terceros agraviados, en cuanto a los programas que utilizan los ciberdelincuentes son E. SPYWARE es un programa insertado en un ordenador con la finalidad de recopilar información de su computador y luego transmitido dicha información a una fuente externa sin el consentimiento y conocimiento del propietario del ordenador.

El término Spyware es un vocablo derivado del idioma inglés, estando ampliamente preparado en el campo de la informática y que en español se vuelve como exposición espía, que se ubica dentro de la clase de malware, conocido también como código perverso o software que tiene como misión introducirse en el sistema interno de la computadora sin la autorización del propietario para dañarla desde algún nivel, en cambio el F. Phishing, consiste en enviar de forma masiva los encargos que supuestamente proceden de fuentes honestos con la finalidad de lograr que el usuario suministre datos íntimos (ejemplo: contraseña de su cuenta de ahorro) en la práctica el caso típico de Phishing es el envío de correos electrónicos aparentando ser páginas originarios de una entidad financiera online, con el fin de lograr que los usuarios introduzcan sus caracteres de una página web falsa. Además, se caracteriza por obtener información confidencial de forma fraudulenta, como son las contraseñas o fuente de información puntualizada sobre tarjetas de crédito u otra información bancaria, con su accionar delictivo se hace pasar de una persona o empresa de confianza es una aparente noticia oficial electrónica, por lo común un correo electrónico o algo sistema de carteo breve, en consecuencia, este ciberdelincuente sustituye la identidad.

En la legislación nacional el delito de fraude informático se encuentra prevista y sancionada de conformidad al artículo 8 de la ley de contravenciones informáticos Ley Nº 30096, modificada por el artículo 01 de la Ley Nº 30171, mediante dicha instrumento legal se señala lo siguiente: el que deliberadamente e ilegítimamente orienta para sí o para otro un beneficio ilícito en deterioro de tercero mediante el bosquejo, prefacio, variación, borrado, exclusión, de datos informáticos o cualquier obstáculo o manejo en el trabajo de un método informático será merecedor de una pena privativa de libertad no menor de 03 ni mayor de 08 años y con sesenta a ciento veinte días de multa, asimismo la pena privativa de libertad será no menor de 05 ni mayor de 10 años y de 80 a 150 días de multa cuando se afecta el propiedad del Estado que sean propuestos a fines asistenciales o a programas de soporte social.

Por otro lado en el derecho comparado de España los fraudes sobre las estafas está prevista en el Artículo 248, numeral 02 literal a) del Código Penal Español, señala los que con valor de beneficio y bajo la forma de manejo sistematización o artificio parecido, logren una acción no consentida de cualquier activo patrimonial en quebranto de otro, b) Los que transformaren, metieren, tuvieren o suministraren programas informáticos sucintamente predestinados con el propósito de cometer las estafas previstas en este artículo y c) Los que manipulando tarjetas de crédito, débito, cheques de viaje, o los datos obrantes en cualquiera de ellos, realicen operaciones de cualquier clase en daño de su titular o de un tercero.

En el código cotejada de Italia el dolo informático se reglamenta en el art. 640 ter del Codice Penale sancionando el que de cualquier manera altere la marcha del método informático o telemático ingresando sin autorización con cualquier peculiaridad sobre los antecedentes, informaciones o programas contenidos en el sistema de información y en la que se busca un provecho con el resultado de dañar a otro. Siendo este sancionado con prisión de 06 meses a 03 años y con multa de 51 euros a 1.032 euros. La pena es agravada si se dan algunas de las formas establecidas en el numeral del 640.2º. 1 o bien si el acto doloso es concretado con arbitrariedad de carácter de ejecutor del sistema. El delito es sancionado por querella de la parte agraviada, salvo que asista alguna de las situaciones del 2º, o algún otro suceso agravante. Asimismo, en la legislación de Chile, Ley N° 19.223 de delitos informáticos en el Apartado 2° señala el que, con intensión de adueñarse, utilizar, o conocer ilícitamente de la información habida en un sistema de método de la misma, lo estorbe, obstruya o ingrese a él, será sancionado con pena menor en su grado mínimo a medio.

Seguidamente en nuestra jurisprudencia nacional se establece a través del Recurso de Nulidad con expediente 2041-2018 Sala Penal Permanente a través de este instrumento legal en el noveno fundamento se deja establecido que la reparación civil de S/.4000 (cuatro mil soles) solicitada a favor de la empresa Selme S. A. C. no fue objetada por aquella y, por ende, el Tribunal Superior no podía alterarla sorpresivamente en perjuicio de los imputados. Aquel monto peticionado

por el fiscal superior en su acusación incluyó los conceptos de daño patrimonial y extramatrimonial por el delito de fraude informático y, si bien se aprecia que no cubre el monto indebidamente apropiado por los acusados, no corresponde al órgano jurisdiccional modificarlo, pues el titular del objeto civil se ha conformado.

En la jurisprudencia internacional Colombiana recaído en el expediente 42724 – 2015, Sala de Casación Penal por el delito de Hurto por medios informáticos y semejantes para delinquir falsedad en documento privado, resuelve la suspensión condicional de la ejecución, manera de obiter dicta, no sobra aclarar que de haber satisfecho el procesado dicho requerimiento objetivo, no habría sido posible negarle la condena de ejecución condicional con fundamento en el artículo 68A -que prohíbe la concesión de este beneficio a quienes sean condenados por el delito de hurto calificado, para el efecto, la similitud dogmática del delito de hurto por medios informáticos con el descrito en el artículo 240 del Código Penal Colombiano.

Respecto del delito contra el patrimonio Jiménez (2017) señaló que la particularidad de los hechos ilícitos denominados generalmente fraude informático, vienen dada sin tomarse en cuenta la cosa material, más bien se toma su peculiar forma de comisión, y que en ella se emplea como herramienta el sistema informático para producir el hecho dañoso de propiedad ajeno, sobre determinados casos posibles en la que puedan concurrir expresiones que se ejecutan contra universos informáticos y por técnicas y clasificaciones informáticos.

Según los principios de la delegación Federal del Comercio Fernández (2015) informó que se ha sistematizado las formas más frecuentes de fraude patrimonial por medio del internet clasificándola así: a). Fraudes en ofertas y subastas, una vez efectuada la transacción, utilizando los soportes del comercio del comercio electrónico no son enviados o prestados los servicios o bienes adquiridos o existe la gran diferencia entre lo solicitado y lo que se recibe, b) acceso supuestamente gratuito a servicios de internet, en estos casos el usuario recibe una oferta de servicios gratuitos cuya aceptación conlleva implícito, sin él saberlo, un compromiso contractual a largo plazo con cláusulas penales en caso de desistimiento, c) Adult Check, se trata de una modalidad de estafa realizada a

través de páginas generalmente pornográficas en las que de forma aparentemente inocua, se solicita la serie de una tarjeta de crédito a fin de comprobar que el internauta es mayor de dieciocho años, d) oferta de servicios gratuitos durante un periodo de tiempo reducido, aproximado de 30 días naturales que son seguidos de cargos por el mantenimiento no solicitado, e) ventas de tipo piramidal, f) defraudaciones en la venta de oferta, venta y contratación de billetes de avión, viajes, arrendamientos, g) La llamada de estafa del 906, que consiste en el acceso de determinados servicios confidenciales por internet a través de los números de pago 906, que posteriormente instalan software internos en la terminal del usuario sin su autorización siendo muchas de sus conexiones informáticas se efectúan a través de estas líneas con tarifas exorbitantes h) oferta de compras online dudosas, pues al final del producto no podría llegar al cliente.

Por su parte, Arbulú (2019) opinó que los delitos informáticos contra el patrimonio aparentemente a un fraude si lo interpretamos a la luz del convenio de Budapest, entonces estamos ante la figura de la estafa, es decir que se produce el uso del engaño o alteración de la verdad como parte del comportamiento del sujeto activo.

III.- METODOLOGÍA

3.1 Tipo y diseño de investigación

Según, Sandín (2003) señaló que la investigación cualitativa “es una actividad sistemática orientada a la comprensión en profundidad de fenómenos educativos y sociales, a la transformación de prácticas y escenarios socioeducativos, a la toma de decisiones y también hacia el descubrimiento y desarrollo de un cuerpo organizado de conocimientos”. Por lo antes mencionado el proyecto de investigación tendrá un enfoque cualitativo.

El nivel de la investigación es Descriptivo; asumiendo lo precisado por Babbie (2013) quien precisó que esta investigación usa el método descriptivo para caracterizar un objeto de estudio; permitiendo identificar en las variables de estudio las características relevantes que determinan el problema actual.

La investigación es de tipo no experimental, por cuanto, no se ha desarrollado ningún trabajo de campo en un laboratorio y no se han manipulado las variables de estudio; y es Transversal porque el recojo de información se realizó en un solo momento. El método utilizado fue de trabajo de campo, la observación participante y la entrevista en profundidad.

El diseño de la presente tesis es socio crítico de la fenomenología, la misma que se fundamenta en la siguiente premisa (Hernández, Fernández, & Baptista, 2006) refirió que "El investigador contextualiza las experiencias en términos de su temporalidad (tiempo en que sucedieron), espacio (lugar en el cual ocurrieron), corporalidad (las personas físicas que la vieron) y el contexto relacional (los lazos que se generaron durante las experiencias)".

3.2. Escenario de estudio

En el presente trabajo de investigación el escenario de estudio se desarrolló en el Distrito Fiscal de Lima Norte, donde los entrevistados proporcionaron sus conocimientos en base a su experiencia en la presente tesis, del mismo modo fuentes documentadas, artículos científicos de ámbito nacional e internacional, los mismos han sido de utilidad que ha permitido coadyuvaron a tener una mejor conceptualización del problema general.

3.3. Participantes

Son aquel sujeto o informantes de estudio para la presente investigación personas idóneas, por ello se eligió a los representantes del Ministerio Público del Distrito Fiscal de Lima Norte, Jueces Penales y los operadores de justicia ya que ellos conocen el problema general y específicos que han sido identificados en el presente trabajo de investigación.

***Tabla 1*: Caracterización de participantes**

Participantes	Descripción
Experto 1 **-** Operador de Justicia	**(E1)** Dra. Ana María Revilla Palacios, Juez del Quinto Juzgado Especializado en lo Penal de la Corte Superior de Justicia de Lima Norte.

Experto 2 **-** Operador de Justicia	**(E2)** Dra. Cris Lloly Ruiz Cárdenas, Jueza Especializada Supernumeraria del Juzgado de Investigación Preparatoria Transitoria de Ancón y Santa Rosa de la Corte Superior de Justicia de Ventanilla.
Experto 03 - Operador de Justicia	**(E3)** Dr. Alejandro Sánchez Crisólogo, Fiscal Ajunto Provincial, Distrito Fiscal de Lima Norte.
Experto 04 - Operador de Justicia	**(E4)** Dra. María del Carmen Ampuero Quinteros Fiscal Adjunta Provincial, Distrito Fiscal Lima Norte.
Experto 05 - Operador de Justicia	**(E5)** Dra. Paola Guerra Arauco, Fiscal Adjunta Provincial del Distrito Fiscal de Lima Norte.
Experto 06 - Operador de Justicia	**(E6)** Zebastián Zegarra Gonzales, Asistente en función Fiscal, Distrito Fiscal de Lima Norte.
Experto 07 - Operador de Justicia	**(E7)** Dr. Fredy Ramírez Bailón, Asistente en función Fiscal, Distrito Fiscal de Lima Norte.
Experto 08 - Operador de Justicia	**(E8)** Dr. Guillermo Jesús Matallana Lucero, Asistente en función Fiscal, Distrito Fiscal de Lima Norte

***Tabla 2*: Matriz de construcción de categorías y subcategorías**

Categorías	Subcategorías	Fuente	Técnica	Instrumento
Fraude informático	Alterar el ingreso de datos de manera ilegal	Expertos o especialistas	Entrevistas	Guía de preguntas de entrevista
	Alterar, destruir, suprimir o robar datos.			
	Alterar o borrar archivos			
	Alterar o dar un mal uso a sistemas o software		Observación	
	Bien Jurídico protegido			

Protección penal	Tipicidad objetiva Tipicidad subjetiva Pena y circunstancia agravante	Análisis de las normas nacionales

3.4.- Técnicas e instrumentos de recolección de datos

Por su parte, Hernández et al. (2014) refirió que la recolección de datos implica un conjunto de acciones no normalizadas ni completas, porque, se obtiene dicha información producto de opiniones que si bien son expertos del tema; sin embargo, son personas con criterios y formas individuales de observar los eventos. La información se recogió con el propósito de realizar un análisis y contrastar sus opiniones con la realidad empírica y los aspectos teóricos citados en nuestro marco teórico.

Para el recojo de información se utilizaron las siguientes técnicas:

La entrevista según, Hernández et al. (2014) precisó que esta técnica es significativa y relevante porque representa la opinión del experto quien responde a una gama de preguntas elaboradas por el entrevistador.

La observación, es la técnica consistente en la primera forma de contacto que ha sido empleada para examinar directamente el presente fenómeno de manera espontánea y natural, al momento de recopilar los datos de los expertos durante el desarrollo de la entrevista en el escenario de estudio, conforme lo sostiene Hurtado (2000).

Los instrumentos de recolección de datos utilizados en el desarrollo de la presente investigación, son:

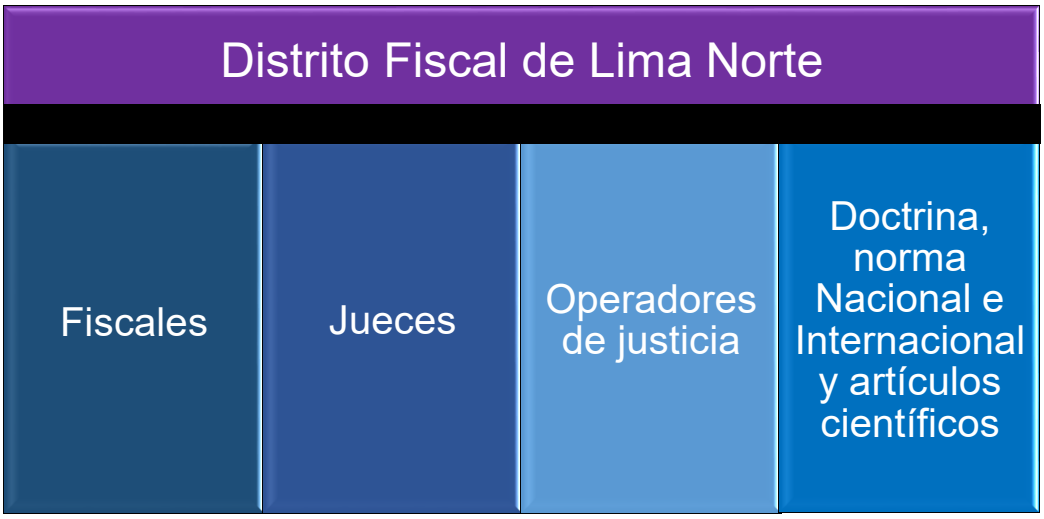
Guía de entrevista, es el instrumento de recolección de datos para lo cual se elaboraron 8 preguntas abiertas, teniendo en cuenta las Categorías y Subcategorías planteadas como parámetro de sus respuestas.

Guía de observación, es el instrumento con el cual se realizó el proceso de atención, recopilación y registro de la información en su estado natural, durante el desarrollo de la entrevista en el escenario de estudio.

Guía de análisis de fuente documental, este instrumento permitió realizar un análisis y contrastación de la información obtenida por autores citados y las respuestas de los entrevistados.

Mapeamiento: Esta investigación se llevará a cabo en el Distrito Fiscal de Lima Norte, y se tendrá como principales sujetos de entrevista a los funcionarios de este distrito fiscal.

***Figura 1*: Mapeamiento**



3.5. Procedimiento

Para el trabajo de campo, en cuanto al desarrollo de las entrevistas se coordinaron con los entrevistados en sus respectivas oficinas de trabajo, aplicándoles el motivo de la visita y la necesidad de contribuir con su experiencia en el ámbito jurídico en la presente investigación respecto a la vulneración del derecho fundamental a la prueba en la etapa preprocesal; los entrevistado accedieron y dieron el permiso voluntario para ser entrevistados en diferentes fechas, las mismas que se materializaron en sus respectivas oficinas.

Figura 2: Trayectoria metodológica de la investigación

3.6. Métodos de análisis de información

Según, Hernández et al. (2015) opinaron que la fase de recojo de información es importante en todo estudio; este proceso viabiliza el análisis y comprensión de forma integral, permitiendo a los entrevistados proporcionar sus respuestas a las preguntas elaboradas generando relevantes críticas y nociones conceptuales.

En el análisis de la investigación se ha utilizado diversos métodos que son propios de la investigación cualitativa, entre las cuales son: a). Método Comparativo: Se utiliza para comparar los diversos resultados en una encuesta o entrevista, al igual que en la comparación de documentos que son guía del presente estudio, b). Método Descriptivo: Expone las diversas posturas tanto de los entrevistados como el de los juristas que han sido citado en el estudio, c). Método Deductivo: Es empleado como táctica de demostración para inferir o suponer un

resultado razonable y justo, este método parte de lo habitual o genérico a lo especifico, ya que sus resultados se basan de sus mismas hipótesis y, d). Método Analítico: Es usado para realizar el estudio de manera singular cada obtuvo o problema.

En este estudio, se realizó el análisis de las normas nacionales e internacionales, los cuales ayudaran a resolver el interrogante principal de este estudio, asimismo se debe tener presente que dentro de la investigación su subjetivos se convertirán en categorías y a su vez en categorías y subcategorías las cuales se analizaran de forma responsable.

3.7. Aspectos éticos

El presente trabajo de investigación cumple con la formalidad y rigor científico exigido por la sociedad académica científica, las fuentes bibliográficas, artículos científicos, tesis, tiene la debida citación acorde a las normas internacionales de referencias bibliográficas, en aplicación de las normas APA, la recolección de información en campo es auténtica y fiable por el empleo de las técnicas e instrumentos de recolección, por lo que cumple con los criterios de Credibilidad, Transferibilidad, y Confortabilidad.

IV. RESULTADOS Y DISCUSIÓN

Con respecto a resultado se ha realizado la transcripción de los datos recopilados mediante el instrumento de guía de entrevista a los expertos idóneos conocedores en materia de derecho penal y procesal penal, las informaciones completas de estos aspectos están insertados en la parte de los anexos del presente trabajo de investigación.

La discusión es una dialéctica entre los objetivos propuestos, los resultados de las entrevistas, los antecedentes y la teoría utilizada, surgiendo un debate armonioso y/o no armonioso entre dichos elementos, dando como resultado un aporte a la academia científica. Esto es, la discusión reside en presentar el significado de los descubrimientos logrados y cotejarlos con los estudios anteriores utilizados como antecedentes con el fin de encontrar analogías, divergencias y convergencias (Arias, 2012).

Bajo esa lógica procederemos a desarrollar la discusión de los datos informativos recopilados durante el curso del presente trabajo de investigación. El resultado de la guía de entrevista utilizada para recabar las opiniones de los expertos idóneos en la materia como son los Jueces, Fiscales penales y los operadores de justicia del Distrito Fiscal de Lima Norte, serán contrarrestadas y comparadas con las fuentes académicas empleadas, las tesis nacionales e internacionales, así como la literatura en lengua castellana e inglesa que se han utilizado para lograr a entender científicamente el fenómeno problemático descrito en la introducción, para lo cual se propusieron cuatro objetivos.

El primer objetivo de la presente investigación, es determinar cuáles son las implicancias jurídicas del fraude informático y la protección penal del delito contra el patrimonio Distrito Fiscal de Lima Norte. Los resultados conseguidos en las entrevistas los magistrados coinciden con las posiciones arribadas en los antecedentes nacionales y extranjeras respecto al fraude informático. En el sentido de que el delito contra el patrimonio de fraude informático se viene incrementando por ser más habitual utilizando los medios informáticos por los ciberdelincuentes, pero el método jurídico penal es muy compleja abierta y ambigua sin tener la efectividad de la sanción penal, asimismo en sus trabajos de investigación de, Pardo (2018), Blossiers (2018), Mesa (2017), Utreras (2017), Florentina (2016), Chungata (2015), Acurio (2015), Gonzáles (2014), Gil (2015) y Mayer y Oliver (2020) quienes también han coincidido con sus puntos de vista de manera uniforme respecto al fraude informático.

Del mismo modo, a nivel de marco teórico, también existe coincidencia en líneas generales con las posiciones de los autores Pérez (2017), Jiménez (2017), Villavicencio (2015), Fernández (2015) Aboso (2011), Vizcardo y Silfredo (2014), Costa (2014), quienes opinaron que el fraude informático se ha sistematizado de manera más frecuente el fraude patrimonial por medios informáticos causando perjuicio económico. Las posesiones de los magistrados entrevistados, con algunas diferencias entre sí, llegaron a sostener que los delitos contra el patrimonio en la modalidad de fraude informático provocan perjuicio económico a la parte agraviada la cual implica una sanción penal pero no se logra efectivizar por la complejidad en la forma de operar el accionar delictivo los medios tecnológicos.

En cuanto a lo más específico los antecedentes nacionales e internacionales la mayor parte coinciden que el fraude informático en los delitos contra el patrimonio implica la sanción penal, sin embargo ello en la práctica actualmente no tiene efectividad para imponer dicha sanción debido a la complejidad de investigación para seguir el rastro e identificar al autor material del delictivo, la misma que según Mata y Hernández (2011) refieren las conductas del fraude informático, consisten en lograr los traspasos que no son consentidos de fondos a través de disposiciones fingidas o de la alteración del funcionamiento de sistemas informáticos. Ahora bien, se coincide entre las fuentes consultadas y los resultados de la investigación cuando se altera el ingreso de datos de manera ilegal dicha conducta implica una sanción penal en contra de quien lo realiza a través de medios informáticos.

En cuanto al segundo objetivo, describir de qué manera repercute el fraude informático en la protección penal del delito contra el patrimonio Distrito Fiscal de Lima Norte 2020, conviene destacar que efectivamente como lo sostienen Pardo (2018) y Blossiers (2018) en sus tesis de delitos informáticos en la modalidad de fraude informático señalan que protege ahorros que se encuentra depositadas ante las entidades Bancarias, los llamados hackers se burlan para acceder y violentar los sistemas de seguridad informática. Tal posición es convergente con los resultados, debido a que, los magistrados del distrito fiscal de Lima Norte opinan en esa misma línea, el fraude informático repercute de manera negativa en los derechos patrimoniales de los privados inclusive del Estado mismo porque les causa el perjuicio económico.

En cuanto al tercer objetivo, describir cómo se relaciona el fraude informático en el delito contra el patrimonio Distrito Fiscal de Lima Norte, al respecto cabe destacar que efectivamente como lo sostienen Utreras (2017) Mayer y Oliver (2020) en su tesis coinciden que el fraude informático se relaciona con el delito contra el patrimonio respecto al resultado y su disposición típica con el perjuicio patrimonial impropio y, la representación de lucro en el agente de su conducta incriminada. Tal posesión es convergente con los hallazgos de las entrevistas debido a que los Magistrados del Distrito Fiscal de Lima Norte coinciden que el fraude informático consiste en el menoscabo del patrimonio y perjuicio económico de la víctima, le dan mayor peso a la forma en que se concreta y materializa el acto doloso.

Al respecto en los resultados de las entrevistas dirigido a los Jueces, Fiscales y operadores de justicia en relación a alterar, destruir, suprimir o robar datos informáticos puede ser difícil de detectar la conducta ilícita del ciberdelincuente en el delito contra el patrimonio, los entrevistados coinciden que el fraude informático con el avance de la ciencia tecnológica implica nuevos retos para la lucha contra la criminalidad y esta surge a la par con la innovación de la tecnología, en este sentido los que luchan contra este flagelo son la Policía, Fiscalía y operadores de justicia quienes deben de contar con los medios tecnológicos y logística sofisticada para estar a la par en la lucha contra la ciberdelincuencia. Tal convergencia con los resultados obtenidos en el trabajo de campo, puesto que los magistrados opinaron de manera concordante que se debe contar con la logística necesaria para estar a la par contra organizaciones criminales de los ciberdelincuentes.

Respecto al cuarto objetivo analizar de qué manera afecta el fraude informático en el derecho patrimonial del agraviado en Distrito Fiscal de Lima Norte, sobre el particular conviene destacar conforme lo sostienen Romero (2016) y Blossiers (2018) en su trabajo de investigación coinciden que el fraude por intermedio de computadoras, abarcan en la manipulación ilícita, mediante la creación de datos falsos o la transformación y manipulación de datos o procedimiento que se enlace en sistemas informáticos, elaborada con la finalidad de conseguir ganancias ilegítimas, en la cuenta de ahorros que se encuentran depositadas en las empresas bancarias que puedan administrar y manipular fuertes capitales, no obstante, con ello los llamados hackers, han logrado acceder y burlando sistemas de seguridad afectando de manera negativa en perjuicio del derecho patrimonial de las víctimas.

Ahora bien, respecto a la entrevista efectuada en la investigación en relación a alterar o borrar archivos no autorizadas sobre datos almacenados en los medios informáticos lo puede realizar cualquier persona en los delitos contra el patrimonio, en este aspecto los entrevistados concuerdan respecto a los involucrados en este accionar delictivo son en muchos casos organizaciones delictivas que cuentan con alta tecnología para cometer este tipo de delitos, valiéndose de métodos informáticos en base a su alto nivel de conocimiento sobre la materia, empleando

instrumentos informáticos de hardware y software del computador y que en muchos casos queda impune por cuanto no son detectables debido a que se puede decir que este es un delito invisible que no causa daño material o físico.

No obstante, podemos señalar que, en casi todas la entrevistas, implícitamente se podría sostener que cuando algunos magistrados sostienen que en cuanto a : que para alterar o dar un mal uso a sistemas o software con propósitos fraudulentos se requiere de un alto nivel de conocimiento informático en los delitos contra el patrimonio, en este aspecto coinciden en que la criminalidad en el mundo en general al parecer siempre se encuentra al avance de nuevas formas de delinquir y crear sobre todo nueva modalidad de delitos y en muchos caos el agente activo como en el caso de delitos de fraude informático requieren de una alta especialización en la materia, pudiéndose decir que son especialistas en este tipo de delitos ya que no cualquiera lo puede realizar sin que antes tenga pleno conocimiento sobre la materia.

Con respecto al bien jurídico protegido en el fraude informático, desde la perspectiva del derecho a la propiedad del sujeto pasivo en los delitos contra el patrimonio, la mayor parte de los entrevistados coinciden que el bien jurídico tutelado es el derecho al patrimonio sobre datos almacenados por medio de sistemas o software la cuenta de ahorros de sus titulares en las entidades financieras siendo el elemento principal para la consumación del delito de fraude informático es a través del sistema informático que permite al ciberdelincuente el poder borrar, sustraer, alterar alguna información reservada, sin embargo algunos opinan con matices diferentes es decir el derecho principal que se transgrede es el secreto de la información que se viola de diversas maneras, ya sea alterando, sustrayendo borrando archivos, con el objeto de causar perjuicio al sujeto pasivo.

Por otro lado, con relación a la entrevista formulada en que consiste la tipicidad objetiva del fraude informático en el delito contra el patrimonio tanto Jueces, fiscales y operadores de justicia concuerdan que en este tipo de delitos se debe analizar si concurren los elementos de la tipicidad conforme a lo prescrito en la normatividad vigente teniendo en cuenta la conducta del agente y el objeto material del hecho ilícito, además debe existir la afectación en el bien patrimonial a

través del fraude informático. Tal posición es parcialmente divergente por la minoría de los entrevistados con los hallazgos encontrados consideran que la tipicidad objetiva consiste en aquella acción humana desplegada con la intención de afectar y burlar el funcionamiento de sistemas de dispositivos informáticos, así como de transmisión de datos con el propósito de obtener el provecho económico.

Ahora bien, respecto cuáles son los criterios para establecer la tipicidad objetiva en el fraude informático del delito contra el patrimonio, al respecto la mayor parte de los entrevistados coinciden que los criterios están orientadas a la exigencia en el cumplimiento de los elementos típicos del fraude informático que debe estar prescrito conforme a la norma, teniendo en cuenta la dimensión del daño patrimonial a través de la manipulación o alteración de datos o programas de sistemas informáticos al sustraerse el mismo la información que puede afectar el patrimonio del agraviado.

En cuanto a los entrevistados mencionan en lo que respecta en que consiste el análisis de la tipicidad subjetiva del fraude informático en los delitos contra el patrimonio, al respecto también la mayor parte de los entrevistados coinciden al señalar que solo comprende la conducta dolosa del sujeto activo excluyendo la modalidad culposa porque resultaría atípica debido a que su accionar reviste de intención conocimiento y voluntad de ejecutar el delito con la finalidad de acceder a datos de una cuenta de ahorros a fin de efectuar trasferencias electrónicas de fondos o con la utilización de tarjetas en los cajeros automáticos y acceso ilícitos a ordenadores de redes a través del internet.

Se puede llegar a la conclusión según las entrevistas realizadas que, en la actualidad, el avance tecnológico en la informática es uno de los instrumentos más utilizados en las actividades diarias que realizan las personas la misma nos permite interactuar a través de la plataforma de internet, por su versatilidad y automatización. Pero lamentablemente esta plataforma últimamente se encuentra siendo utilizada como una herramienta para poder delinquir, teniendo como consecuencia la afectación de los bienes patrimoniales de la propiedad privada y del estado.

V. CONCLUSIONES

Primera: Las implicancias jurídicas del fraude informático están orientadas a la sanción penal por el accionar dolosa de los ciberdelincuentes siempre que estas afecten los derechos patrimoniales de la parte agraviada, no obstante dicha sanción en la práctica no logra su efectividad punitiva, debido a la complejidad del modus operandi empleando el conocimiento y la manipulación de los medios informáticos lo cual limita los tres niveles de exigencia, un fundamento jurídico, amparado en las normas penales- vigentes al caso concreto, fundamento fáctico y probatorio.

Segunda: El fraude informático en la protección penal de los delitos contra el patrimonio repercute de manera negativa frente a los derechos patrimoniales de los privados y del propio Estado debido a que en la mayoría de los casos de investigación a nivel fiscalía no se logra identificar al autor material del hecho ilícito fraudulento teniendo como consecuencia el archivo definitivo de la investigación quedando impune el delito siendo afectado la esfera patrimonial de la parte agraviada.

Tercera: El fraude informático con el delito contra el patrimonio se relaciona con comportamientos que corresponden a otros delitos de carácter patrimonial En principio, la idea de fraude connota la producción de un perjuicio patrimonial a través de la manipulación o alteración de datos y software de sistemas informáticos. No obstante, a pesar del interés que suscita y su relevancia práctica, aún no existe absoluta claridad en el modo de proceder para afrontar las investigaciones para lograr un resultado exitoso.

Cuarta: La conducta de fraude informático en el derecho patrimonial del agraviado afecta de manera negativa porque el accionar del ciberdelincuente provoca grandes pérdidas económicas haciendo uso de su conocimiento tecnológico en la manipulación supresión y clonación de datos con el propósito de efectuar transferencias, electrónicas a cuentas distintas por medios informáticos.

VI. RECOMENDACIONES

Primera: Se recomienda que los Magistrados empleen instrumentos internacionales en cuanto a la tecnología se refiere con intercambio de información capacitación, medios logísticos y doctrinarios de tal manera que sus resoluciones estén completamente motivadas, pues es necesario considerar criterios convencionales por ser parte de nuestro derecho interno.

Segunda: Se recomienda al Ministerio Público al Poder Judicial, la Policía Nacional del Perú que sumen esfuerzos de forma conjunta con la solidaridad y cooperación interinstitucional a fin que con prontitud planifiquen y establezcan los lineamientos y protocolos a seguir ceñido a los avances vertiginosos de la vanguardia tecnológica para tener mayores alcances y posibilidades de enfrentar con mayor efectividad la ciberdelincuencia.

Tercera: Para que la nueva creación de las fiscalías especializadas en la lucha contra los delitos informático específicamente en la modalidad de fraude informático recientemente creadas que invierta más en contar con personal capacitada en informática y logística necesaria para combatir este tipo de delitos, así como que tenga alcance para todos los recursos indispensables para la prevención del delito y afrontar la ciberdelincuencia.

Cuarta: Es necesario utilizar nuevos instrumentos tecnológicos como requisito obligatorio a fin de que los Magistrados y operadores de justicia tengan mayor soporte científico al momento de investigar los delitos de fraude informáticos, deben complementar y profundizar la presente investigación, sobre todo adaptarlo a su contexto social. Se sugiere que se realice investigaciones de enfoque mixto cualitativo y cuantitativo para tener mayor profundidad en el estudio, incluso realizar trabajos comparativos entre Distritos Judiciales. La tarea es muy difícil, pues muchos magistrados no disponen de tiempo y otros no colaboran con las investigaciones académicas.

Referencias

Aboso, G. (2011). *La nueva regulación de los llamados delitos informáticos en el Código Penal Argentino.* Lima: USMP.

Acurio, S. (2015). *Delitos informatico generalidades*. Obtenido de https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

Alcívar C., Blanc G., y Calderón J. (2018). Aplicación de la ciencia forense en los delitos informáticos en el Ecuador y su punibilidad. http://www.revistaespacios.com/a18v39n42/a18v39n42p15.pdf. Obtenido de http://www.revistaespacios.com/a18v39n42/a18v39n42p15.pdf

Arbulú, V. (2019). *Derecho Penal Parte Especial los delitos contra el patrimonio.* Lima: Instituto Pacífico.

Babbie, E. (2013). *Fundamentos de la investigación social.* Mexico, D. F.: nternacional Thompson Editores.

Biblioteca del congreso nacional de Chile. (1993). *Delitos informáticos, sistemas de información Ley Nº 19223 - Chile*. Obtenido de https://www.bcn.cl/leychile/navegar?idNorma=30590

Blossiers, J. (2018). *El delito informático y su incidencia en la empresa bancaria*. Obtenido de http://repositorio.unfv.edu.pe/handle/UNFV/2608

BOE Legislación Española. (1995). *Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.* Obtenido de https://www.boe.es/buscar/pdf/1995/BOE-A-1995-25444-consolidado.pdf

Cevallos, Y., et al (2020) La interpretación extensiva y la analogía en los delitos de estafa con documento bancario. https://www.recimundo.com/index.php/es/article/view/774/1208.

Chungata, A. (2015). *El fraude como delito informatico*. Obtenido de http://dspace.ucuenca.edu.ec/bitstream/123456789/21321/1/TESIS.pdf

Congreso de la República del Perú. (2014). *Ley que modifica la ley 30096, ley de delitos informáticos*. Obtenido de https://leyes.congreso.gob.pe/Documentos/Leyes/30171.pdf

Corte Suprema de Justicia del Perú (2018) *Recurso de Nulidad*. Obtenido de https://drive.google.com/file/d/1F3DJOLOtea5TZ1U4qnAUSqvTtyllVydz/view

Council of Europe, serie de Tratados Europeos Nº 185. (2001). *Convenio sobre la ciberdelincuencia - Budapest, 23.XI.2001*. Obtenido de https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

De la Mata, N., y Hernandez, L. (2011). *Problemas de tipiciaicón de los delitos informáticos: en Dogmática Penal de Derecho Penal Económico y Política Criminal.* Lima: USMP.

De las Heras, L. (2017). *Protección penal de la intimidad una revisión crítica a propósito del nuevo artículo 197.7 del Código Penal Español*. Obtenido de https://ddd.uab.cat/pub/tesis/2018/hdl_10803_461084/ldlhv1de1.pdf

Diario el Peruano. (2019). Obtenido de https://busquedas.elperuano.pe/download/url/resolucion-legislativa-que-aprueba-el-convenio-sobre-la-cibe-resolucion-legislativa-n30913-1740637-2

Diario el Peruano. (2019). *Ratifican el "Convenio sobre la Ciberdelincuencia" Decreto Supremo Nº 010-2019-RE*. Obtenido de https://busquedas.elperuano.pe/normaslegales/ratifican-el-convenio-sobre-la-ciberdelincuencia-decreto-supremo-n-010-2019-re-1748338-2/#:~:text=N%C2%BA%20010%2D2019%2Dre&text=a)%20De%20conformidad%20con%20lo,cometa%20infringiendo%20medidas%20de%20seguridad

Ezequiel, L. (2019). *Los delitos informáticos en el Código Penal Italiano- Computer crimes in the Italian Criminal Law*. Obtenido de http://www.scielo.org.mx/pdf/dgedj/v5n14/2448-5136-dgedj-5-14-127.pdf

Florentina, C. (2016). *Fraudes en internet*. Obtenido de http://repositori.uji.es/xmlui/bitstream/handle/10234/161252/TFG_2016_DincaClaudia.pdf?sequence=1

Gómez, J. (2016). *El tipo penal de fraude informático*. Obtenido de https://epikeia.leon.uia.mx/old/numeros/04/epikeia04-fraude_informatico.pdf

Gonzáles, M. (2014). *Fraude en Internet y Estafa Informática*. Obtenido de https://digibuo.uniovi.es/dspace/bitstream/handle/10651/27824/TFM_Gonzalez%20Suarez,%20Marcos.

Habirovs, A. (2018). *Factors that shape cybercrime victimisation and use of prevention measuresin* . Obtenido de http://eprints.hud.ac.uk/id/eprint/35042/1/FINAL%20THESIS%20-%20HABIROVS.pdf

Hernández, R., Fernandez, C., y Baptista, P. (2014). *Metodología de investigación* (6º ed.). Mexico: Mc Graw Hill.

Hurtado, J. (2000). *Metodología d ela investigación holística*. Obtenido de https://ayudacontextos.files.wordpress.com/2018/04/jacqueline-hurtado-de-barrera-metodologia-de-investigacion-holistica.pdf

Jiménes, J. (2017). *Manual de Derecho Penal Informático* (1º ed.). Lima: Jurista Editores.

Mata, N. y Martín, R. (2003). *Delincuencia Informática y Derecho Penal.* Hispamer , Managua.

Mayer, L. y Oliver, G. (2020). *El delito de fraude informatico concepto y delimitación*. Obtenido de https://scielo.conicyt.cl/pdf/rchdt/v9n1/0719-2584-rchdt-9-1-00151.pdf

Mazuelos, L. (2001). Los Delitos Informáticos: una aproximación a la regulación del Código Penal Peruno, en Revista de Doctrina y Jurisprudencia Penales Nº 02.

Mesa, D. (2017). *La ciberdelincuencia y sus consecuencias jurídicas*. Obtenido de https://uvadoc.uva.es/bitstream/handle/10324/26749/TFG-D_0368.pdf?sequence=1&isAllowed=y

MInisterio Público. (2019). *Boletín Estadístico del Ministerio Público*. Obtenido de https://www.mpfn.gob.pe/Docs/0/files/boletin_estadistico_febrero_2019.pdf

Mori, F. (2019). *Los delitos informáticos y la protección penal de la intimidad en el distrito judicial de lima, periodo 2008 al 2012*. Obtenido de http://repositorio.unfv.edu.pe/handle/UNFV/3519

Muñoz, L. (2018). *Protección penal de la intimidad social en la redes sociales*. Obtenido de http://tesis.unap.edu.pe/bitstream/handle/UNAP/9897/Mu%C3%B1oz_Quispe_Lenin_Leonir.pdf?sequence=1&isAllowed=y.

Pardo, A. (2018). *Tratamiento jurídico penal de los delitos informáticos contra el patrimonio, Distrito Judicial de Lima, 2018*. Obtenido de https://repositorio.ucv.edu.pe/handle/20.500.12692/20372

Prias, J. (2016). *Aproximación al estudio de los delito informáticos, en Derecho Penal Contemporaneo. Revista Internacional Nº 17.*

Real Academia Española (s.f.) *Diccionario virtual Real Academia Española*. Obtenido de https://www.asale.org/academias/real-academia-espanola

Romero, M. (2017). *Delitos informáticos cometidos a través de redes sociales y su tratamiento en el Ministerio Público en la ciudad de Huánuco, 2016.* Obtenido dehttp://repositorio.udh.edu.pe/bitstream/handle/123456789/331/T_047_%2025858529_T.pdf?sequence=1&isAllowed=y

Sáenz, J. (2013). *LOs Delitos y su relación con los ordenadores, El mal llamado delito informático: en temas de ciencias penales I. Libro homenaje a 50º aniversario de la USMP.* Lima: U.S.M.P.

Sandín, M. (2003). *Investigación Cualitativa en Educación. Fundamentos y tradiciones*. Obtenido de https://www.academia.edu/5026577/Investigaci%C3%B3n_Cualitativa_en_Educaci%C3%B3n_Fundamentos_y_tradiciones

Kavipriya, T. y Geetha, N, (2018). *An identification and detection of fraudulence in credit card fraud transaction system using data mining techniques*.Obtenido dehttps://d1wqtxts1xzle7.cloudfront.net/55859535/IRJETV5I1263.pdf?1519196638=&response-content-disposition=inline%3B+filename%3DAN_IDENTIFICATION_AND

Temitayo, O. y Olaniyan, F. (2018). *The Impact of Fraud on the Performance of Deposit Money*. Obtenido de file:///C:/Users/HP/Downloads/IJIFER-M-4-2018.pdf

Tirado, J. (2015). *La protección penal de la propiedad intelectual (análsis tras la reforma del código penal del 2015)*. Obtenido de https://www.tdx.cat/bitstream/handle/10803/650847/2015_Tesis_Tirado%20Estrada_JesusJose.pdf?sequence=1&isAllowed=y

Tobias, K. (2018) *I declare that this work has not been submitted for any other degree or professional qualification. The thesis is the result of my own independent work*. Obtenido de https://www.napier.ac.uk/~/media/worktribe/output-1256175/fraud-preventio-in-the-b2c-

Tribunal de Justicia de Colombia. (2015). *Sala de Casaciones Penal Exp. 42724 - 2015*. Obtenido de https://cortesuprema.gov.co/corte/wp-content/uploads/relatorias/pe/b1mar2015/SP1245-2015.pdf

Utreras, P. (2017) *La necesidad de tipicar el delito de fraude informatico en Chile*. Obtenido de http://repositorio.uchile.cl/bitstream/handle/2250/151758/La-necesidad-de-%20tipificar-el-delito-de-fraude-inform%C3%A1tico-en-Chile-an%C3%A1lisis-%20jurisprudencial-doctrinario-y-normativo.pdf?sequence=1&isAllowed=y

Villavicencio, F. (2014) *Delitos informáticos Cybercrímenes*. Obtenido de file:///C:/Users/HP/Downloads/13630-Texto%20del%20art%C3%ADculo-54269-1-10-20150811.pdf

Vizcardo, H., y Silfredo, J. (2014) *Tipificación de los delitos informáticos patrimoniales en la nueva ley de delitos informáticos Nº 30096, en alma mater Nº 01.* Lima: Universidad Nacional Mayor de San Marcos.

You-lu, L, y Cynthia T. (2016) *Analysis of Computer Crime Characteristics in Taiwan*. Obtenido de https://link.springer.com/chapter/10.1007/11734628_6

Anexo 01 - Matriz de categorización de datos

TÍTULO: Implicancias jurídicas del fraude informático y la protección penal del delito contra el patrimonio Distrito Fiscal de Lima Norte 2020

Línea de investigación: Derecho penal

PLANTEAMIENTO DEL PROBLEMA	PROBLE DE INVESTIGACIÓN	OBJETIVOS DE INVESTIGACIÓN	CATEGORIAS	SUBCATEGORIAS	FUENTE	TÉCNICAS	INSTRUMENTO
En la actualidad, el avance de la tecnología en la informática es uno de los instrumentos más utilizados en las actividades cotidianas que realiza la persona les permite interactuar a través de la plataforma de internet por su versatilidad y automatización; sin embargo, esta herramienta viene siendo aplicado de forma incorrecta debido al incremento de las conductas delictivas por medio de las redes informáticas teniendo como consecuencia la afectación de los derechos patrimoniales de la propiedad privada y del Estado. Esta situación ha motivado que los países de cada estado adopten mecanismos legales a efectos de regular este tipo de conductas, nuestro país no es ajeno a esta problemática ya que en los últimos años se han reportado lo delitos informáticos más frecuentes los cuales son el fraude informático conforme lo señala el artículo 8 de la 30096 modificado por el Artículo 1 de la Ley No 30171, publicada el 10 marzo 2014 y las transacciones ilegales y otras amenazas fueron los más frecuentes todo esto, con la finalidad de proteger derechos patrimoniales. El auge cibercriminal se presenta por el constante avance de la tecnología informática con el aprovechamiento de la globalización de informaciones siendo estas promovidas por las políticas del estado, las empresas privadas, medios de comunicación y entidades financieras con la finalidad de promover la utilización de los recursos digitales que les permite facilitar el intercambio de la información a las personas a través de las plataformas informáticas que les permite acceder con mayor versatilidad y facilidad para que se puedan interrelacionar, comunicarse de manera instantánea, tratativas de negocios nacionales e internacionales, no obstante, el uso de la tecnología informática ha tenido repercusiones negativas en nuestra sociedad, del cual algunos ciudadanos aprovechando de su conocimiento tecnológico han incursionado en la novedosa forma de delinquir a través de las redes informáticas del internet con la finalidad de cometer los delitos contra el patrimonio como es el fraude informático y las transacciones ilegales para apoderarse de los bienes patrimoniales ajenos en beneficio propio de los ciberdelincuentes	**PROBLEMA GENERAL** ¿Cuáles son las implicancias jurídicas del fraude informático y la protección penal del delito contra el patrimonio Distrito Fiscal de Lima Norte 2020?	**OBJETIVO GENERAL** Determinar cuáles son las implicancias jurídicas del fraude informático y la protección penal del delito contra el patrimonio Distrito Fiscal de Lima Norte 2020	**Fraude informático**	Alterar el ingreso de datos de manera ilegal	Distrito Fiscal de Lima Norte	Entrevista Fuentes documentarias Análisis de las normas	Guía de preguntas de entrevista
				Alterar, destruir, suprimir o robar datos.			
				Alterar o borrar archivos			
				Alterar o dar un mal uso a sistemas o software			
	PROBLEMA ESPECÍFICO 01 ¿De qué manera repercute el fraude informático en la protección penal del delito contra el patrimonio Distrito Fiscal de Lima Norte 2020?	**OBJETIVO ESPECIFICO 01** Describir de qué manera repercute el fraude informático en la protección penal del delito contra el patrimonio Distrito Fiscal de Lima Norte 2020	**Protección penal**	Bien Jurídico protegido			
				Tipicidad objetiva			
	PROBLEMA ESPECÍFICO 02 ¿Cómo se relaciona el fraude informático en el delito contra el patrimonio Distrito Fiscal de Lima Norte 2020?	**OBJETIVO ESPECIFICO 02** Describir cómo se relaciona el fraude informático en el delito contra el patrimonio Distrito Fiscal de Lima Norte 2020		Tipicidad subjetiva			
	PROBLEMA ESPECÍFICO 03 ¿De qué manera afecta el fraude informático en el derecho patrimonial del agraviado Distrito Fiscal de Lima Norte 2020?	**OBJETIVO ESPECIFICO 03** Analizar de qué manera afecta el fraude informático en el derecho patrimonial del agraviado Distrito Fiscal de Lima Norte 2020		Pena y circunstancia agravante			

Anexo 02 - Matriz de análisis de ítems

CATEGORIAS	SUBCATEGORIAS	ITEMS
Fraude informático	**Alterar el ingreso de datos de manera ilegal**	**1.** ¿Cuáles son las consecuencias jurídicas de alterar el ingreso de datos de manera ilegal mediante sistemas informáticos en el fraude informático del delito contra el patrimonio? Explique.
	Alterar, destruir, suprimir o robar datos.	2.- ¿Considera usted que alterar, destruir, suprimir o robar datos informáticos puede ser difícil de detectar la conducta ilícita del ciberdelincuente en el delito contra el patrimonio? Explique.
	Alterar o borrar archivos	3.-¿Considera usted que alterar o borrar archivos no autorizadas sobre datos almacenados en los medios informáticos lo puede realizar cualquier persona en los delitos contra el patrimonio? Explique.
	Alterar o dar un mal uso a sistemas o software	4.- ¿Considera usted para alterar o dar un mal uso a sistemas o software con propósitos fraudulentos se requiere de un alto nivel de conocimiento informático en los delitos contra el patrimonio? Explique
Protección penal	**Bien Jurídico protegido**	**5.-** ¿Cuál es el bien jurídico protegido en el fraude informático, desde la perspectiva del derecho a la propiedad del sujeto pasivo en los delitos contra el patrimonio? Explique
	Tipicidad objetiva	**6.-** ¿En qué consiste la tipicidad objetiva del fraude informático en el delito contra el patrimonio? Explique
		7.- ¿Cuáles son los criterios para establecer la tipicidad objetiva en el fraude informático del delito contra el patrimonio? Explique.
	Tipicidad subjetiva	8.- ¿En qué consiste el análisis de la tipicidad subjetiva del fraude informático en los delitos contra el patrimonio? Explique.
		9.- ¿Considera usted que la tipicidad subjetiva en el delito de fraude informático comprende solo el análisis de la conducta dolosa? Explique
	Pena y circunstancia agravante	**10.-** ¿Cuáles son los criterios para establecer la pena y circunstancias agravantes en el delito de fraude informático? Explique

Anexo 03 - Matriz de triangulación
Categoría 01- Fraude informático

Pregunta	E1	E2	E3	E4	E5	E6	E7	E8	Convergencia	Divergencia	Interpretación
1. ¿Cuáles son las consecuencias jurídicas de alterar el ingreso de datos de manera ilegal mediante sistemas informáticos en el fraude informático del delito contra el patrimonio? Explique.	Las consecuencias jurídicas vendrían a ser la sanción penal a imponer al sujeto activo por la violación a través del uso de medios tecnológicos con un fin de menoscabar el patrimonio y perjuicio económico de la víctima.	Es la sanción penal por la conducta ilícita que realiza el imputado al haberle sustraído de manera fraudulenta de una cuenta personal afectado directamente su patrimonio económico de la parte agraviada.	Es el reproche penal Esto cumple la manipulación o actuación de datos programas a través de comportamientos dolosos que en lo general se efectúan en el contexto de operaciones informáticos por los ciberdelincuentes aplicando sus conocimientos de la parte hardware y software del computador o cualquier otro instrumento tecnológico análogo.	Las consecuencias jurídicas son la imposición de una sanción penal por actos que viola el secreto de información por medios informáticos y como consecuencia de ello ocasiona un perjuicio económico en el sujeto pasivo.	Viene a ser la sanción penal en contra del imputado por haber alterado los datos sin la autorización de su propietario, la que en muchos casos es adulterada y borrada del sistema informático	En este aspecto se viola el principio de privacidad reserva de la información almacenada en formato informático y que su alteración, sustracción o vulneración de manera ilegal implica la comisión de un ilícito penal.	Esta conducta constituye acto de ciberdelincuencia que tiene la finalidad de lograr un objetivo ilícito en perjuicio de los bienes patrimoniales del agraviado a través de los medios informáticos.	Por definición al tratarse de un ingreso ilegitimo en sistemas informáticos la consecuencia jurídica sería la de una sanción penal o administrativa conforme la conducta especifica se encuentre tipificada en la norma	Hubo siete entrevistados que señalan que las consecuencias jurídicas de alterar el ingreso de datos de manera ilegal mediante sistemas informáticos implica la sanción penal .	Solo uno de los entrevistados considera que las consecuencias jurídicas de alterar el ingreso de datos de manera ilegal mediante sistemas informáticos merece una sanción penal o administrativa	Según lo expresado por la mayoría de los entrevistados puedo concluir que cuando se altera el ingreso de datos de manera ilegal mediante sistemas informáticos dicha conducta implica una sanción penal en contra de quien lo realiza a través de medios informáticos provocando el perjuicio patrimonial a la parte agraviada.
2. ¿Considera usted que alterar, destruir, suprimir o robar datos informáticos puede ser difícil de detectar la conducta ilícita del ciberdelincuente en el delito contra el	El avance de la ciencia implica nuevos retos para la lucha contra la criminalidad y surge en base a que conforme avanza la ciencia se crean nuevas modalidades delictivas, en este caso el fraude informático,	Detectar delitos informáticos se ha vuelto un problema para nuestra policía, lo vemos a diario en los medios de comunicación con la clonación de tarjeta, así como la sustracción de	En la actualidad la ciberdelincuencia es una nueva forma de delinquir pues conforme avanza el mundo de la ciencia también cambian e innovan en los modos de cometer los delitos lo que universalmente hacen difícil de	Definitivamente sí, porque el medio empleado es algo que no se puede ver en muchos casos es un accionar silencioso que se escuda en los medios tecnológicos que se emplean, no	El detectar este tipo de delitos nos ha demostrado que en muchos casos es difícil de detectar en donde nacen del accionar delictivos, pues aquí se emplean medios tecnológicos	En los delitos tecnológicos debe entenderse que estos por su alta complejidad en el modus operandi es difícil de detectar sobre todo al autor material en consecuencia implica que se tenga que tener una alta preparación por parte de los agentes que lo	La conducta ilícita es difícil de detectar en la medida que se puede confundir con la conducta del usuario y no se encuentra evidencia de la misma, debido a que los ciberdelincu	Considero que dichas conductas serian de difícil detección por el usuario por medio de los sistemas informáticos, ya que la mayoría se limitan al uso de programa de ofimática, mientras que conocimiento de redes y	Seis de los entrevistados consideran que la conducta del ciberdelincuente en los delitos contra el patrimonio del fraude informático es difícil de detectar debido al avance tecnológico	Dos de los entrevistados considera que el accionar delictiva del ciberdelincuente es muy complejo para detectar debido a que innovan en los modos de cometer el delito lo cual requiere de una tecnología moderna para	Según lo expresado por la mayor parte de los entrevistados puedo concluir que el accionar de la conducta delictiva del ciberdelincuente en los delitos contra el patrimonio en la modalidad de fraude

patrimonio ? Explique.	basado en una tecnología cibernética y si la policía no cuenta con los medios idóneos para combatir este tipo de criminalidad no se puede tener éxito en la lucha contra este tipo de delitos.	información confidencial de las personas que en este caso son agraviadas al violárseles su secreto de comunicación.	ser detectados, puesto que se requiere de una tecnología moderna para combatir la ciberdelincuencia.	ocasiona un daño físico, pues este delito se basa principalmente en el medio tecnológico que se emplea.	en muchos casos difíciles de detectar.	van a combatir, en este caso la policía, la cual debe contar con una unidad especializada para poder estar a la par con estos cyber-delincuentes, y para ellos debe de contar con todo el apoyo y la logística necesaria para su cumplimiento.	entes lo realizan por medios informáticos de forma virtual en muchos casos sin dejar rastro de sus actos.	encriptación informático necesarios para causar una conducta pasible de ser calificada como delito informático requieren cierto nivel de especialización mínimo.	y en el modo de operar que estos tienen a través de los medios informáticos.	que unidad especializada de alta tecnología de la Policía Nacional del Perú pueda combatir en la lucha contra el fraude informático.	informático se hace cada vez más difícil de detectar los rastros en el modo en que operan debido a su complejidad valiéndose de su conocimiento en el manejo de los medios informáticos.
3. ¿Considera usted que alterar o borrar archivos no autorizadas sobre datos almacenados en los medios informáticos lo puede realizar cualquier persona en los delitos contra el patrimonio ? Explique.	Se ha descubierto que los que cometen este tipo de delitos cibernéticos, muchos de estos son organizaciones bien formadas y que cuentan con tecnología y gente muy preparada para estos actos criminales.	No, cualquier persona puede hacerlo, se ha visto en los medios de comunicación que en muchos casos son organizaciones criminales las que cometen este tipo de delitos y lamentablemente cada vez son más las que se dedican a este tipo de delitos.	Toda violación de información ya sea procesada ya sea personal o privada puede ser sujeto de estas modalidades delictivas que lógicamente se requiere de personas capacitadas en el mundo de la informática en tal sentido no podría realizar la conducta delictiva cualquier persona que desconozca la informática.	Lamentablemente, este tipo de delitos requiere de personas que tengan un conocimiento pleno en muchos casos especializados en medios informáticos, de tal manera que pueda ingresar a sistemas privados de información y que para lograrlo el agente criminal tiene que tener cierta capacidad para poder cometer este tipo de delitos.	Para poder realizar este tipo de delitos necesariamente el sujeto activo tiene que ser una persona entendida en la materia, pues en este caso es el sistema informático el que se viola, del cual se aprovecha el ciber-delincuente para poder tener un provecho económico.	Actualmente la tecnología cuenta con sistemas de seguridad que creemos en muchos casos son altamente seguros, por tanto aquel que viole este secreto es porque posee un alto grado de conocimiento y capacidad para poder tener acceso a información reservada, y esto se puede hacer teniendo un acto grado de preparación y conocimiento sobre la materia.	No, lo puede realizar cualquier persona dado que por la especialidad se requiere de cierto conocimiento informáticos que se encuentran inmersos en los dispositivos tecnológicos para su manipulación y aplicación correcta con fines ilícitas.	Si bien los delitos informáticos no son delitos especiales, pues en principio pueden ser cometidos por cualquier persona, en la práctica se requiere un nivel de conocimiento y especialización para poder alterar los sistemas informáticos a nivel que puedan causar un perjuicio capaz de subsumirse como delito informático.	seis de los entrevistados concuerdan que el accionar delictivo por medios informáticos no cualquier persona lo puede realizar porque en muchos caos debe conocer de métodos informáticos en base a su alto conocimiento sobre la materia empleando instrumentos informáticos de hardware y software del computador.	Solo dos de los entrevistados considera que que en algunos casos el accionar delictivo pueden ser dirigidas por organizaciones delictivas que cuentan con gente muy preparada en alta tecnología para perpetrar este tipo de delitos, valiéndose de alto conocimiento sobre la materia.	De acuerdo a lo señalado por la mayor parte de los entrevistados puedo concluir que no cualquier persona puede cometer los delitos contra el patrimonio valiéndose de medios informáticos para alterar o borrar archivos no autorizadas sobre datos almacenados en los sistemas informáticos.

4. ¿Considera usted para alterar o dar un mal uso a sistemas o software con propósitos fraudulentos se requiere de un alto nivel de conocimiento informático en los delitos contra el patrimonio ? Explique.	La criminalidad en el mundo en general al parecer siempre se encuentra al avance de nuevas formas de delinquir y crear sobre todo nuevas modalidades de delitos y muchas veces el agente delictivo es una persona que, aunque parezca contradictorio es especializada en la informática para que pueda lograr sus objetivos, para perpetrar los delitos informáticos debe tener un grado de preparación sobre la misma.	Lógicamente que ingresar a un sistema informático requiere cierto nivel de conocimiento para la manipulación de medios tecnológicos y no cualquier persona lo puede hacer, debe tener cierta preparación sobre el tema.	AL respecto necesariamente tiene que tener un nivel de capacidad y preparación para poder tener acceso a sistemas o software por medio de la red y plataforma informática, así como a la base de datos del computador con fines delictuosos en menoscabo de bienes patrimoniales de las personas que se encuentran afectados sus derechos patrimoniales	Sin lugar a duda para ingresar a un sistema privado de información que no es autorizada por su propietario, requiere de un alto nivel de conocimiento sobre el dominio de redes y medios informáticos puesto que no cualquier persona lo puede hacer.	Es base principal saber sobre sistemas de información del sujeto criminal, cuyo conocimiento sobre la materia es su principal herramienta para cometer el hecho delictuoso.	Al respecto necesariamente quien va a cometer un delito informático debe tener un grado de conocimiento para violar secretos de información que le permitan tener acceso a información reservada y que incluso daña el patrimonio del agraviado.	No, necesariamente porque, depende de los actos ilícitos, en algunos casos se requiere de conocimiento básico y en otros más especializados según la magnitud del daño patrimonial causado en perjuicio del agraviado.	Considero que si es necesario un alto nivel de conocimiento informático, que el usuario promedio no posee.	Siete de los entrevistados consideran que se requiere de un alto nivel de conocimiento y especialización para el acceso de sistemas informáticos sobre el fraude informático pudiéndose decir que son especialistas en este tipo de delitos ya que no cualquiera lo puede realizar sin que antes tenga pleno conocimiento sobre la tecnología.	Solo un entrevistado de los ocho considera que no necesariamente se requiere de alto nivel de conocimiento porque depende de los actos ilícitos y de la magnitud del daño causado en algunos casos solo basta que cuente con conocimiento básico en informática.	Según lo manifestado por la mayor parte de los entrevistados puedo concluir que, para alterar o dar un mal uso a sistemas o software con propósitos fraudulentos si se requiere de alto nivel de preparación en la manipulación de sistemas informáticos en los delitos contra el patrimonio.

Matriz de triangulación
Categoría Nº2 - Protección penal

Pregunta	E1	E2	E3	E4	E5	E6	E7	E8	Convergencia	Divergencia	Interpretación
5. ¿Cuál es el bien jurídico protegido en el fraude informático, desde la perspectiva del derecho a la propiedad del sujeto pasivo en los delitos contra el patrimonio ? Explique	El derecho principal que se protege es el secreto de la información que se viola de diversas maneras, ya sea basado, archivos, alterando los mismos causando un perjuicio al agraviado que incluso puede ser el mismo estado a quien se le puede sustraer información confidencial.	Se protege el secreto informativo de aquella información que se tiene en la esfera virtual y que de alguna manera se violada por persona no autorizada, cuyo fin es obtener un beneficio económico en perjuicio de una persona natural, jurídica incluso puede ser el propio Estado cuando se ingresa sin autorización a los sistemas informáticos.	En lo general es el patrimonio al igual que la integridad de datos que se encuentran almacenados a través de un sistema de programas o software que son protegidos con el secreto de seguridad en la cuenta de ahorros ante las entidades bancarias de las personas agraviadas por la conducta ilícita de los ciberdelincuentes.	El bien jurídico protegido en este caso es el patrimonio , respecto a la base de datos informáticos pues este puede ser alterado, borrado o suprimido según el actuar del sujeto activo del delito.	El bien jurídico tutelado es el derecho al patrimonio sobre la base de datos almacenados en el sistema de información en donde se perjudica al sujeto pasivo en el correcto funcionamiento de del sistema informático	Está en el hecho del secreto de información que de alguna manera se guarda a través de medios tecnológicos y del cual se quebranta su seguridad y que perjudica al agraviado.	El bien jurídico tutelado es el patrimonio en relación al derecho de propiedad que tiene el sujeto pasivo sobre la base de datos informáticos y su adecuado funcionamiento de un sistema informático.	El bien jurídico protegido lo configura el patrimonio, el cual es afectado haciendo uso de los sistemas informáticos y digitales.	Cinco de los entrevistados expresan que se protege al patrimonio sobre la base de datos almacenados a través de un sistema de programas o software que son protegidos con el secreto de seguridad en la cuenta de ahorros ante las entidades financieras.	Tres de los entrevistados consideran que el derecho principal que se tutela es el secreto de la información que se viola de diversas maneras, ya sea alterando, sustrayendo borrando archivos, con el objetivo principal de causar perjuicio al sujeto pasivo, incluso puede ser el propio Estado.	De las respuestas obtenidas de los especialistas entrevistados puedo concluir que la mayor parte coinciden al señalar que el bien jurídico protegido en el fraude informático es el derecho al patrimonio sobre datos almacenados por medio de sistemas o software que son protegidos con el secreto de seguridad en la cuenta de ahorros de las personas ante las entidades financieras.
6. ¿En qué consiste la tipicidad objetiva del fraude informático en el delito contra el patrimonio ? Explique	Consiste en analizar si concurren los elementos del tipo penal para determinar la existencia de afectación en el bien patrimonial a través del fraude informático cuando se altera o se borra archivos	Está en el hecho de reservar el secreto que se tiene a través de un sistema la información sobre un determinado patrimonio que el objeto del agente delictivo es precisamente el vulnerar los datos	Consiste en aquella acción humana dirigido con la intención de afectar y burlar el funcionamiento de sistemas de dispositivos informáticos, así como de transmisión de datos con	En este caso radica principalmente en analizar la concurrencia de los elementos del tipo penal que describe la norma respecto al evento delictivo	Consiste en la evaluación de los elementos señaladas en la norma y si estos convergen de manera conjunta como son los sujetos, la conducta y el objeto material del	Consiste en realizar el análisis si reúnen los elementos de la tipicidad conforme a la disposición normativa vigente puesto que, es necesario saber cumple con	Consiste en efectuar el análisis si concurren los elementos del tipo penal prescrito de acuerdo a la normatividad vigente en relación a la conducta del sujeto activo y el objeto material del delito.	La tipicidad objetiva es la actividad externa desarrollada por el sujeto activo con fines fraudulentos del correcto funcionamiento en el sistema informático o de transmisión	Cinco de los entrevistados opinaron que la tipicidad objetiva en el fraude informático consiste en analizar si los elementos de la tipicidad concurren conforme a lo prescrito en la normatividad vigente teniendo en cuenta la	Solo tres de los ocho encuestados consideran que la tipicidad objetiva consiste en aquella acción humana desplegada con la intención de afectar y burlar el funcionamient	Del análisis interpretativo realizado a las respuestas recibidas ese concluye que la mayor parte de los entrevistados coinciden en sus puntos de vista al explicar que la tipicidad objetiva del fraude informático consiste en que el sujeto activo

	y datos por medios informáticos cuya valiosa información solo le afecta a la parte agraviada.	informáticos y con ello lograr su cometido para conseguir el provecho económico a través de supresión o alteración de datos de un sistema informático.	el propósito de obtener el provecho económico con contenido de conducta ilícita.	del fraude informático con el objetivo de establecer la sanción penal del agente criminal.	que necesariamente debe vulnerar alterada o borrada clonación de datos informáticos que acarrea un perjuicio económico para el agraviado.	todo los requisitos exigidos que establece la ley a fin de determinar la conducta desplegada del sujeto activo y la responsabilidad penal.		de datos con el propósito de lograr una ventaja económica con contenido ilícito.	conducta del agente y el objeto material del hecho ilícito.	o de sistemas de dispositivos informáticos, así como de transmisión de datos con el propósito de obtener el provecho económico.	despliegue la conducta con fines fraudulentos respecto al funcionamiento del sistema informático y la transmisión de datos con fines lucrativos a favor del sujeto activo.
7. ¿Cuáles son los criterios para establecer la tipicidad objetiva en el fraude informático del delito contra el patrimonio ? Explique.	Los criterios de la tipicidad objetiva están orientadas a la exigencia en el cumplimiento de los elementos típicos del fraude informático que debe estar prescrito conforme a la norma, teniendo en cuenta la provocación del daño patrimonial a través de la manipulación o alteración de datos o programas de sistemas informáticos al sustraerse del mismo la información que puede afectar el patrimonio del agraviado.	Está en el patrimonio que se daña a través de medios informáticos con conexión a una red informática de internet por los ciberdelincuentes, así como el perjuicio económico que se ocasiona en el patrimonio y que afecta directamente los intereses del agraviado.	Consiste en establecer la conducta ilícita del agente por medio del sistema informático, haciendo el uso de sus conocimientos informáticos que vulnera, altera, clona o suprime los datos de sistema de seguridad informática.	El criterio está en el daño patrimonial y la repercusión que implica el mismo, patrimonio que puede poner incluso en peligro a un estado dependiendo el grado de información confidencial que contenga el mismo.	El criterio consiste en el análisis de los elementos del fraude informático conforme lo señala el artículo 8 del instrumento legal 30096 con realización de las conductas de alteración o supresión de sistema de informática en consecuencia de ello se afecte el derecho patrimonial del agraviado.	En primer orden que la conducta del sujeto activo reúna los elementos del tipo penal debiendo advertir que el mismo afecte daño directamente el patrimonio económico del agraviado.	Al respecto, si la conducta está prevista ley de los delitos informáticos, el cual sea susceptible de, verificar la tipicidad, antijuricidad y la culpabilidad y el reproche penal en contra del sujeto activo.	El criterio sería que el hecho ilícito de la conducta cumpla la configuración del tipo penal y que encuadre dentro del análisis de la tipicidad en el plano informático, es decir las vulneraciones, alteraciones o supresiones de sistema de seguridad informática contravengan la norma teniendo como consecuencia la sanción penal.	Cinco de los entrevistados coinciden en el sentido de que los criterios de la tipicidad objetiva están orientados la exigencia en el cumplimiento de los elementos típicos del fraude informático que debe estar prescrito conforme a la norma, teniendo en cuenta la dimensión del daño patrimonial a través de la manipulación o alteración de datos o programas de sistemas informáticos cause afectación en el patrimonio del agraviado.	Tres de los entrevistados señalan que los criterios para establecer la tipicidad objetiva del fraude informático están consiste en que el agente haciendo uso de sus conocimientos a través de medios informáticos vulnere, altere clone y suprima los datos del sistema informático	Del análisis interpretativo realizado se concluye que los criterios para establecer la tipicidad objetiva en el fraude informático del delito contra el patrimonio debe cumplir las exigencias de los elementos típicos del fraude informático teniendo en cuenta la dimensión del daño patrimonial a través de la manipulación o alteración de datos o programas de sistemas informáticos al sustraerse el mismo la información que afecte el patrimonio del agraviado.

8. ¿En qué consiste el análisis de la tipicidad subjetiva del fraude informático en los delitos contra el patrimonio ? Explique	Esto implica que de alguna el accionar deliberada del ciberdelincuente busca beneficiarse del patrimonio ajeno sobre el fondo de ahorros que se encuentran almacenados dentro de un sistema informático.	Consiste en realizar el análisis de la conducta del agente activo, respecto del modus operandi que condujeron a cometer el hecho delictuoso que se concreta, con el propósito de obtener una ventaja económica de contenido ilícito por medios informáticos introduciendo datos falsos y suprimiendo de datos auténticos.	Es el aspecto subjetivo del accionar del sujeto activo cuando se emplea la tecnología, para realizar maniobras fraudulentas que se puedan hacer por computador a con el fin de obtener el provecho económico que puede lesionar el aspecto económico del agraviado.	La tipicidad subjetiva consiste en el análisis del dolo en la forma en que el agente comete el delito y el medio o instrument o tecnológic o que ha empleado con conocimie nto y voluntad para concretar su cometido del lucro ilícito.	Al respecto consiste en realizar el análisis sobre la intención y la voluntad del agente criminal para cometer el hecho con el propósito de obtener el provecho económico y que dicha acción cause la afectación en agravio de la víctima sobre su bien patrimonial.	Consiste en efectuar el análisis de la conducta a fin de determinar si es doloso o culposa es decir la se valora la intensión que tiene el sujeto activo en cometer el hecho del fraude informático causando la afectación económica a su víctima.	Consiste en establecer el accionar del agente es doloso o culposo es decir se analiza la voluntad y el conocimiento en la realización de la conducta delictiva del fraude informático a través de medios informáticos o en su defecto si la conducta delictiva es culposa o no del agente.	Implica el análisis de la conducta dolosa del sujeto activo el cual se compone de dos elementos el volitivo se refiere al ánimo y la voluntad de querer realizar el hecho ilícito, y el cognitivo este elemento se analiza si el sujeto activo tiene conocimient o respecto del evento delictivo que va a cometer incluso de los alcances o consecuenci as jurídicas.	Seis de los entrevistados considera que la tipicidad subjetiva del fraude informático en los delitos contra el patrimonio, consiste en analizar que la conducta del criminal necesariamente tiene que ser dolosa teniendo en cuenta el elemento volitivo y el cognitivo es decir si el sujeto activo tiene ánimo voluntad y conocimiento respecto del evento delictivo que ha perpetrado.	Dos de los entrevistados consideran que la tipicidad subjetiva del fraude informático en los delitos contra el patrimonio, consiste en analizar la forma y modo de proceder del sujeto activo respecto a la conducta fraudulenta utilizando como herramienta los medios informáticos para lograr su cometido.	Según lo expresado por los entrevistados puedo concluir que la mayoría coincide que la tipicidad subjetiva del fraude informático en los delitos contra el patrimonio, consiste en hacer el estudio de análisis sobre la conducta del criminal es doloso o culposa teniendo en cuenta la presencia o no del elemento volitivo y el cognitivo en el accionar del sujeto activo para consumar el crimen.
9. ¿Considera usted que la tipicidad subjetiva en el delito de fraude informático comprende solo el análisis de la conducta dolosa? Explique	Es el medio empleado para cometer el delito que puede ser a través del sistema informático o que puede servir para que se emplee en borrar, alterar algún tipo de información reservada.	La conducta del agente activo se materializa con lucrar económicame nte para sí o para otro un provecho ilícito y en la a través de los medios empleados para causar el perjuicio patrimonial de un tercero, para tal efecto	Que siendo las actividades directas el uso de técnicas informáticas esta la conducta del sujeto activo que al hacer uso de su conocimient o en sistema s informáticas emplea lo	Considero que sí, porque, quien comete el delito y la forma en que lo concreta utilizando instrument os informátic os ocasionan do daño un	Sí, porque, tiene que existir este elemento como tal, ya que la intención dolosa en cometer el fraude radica principalmen te en el hecho del agente en cuanto a su intención y	Claro, porque tiene que existir este elemento como tal y que la intensión dolosa en cometer el fraude radica precisament e en la conducta de intromisión con ánimo	Si, porque, el dolo excluye la modalidad culposa es decir el agente deberá comprender la falta de autorización para realizar la conducta delictiva con propósito de obtener el provecho económico en perjuicio de un	Conforme lo define la propia ley de delitos informáticos, el delito de fraude informático solo puede ser a título de dolo porque el agente actúa motivado con animus lucrandi, desde el	Siete de los entrevistados opinan que el análisis de la tipicidad subjetiva en el delito de fraude informático considera que solo comprende la conducta dolosa del sujeto activo excluyendo la modalidad culposa porque resultaría atípica	Dos de los entrevistados consideran que la tipicidad subjetiva en el delito de fraude informático considera bajo la misma premisa que solo se verifica el análisis de la conducta dolosa pero con diferentes	Según lo expresado por la mayor parte de los entrevistados puedo concluir que la conducta del sujeto activo en el delito de fraude informático solo debe analizarse el accionar dolosa del imputado respecto a la materialización del delito que

		solo se debe verificar si concurren los elementos del dolo y ella se encuentra en la tipicidad subjetiva como elemento del tipo.	ejecuta pese a tener conocimiento que su accionar tiene como consecuencia la sanción penal.	perjuicio económico y patrimonial en agravio del sujeto pasivo.	voluntad de delinquir y ocasionar un perjuicio económico.	de lucro pues el sujeto activo persigue la obtención de un beneficio económico para sí o para otro en agravio de un tercero.	tercero utilizando instrumentos informáticos para efectuar trasferencias electrónicas de fondos o con la utilización de tarjetas en los cajeros automáticos y acceso ilícitos a ordenadores de redes a través del internet.	inicio hasta la consumación de la conducta ilícita.	debido a que su accionar reviste de intención conocimiento y voluntad en querer realizar el delito para tener acceso ilícito a ordenadores de redes a través del internet y a cuenta de ahorros de tarjetas en los cajeros automáticos.	matices respecto al medio empleado y el modo de operar el crimen	revista intencionalidad, conocimiento y voluntad de querer realizar el delito mediante el uso de ordenadores de redes del sistema informático.
10. ¿Cuáles son los criterios para establecer la pena y circunstancias agravantes en el delito de fraude informático ? Explique	La modalidad del delito, el agente viola el secreto de información que se acopia en medios y plataformas virtuales se ha susceptibles de afectación a su contenido del mismo y que las mismas se han de interés nacional.	El agente con la conducta desplegada cumpla los elementos previstos en la norma, las circunstancias agravante radica en la magnitud del daño patrimonial que se ocasiona, con el resultado de mayor afectación en el patrimonio del Estado y que además dichos bienes estén destinados a programas de apoyo social.	Como todo delito lógicamente este se basa de la gravedad del hecho en cuanto a la información válida que pueda causar un perjuicio económico y de seguridad de un particular como el estado y la calidad del agente.	En cuanto a la pena, son la forma en que se concreta el delito y quienes interviene n en el mismo, y sus circunstancias agravantes estarían en evaluar el nivel de afectación del daño en el patrimonio del agraviado, así como los que interviene n en el mismo para su realización.	En primer orden tiene que verse los elementos constitutivos del caso concreto y las circunstancias agravantes que pueda haber, que en este caso podría ser cuando se afecte directamente el interés nacional y ponga incluso en peligro la seguridad nacional.	Se tiene que observar que reúnan los elementos que conforman el caso concreto, y como circunstancias agravantes se debe advertir que se afecta directamente la información de interés nacional y ponga incluso en peligro la seguridad nacional.	Que la acción de la conducta cumpla con los elementos de tipicidad en la norma, para establecer la pena a imponer de acuerdo a las circunstancias agravantes esto es según la magnitud del daño provocado, en el patrimonio del Estado y que además dichos patrimonios estén orientados en programas de apoyo social.	Como los delitos previstos en el Código Sustantivo los criterios para establecer la pena lo configuran las agravantes genéricas y especificas del artículo 46° de dicho cuerpo legal. Y las circunstancias agravantes se presenta cuando el delito se comete afectando el patrimonio del Estado con fines asistenciales	Siete entrevistados considera que los criterios para establecer la pena y circunstancias agravantes en el delito de fraude informático, radica en la magnitud del daño patrimonial que se ocasiona, a un tercero e incluso al propio Estado respecto a los bienes que estén destinados a programas de apoyo social	Solo dos de los entrevistados considera que el sujeto activo transgrede el secreto de la información que se acopia en medios tecnológicos y plataformas virtuales causando afectación de manera directa respecto a la información de interés nacional y ponga incluso en peligro la seguridad nacional.	Según lo expresado por la mayor parte de los entrevistados puedo concluir que los criterios, radica en la magnitud del daño patrimonial que se ocasiona, a un tercero e incluso al Estado sobre los bienes patrimoniales que estén destinados a programas de apoyo social.

Anexo 04 – Instrumento guía de entrevista

ESCUELA DE POSGRADO
UNIVERSIDAD CÉSAR VALLEJO

TÍTULO: Implicancias Jurídicas del Fraude Informático y la Protección Penal del Delito Contra el Patrimonio Distrito Fiscal de Lima Norte 2020

ENTREVISTADO:

Cargo/Profesión/Grado académico:

FECHA:

INDICACIONES: *El presente instrumento forma parte de una investigación jurídica. Se le ruega contestar de forma objetiva. Recuerde que no hay respuestas correctas o incorrectas, su participación y experiencia es lo que se valorará.*

CATEGORIA N°01

FRAUDE INFORMÁTICO

1. ¿Cuáles son las consecuencias jurídicas de alterar el ingreso de datos de manera ilegal mediante sistemas informáticos en el fraude informático del delito contra el patrimonio? Explique.

……

……

……

……

2. ¿Considera usted que alterar, destruir, suprimir o robar datos informáticos puede ser difícil de detectar la conducta ilícita del ciberdelincuente en el delito contra el patrimonio? Explique.

……

……

……

……

3. ¿Considera usted que alterar o borrar archivos no autorizadas sobre datos almacenados en los medios informáticos lo puede realizar cualquier persona en los delitos contra el patrimonio? Explique.

……

……

……

……

4. ¿Considera usted para alterar o dar un mal uso a sistemas o software con propósitos fraudulentos se requiere de un alto nivel de conocimiento informático en los delitos contra el patrimonio? Explique.

……

……

……

……

CATEGORIA N° 02

PROTECCIÓN PENAL

5. ¿Cuál es el bien jurídico protegido en el fraude informático, desde la perspectiva del derecho a la propiedad del sujeto pasivo en los delitos contra el patrimonio? Explique

……

……

……

……

6. ¿En qué consiste la tipicidad objetiva del fraude informático en el delito contra el patrimonio? Explique

……

……

……

……

7. ¿Cuáles son los criterios para establecer la tipicidad objetiva en el fraude informático del delito contra el patrimonio? Explique.

……

……

……

……

8. ¿En qué consiste el análisis de la tipicidad subjetiva del fraude informático en los delitos contra el patrimonio? Explique.

……

……

……

……

9. ¿Considera usted que la tipicidad subjetiva en el delito de fraude informático comprende solo el análisis de la conducta dolosa? Explique

……

……

……

……

10. ¿Cuáles son los criterios para establecer la pena y circunstancias agravantes en el delito de fraude informático? Explique

……

……

……

……

Nombre del entrevistado	Sello y Firma

Anexo 05 – Escaneo de entrevistas

GUÍA DE ENTREVISTA

TÍTULO: Implicancias jurídicas del fraude informático y la protección penal del delito contra el patrimonio Distrito Fiscal de Lima Norte 2020

ENTREVISTADO: Dra. Ana María Revilla Palacios

Cargo: Juez del Quinto Juzgado Especializado en lo Penal de la Corte Superior de Justicia de Lima Norte

Profesión: Abogada

Grado académico: Magister

FECHA: 07 /01 /2021

INDICACIONES: *El presente instrumento forma parte de una investigación jurídica. Se le ruega contestar de forma objetiva. Recuerde que no hay respuestas correctas o incorrectas, su participación y experiencia es lo que se valorará.*

CATEGORIA N°01

FRAUDE INFORMÁTICO

1. ¿Cuáles son las consecuencias jurídicas de alterar el ingreso de datos de manera ilegal mediante sistemas informáticos en el fraude informático del delito contra el patrimonio? Explique.

   Las consecuencias jurídicas vendrían a ser la sanción penal a imponer al sujeto activo por la violación a través del uso de medios tecnológicos con un fin de menoscabar el patrimonio y perjuicio económico de la víctima.

2. ¿Considera usted que alterar, destruir, suprimir o robar datos informáticos puede ser difícil de detectar la conducta ilícita del ciberdelincuente en el delito contra el patrimonio? Explique.

   El avance de la ciencia implica nuevos retos para la lucha contra la criminalidad y surge en base a que conforme avanza la ciencia se crean nuevas modalidades delictivas, en este caso el fraude informático, basado en una tecnología cibernética y si la policía no cuenta con los medios idóneos para combatir este tipo de criminalidad no se puede tener éxito en la lucha contra este tipo de delitos.

3. ¿Considera usted que alterar o borrar archivos no autorizadas sobre datos almacenados en los medios informáticos lo puede realizar cualquier persona en los delitos contra el patrimonio? Explique.

   Se ha descubierto que los que cometen este tipo de delitos cibernéticos, muchos de estos son organizaciones bien formadas y que cuentan con tecnología y gente muy preparada para estos actos criminales.

4. ¿Considera usted para alterar o dar un mal uso a sistemas o software con propósitos fraudulentos se requiere de un alto nivel de conocimiento informático en los delitos contra el patrimonio? Explique.

   La criminalidad en el mundo en general al parecer siempre se encuentra al avance de nuevas formas de delinquir y crear sobre todo nuevas modalidades de delitos y muchas veces el agente delictivo es una persona que, aunque parezca contradictorio es especializada en la informática para que pueda lograr sus objetivos, para perpetrar los delitos informáticos debe tener un grado de preparación sobre la misma.

CATEGORIA N° 02

PROTECCIÓN PENAL

5. ¿Cuál es el bien jurídico protegido en el fraude informático, desde la perspectiva del derecho a la propiedad del sujeto pasivo en los delitos contra el patrimonio? Explique

   El derecho principal que se protege es el secreto de la información que se viola de diversas maneras, ya sea basado, archivos, alterando los mismos causando un perjuicio al agraviado que incluso puede ser el mismo estado a quien se le puede sustraer información confidencial.

6. ¿En qué consiste la tipicidad objetiva del fraude informático en el delito contra el patrimonio? Explique

   Consiste en analizar si concurren los elementos del tipo penal para determinar la existencia de afectación en el bien patrimonial a través del fraude informático cuando se altera o se borra archivos y datos por medios informáticos cuya valiosa información solo le afecta a la parte agraviada.

7. ¿Cuáles son los criterios para establecer la tipicidad objetiva en el fraude informático del delito contra el patrimonio? Explique.

   Los criterios de la tipicidad objetiva están orientadas a la exigencia en el cumplimiento de los elementos típicos del fraude informático que debe estar prescrito conforme a la norma, teniendo en cuenta la provocación del daño patrimonial a través de la manipulación o alteración de datos o programas de sistemas informáticos al sustraerse del mismo la información que puede afectar el patrimonio del agraviado

8. ¿En qué consiste el análisis de la tipicidad subjetiva del fraude informático en los delitos contra el patrimonio? Explique.

   Esto implica que de alguna el accionar deliberada del ciberdelincuente busca beneficiarse del patrimonio ajeno sobre el fondo de ahorros que se encuentran almacenados dentro de un sistema informático.

9. ¿Considera usted que la tipicidad subjetiva en el delito de fraude informático comprende solo el análisis de la conducta dolosa? Explique

   Es el medio empleado para cometer el delito que puede ser a través del sistema informático o que puede servir para que se emplee en borrar, alterar algún tipo de información reservada.

10. ¿Cuáles son los criterios para establecer la pena y circunstancias agravantes en el delito de fraude informático? Explique

    La modalidad del delito, el agente viola el secreto de información que se acopia en medios y plataformas virtuales se ha susceptibles de afectación a su contenido del mismo y que las mismas se han de interés nacional.

Nombre del entrevistado	Sello y Firma
Dra. Ana María Revilla Palacios	María Del Carmen Ampuero Quinteros FISCAL ADJUNTA PROVINCIAL (P) PRIMERA FISCALÍA PROVINCIAL PENAL CORPORATIVA DE CARABAYLLO LIMA NORTE

GUÍA DE ENTREVISTA

TÍTULO: Implicancias jurídicas del fraude informático y la protección penal del delito contra el patrimonio Distrito Fiscal de Lima Norte 2020

ENTREVISTADO: Dra. Cris Lloly Ruiz Cárdenas

Cargo: Jueza Especializada Supernumeraria del Juzgado de Investigación Preparatoria Transitoria de Ancón y Santa Rosa de la Corte Superior de Justicia de Ventanilla.

Profesión: Abogada

Grado académico: Magister

FECHA: 08/01/2021

INDICACIONES: *El presente instrumento forma parte de una investigación jurídica. Se le ruega contestar de forma objetiva. Recuerde que no hay respuestas correctas o incorrectas, su participación y experiencia es lo que se valorará.*

CATEGORIA N°01

FRAUDE INFORMÁTICO

1. ¿Cuáles son las consecuencias jurídicas de alterar el ingreso de datos de manera ilegal mediante sistemas informáticos en el fraude informático del delito contra el patrimonio? Explique.

   Es la sanción penal por la conducta ilícita que realiza el imputado al haberle sustraído de manera fraudulenta de una cuenta personal afectado directamente su patrimonio económico de la parte agraviada.

2. ¿Considera usted que alterar, destruir, suprimir o robar datos informáticos puede ser difícil de detectar la conducta ilícita del ciberdelincuente en el delito contra el patrimonio? Explique.

   Detectar delitos informáticos se ha vuelto un problema para nuestra policía, lo vemos a diario en los medios de comunicación con la clonación de tarjeta, así como la sustracción de información confidencial de las personas que en este caso son agraviadas al violárseles su secreto de comunicación.

3. ¿Considera usted que alterar o borrar archivos no autorizadas sobre datos almacenados en los medios informáticos lo puede realizar cualquier persona en los delitos contra el patrimonio? Explique.

   No, cualquier persona puede hacerlo, se ha visto en los medios de comunicación que en muchos casos son organizaciones criminales las que cometen este tipo de delitos y lamentablemente cada vez son más las que se dedican a este tipo de delitos.

4. ¿Considera usted para alterar o dar un mal uso a sistemas o software con propósitos fraudulentos se requiere de un alto nivel de conocimiento informático en los delitos contra el patrimonio? Explique.

   Lógicamente que ingresar a un sistema informático requiere cierto nivel de conocimiento para la manipulación de medios tecnológicos y no cualquier persona lo puede hacer, debe tener cierta preparación sobre el tema.

CATEGORIA N° 02

PROTECCIÓN PENAL

5. ¿Cuál es el bien jurídico protegido en el fraude informático, desde la perspectiva del derecho a la propiedad del sujeto pasivo en los delitos contra el patrimonio? Explique

   Se protege el secreto informativo de aquella información que se tiene en la esfera virtual y que de alguna manera se violada por persona no autorizada, cuyo fin es obtener un beneficio económico en perjuicio de una persona natural, jurídica incluso puede ser el propio Estado cuando se ingresa sin autorización a los sistemas informáticos.

6. ¿En qué consiste la tipicidad objetiva del fraude informático en el delito contra el patrimonio? Explique

   Está en el hecho de reservar el secreto que se tiene a través de un sistema la información sobre un determinado patrimonio que el objeto del agente delictivo es precisamente el vulnerar los datos informáticos y con ello lograr su cometido para conseguir el provecho económico a través de supresión o alteración de datos de un sistema informático.

7. ¿Cuáles son los criterios para establecer la tipicidad objetiva en el fraude informático del delito contra el patrimonio? Explique.

Está en el patrimonio que se daña a través de medios informáticos con conexión a una red informática de internet por los ciberdelincuentes, así como el perjuicio económico que se ocasiona en el patrimonio y que afecta directamente los intereses del agraviado.

8. ¿En qué consiste el análisis de la tipicidad subjetiva del fraude informático en los delitos contra el patrimonio? Explique.

   Consiste en realizar el análisis de la conducta del agente activo, respecto del modus operandi que condujeron a cometer el hecho delictuoso que se concreta, con el propósito de obtener una ventaja económica de contenido ilícito por medios informáticos introduciendo datos falsos y suprimiendo de datos auténticos.

9. ¿Considera usted que la tipicidad subjetiva en el delito de fraude informático comprende solo el análisis de la conducta dolosa? Explique

   La conducta del agente activo se materialización lucrar económicamente para sí o para otro un provecho ilícito y en la a través de los medios empleados para causar el perjuicio patrimonial de un tercero, para tal efecto solo se debe verificar si concurren los elementos del dolo y ella se encuentra en la tipicidad subjetiva como elemento del tipo.

10. ¿Cuáles son los criterios para establecer la pena y circunstancias agravantes en el delito de fraude informático? Explique

    El agente con la conducta desplegada cumpla los elementos previstos en la norma, la circunstancia agravante radica en la magnitud del daño patrimonial que se ocasiona, con el resultado de mayor afectación en el patrimonio del Estado y que además dichos bienes estén destinados a programas de apoyo social.

Nombre del entrevistado	Sello y Firma
Dra. Cris Lloly Ruiz Cárdenas	PODER JUDICIAL DEL PERÚ DRA. CRIS LLOLY RUIZ CARDENAS JUEZA ESPECIALIZADA SUPERNUMERARIA CORTE SUPERIOR DE JUSTICIA DE VENTANILLA

GUÍA DE ENTREVISTA

TÍTULO: Implicancias jurídicas del fraude informático y la protección penal del delito contra el patrimonio Distrito Fiscal de Lima Norte 2020

ENTREVISTADO: Dr. Alejandro Sánchez Crisólogo.

Cargo: Fiscal Ajunto Provincial, Distrito Fiscal de Lima Norte.

Profesión: Abogado

Grado académico: Magister

FECHA: 22/12/2020

INDICACIONES: *El presente instrumento forma parte de una investigación jurídica. Se le ruega contestar de forma objetiva. Recuerde que no hay respuestas correctas o incorrectas, su participación y experiencia es lo que se valorará.*

CATEGORIA N°01

FRAUDE INFORMÁTICO

1. ¿Cuáles son las consecuencias jurídicas de alterar el ingreso de datos de manera ilegal mediante sistemas informáticos en el fraude informático del delito contra el patrimonio? Explique.

   Es el reproche penal Esto cumple la manipulación o actuación de datos programas a través de comportamientos dolosos que en lo general se efectúan en el contexto de operaciones informáticos por los ciberdelincuentes aplicando sus conocimientos de la parte hardware y software del computador o cualquier otro instrumento tecnológico análogo.

2. ¿Considera usted que alterar, destruir, suprimir o robar datos informáticos puede ser difícil de detectar la conducta ilícita del ciberdelincuente en el delito contra el patrimonio? Explique.

   En la actualidad la ciberdelincuencia es una nueva forma de delinquir pues conforme avanza el mundo de la ciencia también cambian e innovan en los modos de cometer los delitos lo que universalmente hacen difícil de ser detectados, puesto que se requiere de una tecnología moderna para combatir la ciberdelincuencia.

3. ¿Considera usted que alterar o borrar archivos no autorizadas sobre datos almacenados en los medios informáticos lo puede realizar cualquier persona en los delitos contra el patrimonio? Explique.

   Toda violación de información ya sea procesada ya sea personal o privada puede ser sujeto de estas modalidades delictivas que lógicamente se requiere de personas capacitadas en el mundo de la informática en tal sentido no podría realizar la conducta delictiva cualquier persona que desconozca la informática.

4. ¿Considera usted para alterar o dar un mal uso a sistemas o software con propósitos fraudulentos se requiere de un alto nivel de conocimiento informático en los delitos contra el patrimonio? Explique.

   AL respecto necesariamente tiene que tener un nivel de capacidad y preparación para poder tener acceso a sistemas o software por medio de la red y plataforma informática, así como a la base de datos del computador con fines delictuosos en menoscabo de bienes patrimoniales de las personas que se encuentran afectados sus derechos patrimoniales

CATEGORIA N° 02

PROTECCIÓN PENAL

5. ¿Cuál es el bien jurídico protegido en el fraude informático, desde la perspectiva del derecho a la propiedad del sujeto pasivo en los delitos contra el patrimonio? Explique

   En lo general es el patrimonio al igual que la integridad de datos que se encuentran almacenados a través de un sistema de programas o software que son protegidos con el secreto de seguridad en la cuenta de ahorros ante las entidades bancarias de las personas agraviadas por la conducta ilícita de los ciberdelincuentes.

6. ¿En qué consiste la tipicidad objetiva del fraude informático en el delito contra el patrimonio? Explique

   Consiste en aquella acción humana dirigido con la intención de afectar y burlar el funcionamiento de sistemas de dispositivos informáticos, así como de transmisión de datos con el propósito de obtener el provecho económico con contenido de conducta ilícita.

7. ¿Cuáles son los criterios para establecer la tipicidad objetiva en el fraude informático del delito contra el patrimonio? Explique.

Consiste en establecer la conducta ilícita del agente por medio del sistema informático, haciendo el uso de sus conocimientos informáticos que vulnera, altera, clona o suprime los datos de sistema de seguridad informática.

8. ¿En qué consiste el análisis de la tipicidad subjetiva del fraude informático en los delitos contra el patrimonio? Explique.

   Es el aspecto subjetivo del accionar del sujeto activo cuando se emplea la tecnología, para realizar maniobras fraudulentas que se puedan hacer por computadora con el fin de obtener el provecho económico que puede lesionar el aspecto económico del agraviado.

9. ¿Considera usted que la tipicidad subjetiva en el delito de fraude informático comprende solo el análisis de la conducta dolosa? Explique

   Que siendo las actividades directas el uso de técnicas informáticas esta la conducta del sujeto activo que al hacer uso de su conocimiento en sistema s informáticas emplealo ejecuta pese a tener conocimiento que su accionar tiene como consecuencia la sanción penal.

10. ¿Cuáles son los criterios para establecer la pena y circunstancias agravantes en el delito de fraude informático? Explique

    Como todo delito lógicamente este se basa de la gravedad del hecho en cuanto a la información válida que pueda causar un perjuicio económico y de seguridad de un particular como el estado y la calidad del agente.

Nombre del entrevistado	Sello y Firma
Dr. Alejandro Sánchez Crisólogo.	

GUÍA DE ENTREVISTA

TÍTULO: Implicancias jurídicas del fraude informático y la protección penal del delito contra el patrimonio Distrito Fiscal de Lima Norte 2020

ENTREVISTADO: Dra. María del Carmen Ampuero Quinteros
Cargo: Fiscal Adjunta del Provincial Distrito Fiscal de Lima Norte.
Profesión: Abogada
Grado académico: Magister
FECHA: 22/12/2020

INDICACIONES: *El presente instrumento forma parte de una investigación jurídica. Se le ruega contestar de forma objetiva. Recuerde que no hay respuestas correctas o incorrectas, su participación y experiencia es lo que se valorará.*

CATEGORIA N°01

FRAUDE INFORMÁTICO

1. ¿Cuáles son las consecuencias jurídicas de alterar el ingreso de datos de manera ilegal mediante sistemas informáticos en el fraude informático del delito contra el patrimonio? Explique.

   Las consecuencias jurídicas son la imposición de una sanción penal por actos que viola el secreto de información por medios informáticos y comoconsecuencia de ello ocasiona un perjuicio económico en el sujeto pasivo.

2. ¿Considera usted que alterar, destruir, suprimir o robar datos informáticos puede ser difícil de detectar la conducta ilícita del ciberdelincuente en el delito contra el patrimonio? Explique.

   Definitivamente sí, porque el medio empleado es algo que no se puede ver en muchos casos es un accionar silencioso que se escuda en los medios tecnológicos que se emplean, no ocasiona un daño físico, pues este delito se basa principalmente en el medio tecnológico que se emplea.

3. ¿Considera usted que alterar o borrar archivos no autorizadas sobre datos almacenados en los medios informáticos lo puede realizar cualquier persona en los delitos contra el patrimonio? Explique.

Lamentablemente, este tipo de delitos requiere de personas que tengan un conocimiento pleno en muchos casos especializados en medios informáticos, de tal manera que pueda ingresar a sistemas privados de información y que para lograrlo el agente criminal tiene que tener cierta capacidad para poder cometer este tipo de delitos.

4. ¿Considera usted para alterar o dar un mal uso a sistemas o software con propósitos fraudulentos se requiere de un alto nivel de conocimiento informático en los delitos contra el patrimonio? Explique.

   Sin lugar a duda para ingresar a un sistema privado de información que no es autorizada por su propietario, requiere de un alto nivel de conocimiento sobre el dominio de redes y medios informáticos puesto que no cualquier persona lo puede hacer.

CATEGORIA N° 02

PROTECCIÓN PENAL

5. ¿Cuál es el bien jurídico protegido en el fraude informático, desde la perspectiva del derecho a la propiedad del sujeto pasivo en los delitos contra el patrimonio? Explique

   El bien jurídico protegido en este caso es el patrimonio, respecto a la base de datos informáticos pues este puede ser alterado, borrado o suprimido según el actuar del sujeto activo del delito.

6. ¿En qué consiste la tipicidad objetiva del fraude informático en el delito contra el patrimonio? Explique

   En este caso radica principalmente en analizar la concurrencia de los elementos del tipo penal que describe la norma respecto al evento delictivo del fraude informático con el objetivo de establecer la sanción penal del agente criminal.

7. ¿Cuáles son los criterios para establecer la tipicidad objetiva en el fraude informático del delito contra el patrimonio? Explique.

   El criterio está en el daño patrimonial y la repercusión que implica el mismo, patrimonio que puede poner incluso en peligro a un estado dependiendo el grado de información confidencial que contenga el mismo.

8. ¿En qué consiste el análisis de la tipicidad subjetiva del fraude informático en los delitos contra el patrimonio? Explique.

La tipicidad subjetiva consiste en el análisis del dolo en la forma en que el agente comete el delito y el medio o instrumento tecnológico que ha empleado con conocimiento y voluntad para concretar su cometido del lucro ilícito.

9. ¿Considera usted que la tipicidad subjetiva en el delito de fraude informático comprende solo el análisis de la conducta dolosa? Explique

Considero que sí, porque, quien comete el delito y la forma en que lo concreta utilizando instrumentos informáticos ocasionando daño un perjuicio económico y patrimonial en agravio del sujeto pasivo.

10. ¿Cuáles son los criterios para establecer la pena y circunstancias agravantes en el delito de fraude informático? Explique

En cuanto a la pena, son la forma en que se concreta el delito y quienes intervienen en el mismo, y sus circunstancias agravantes estarían en evaluar el nivel de afectación del daño en el patrimonio del agraviado, así como los que intervienen en el mismo para su realización.

Nombre del entrevistado	Sello y Firma
Dra. María del Carmen Ampuero Quinteros	

GUÍA DE ENTREVISTA

TÍTULO: Implicancias jurídicas del fraude informático y la protección penal del delito contra el patrimonio Distrito Fiscal de Lima Norte 2020

ENTREVISTADO: Dra. Paola Guerra Arauco

Cargo: Fiscal Adjunta Provincial del Distrito Fiscal de Lima Norte.

Profesión: Abogada

Grado académico: Magister

FECHA: 28/12/2020

INDICACIONES: *El presente instrumento forma parte de una investigación jurídica. Se le ruega contestar de forma objetiva. Recuerde que no hay respuestas correctas o incorrectas, su participación y experiencia es lo que se valorará.*

CATEGORIA N°01

FRAUDE INFORMÁTICO

1. ¿Cuáles son las consecuencias jurídicas de alterar el ingreso de datos de manera ilegal mediante sistemas informáticos en el fraude informático del delito contra el patrimonio? Explique.

   Viene a ser la sanción penal en contra del imputado por haber alterado los datos sin la autorización de su propietario, la que en muchos casos es adulterada y borrada del sistema informático.

2. ¿Considera usted que alterar, destruir, suprimir o robar datos informáticos puede ser difícil de detectar la conducta ilícita del ciberdelincuente en el delito contra el patrimonio? Explique.

   El detectar este tipo de delitos nos ha demostrado que en muchos casos es difícil de detectar en donde nacen del accionar delictivos, pues aquí se emplean medios tecnológicos en muchos casos difíciles de detectar.

3. ¿Considera usted que alterar o borrar archivos no autorizadas sobre datos almacenados en los medios informáticos lo puede realizar cualquier persona en los delitos contra el patrimonio? Explique.

Para poder realizar este tipo de delitos necesariamente el sujeto activo tiene que ser una persona entendida en la materia, pues en este caso es el sistema informático el que se viola, del cual se aprovecha el ciber-delincuente para poder tener un provecho económico.

4. ¿Considera usted para alterar o dar un mal uso a sistemas o software con propósitos fraudulentos se requiere de un alto nivel de conocimiento informático en los delitos contra el patrimonio? Explique.

   Es base principal saber sobre sistemas de información del sujeto criminal, cuyo conocimiento sobre la materia es su principal herramienta para cometer el hecho delictuoso.

CATEGORIA N° 02

PROTECCIÓN PENAL

5. ¿Cuál es el bien jurídico protegido en el fraude informático, desde la perspectiva del derecho a la propiedad del sujeto pasivo en los delitos contra el patrimonio? Explique

   El bien jurídico tutelado es el derecho al patrimonio sobre la base de datos almacenados en el sistema de información en donde se perjudica al sujeto pasivo en el correcto funcionamiento de del sistema informático.

6. ¿En qué consiste la tipicidad objetiva del fraude informático en el delito contra el patrimonio? Explique

   Consiste en la evaluación de los elementos señaladas en la norma y si estos convergen de manera conjunta como son los sujetos, la conducta y el objeto materialdel que necesariamente debe vulnerar alterada o borrada clonación de datos informáticos que acarrea un perjuicio económico para el agraviado.

7. ¿Cuáles son los criterios para establecer la tipicidad objetiva en el fraude informático del delito contra el patrimonio? Explique.

   El criterio consiste en el análisis de los elementos del fraude informático conforme lo señala el artículo 8 del instrumento legal 30096 con realización de las conductas de, alteración o supresión de sistema de informática en consecuencia de ello se afecte el derecho patrimonial del agraviado.

8. ¿En qué consiste el análisis de la tipicidad subjetiva del fraude informático en los delitos contra el patrimonio? Explique.

Al respecto consiste en realizar el análisis sobre la intención y la voluntad del agente criminal para cometer el hecho con el propósito de obtener el provecho económico y que dicha acción cause la afectación en agravio de la víctima sobre su bien patrimonial.

9. ¿Considera usted que la tipicidad subjetiva en el delito de fraude informático comprende solo el análisis de la conducta dolosa? Explique

Sí, porque, tiene que existir este elemento como tal, ya que la intención dolosa en cometer el fraude radica principalmente en el hecho del agente en cuanto a su intención y voluntad de delinquir y ocasionar un perjuicio económico.

10. ¿Cuáles son los criterios para establecer la pena y circunstancias agravantes en el delito de fraude informático? Explique

En primer orden tiene que verse los elementos constitutivos del caso concreto y las circunstancias agravantes que pueda haber, que en este caso podría ser cuando se afecte directamente el interés nacional y ponga incluso en peligro la seguridad nacional.

Nombre del entrevistado	Sello y Firma
Dra. Paola Guerra Arauco	PAOLA GUERRA ARAUCO Fiscal Adjunta Provincial Distrito Fiscal de Lima Norte

GUÍA DE ENTREVISTA

TÍTULO: Implicancias jurídicas del fraude informático y la protección penal del delito contra el patrimonio Distrito Fiscal de Lima Norte 2020

ENTREVISTADO: Dr. Zebastián Zegarra Gonzales

Cargo: Asistente en función Fiscal Distrito Fiscal de Lima Norte.

Profesión: Abogado

Grado académico: Magister

FECHA: 06/01/2021

INDICACIONES: *El presente instrumento forma parte de una investigación jurídica. Se le ruega contestar de forma objetiva. Recuerde que no hay respuestas correctas o incorrectas, su participación y experiencia es lo que se valorará.*

CATEGORIA N°01

FRAUDE INFORMÁTICO

1. ¿Cuáles son las consecuencias jurídicas de alterar el ingreso de datos de manera ilegal mediante sistemas informáticos en el fraude informático del delito contra el patrimonio? Explique.

   En este aspecto se viola el principio de privacidad reserva de la información almacenada en formato informático y que su alteración, sustracción o vulneración de manera ilegal implica la comisión de un ilícito penal.

2. ¿Considera usted que alterar, destruir, suprimir o robar datos informáticos puede ser difícil de detectar la conducta ilícita del ciberdelincuente en el delito contra el patrimonio? Explique.

   En los delitos tecnológicos debe entenderse que estos por su alta complejidad en el modus operandi es difícil de detectar sobre todo al autor material en consecuencia implica que se tenga que tener una alta preparación por parte de los agentes que lo van a combatir, en este caso la policía, la cual debe contar con una unidad especializada para poder estar a la par con estos cyber-delincuentes, y para ellos debe de contar con todo el apoyo y la logística necesaria para su cumplimiento.

3. ¿Considera usted que alterar o borrar archivos no autorizadas sobre datos almacenados en los medios informáticos lo puede realizar cualquier persona en los delitos contra el patrimonio? Explique.

   Actualmente la tecnología cuenta con sistemas de seguridad que creemos en muchos casos son altamente seguros, por tanto aquel que viole este secreto es porque posee un alto grado de conocimiento y capacidad para poder tener acceso a información reservada, y esto se puede hacer teniendo un acto grado de preparación y conocimiento sobre la materia.

4. ¿Considera usted para alterar o dar un mal uso a sistemas o software con propósitos fraudulentos se requiere de un alto nivel de conocimiento informático en los delitos contra el patrimonio? Explique.

   Al respecto necesariamente quien va a cometer un delito informático debe tener un grado de conocimiento para violar secretos de información que le permitan tener acceso a información reservada y que incluso daña el patrimonio del agraviado.

CATEGORIA N° 02

PROTECCIÓN PENAL

5. ¿Cuál es el bien jurídico protegido en el fraude informático, desde la perspectiva del derecho a la propiedad del sujeto pasivo en los delitos contra el patrimonio? Explique

   Está en el hecho del secreto de información que de alguna manera se guarda a través de medios tecnológicos y del cual se quebranta su seguridad y que perjudica al agraviado.

6. ¿En qué consiste la tipicidad objetiva del fraude informático en el delito contra el patrimonio? Explique

   Consiste en realizar el análisis si reúnen los elementos de la tipicidad conforme a la disposición normativa vigente puesto que, es necesario saber cumple con todo los requisitos exigidos que establece la leya fin de determinar la conducta desplegada del sujeto activo y la responsabilidad penal.

7. ¿Cuáles son los criterios para establecer la tipicidad objetiva en el fraude informático del delito contra el patrimonio? Explique.

   En primer orden que la conducta del sujeto activo reúna los elementos del tipo penal debiendo advertir que el mismo afecte daño directamente el patrimonio económico del agraviado.

8. ¿En qué consiste el análisis de la tipicidad subjetiva del fraude informático en los delitos contra el patrimonio? Explique.

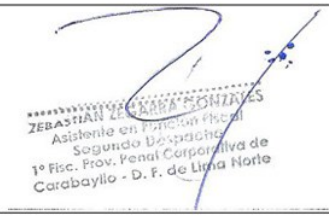
   Consiste en efectuar el análisis de la conducta a fin de determinar si es doloso o culposa es decir la se valora la intensión que tiene el sujeto activo en cometer el hecho del fraude informático causando la afectación económico a su víctima.

9. ¿Considera usted que la tipicidad subjetiva en el delito de fraude informático comprende solo el análisis de la conducta dolosa? Explique

   Claro, porque tiene que existir este elemento como tal y que la intensión dolosa en cometer el fraude radica precisamente en la conducta de intromisión con ánimo de lucro pues el sujeto activo persigue la obtención de un beneficio económico para sí o para otro en agravio de un tercero.

10. ¿Cuáles son los criterios para establecer la pena y circunstancias agravantes en el delito de fraude informático? Explique

    Se tiene que observar que reúnan los elementos que conforman el caso concreto, y como circunstancias agravantes se debe advertir que se afecta directamente la información de interés nacional y ponga incluso en peligro la seguridad nacional.

Nombre del entrevistado	Sello y Firma
Dr. Zebastián Zegarra Gonzales	

GUÍA DE ENTREVISTA

TÍTULO: Implicancias jurídicas del fraude informático y la protección penal del delito contra el patrimonio Distrito Fiscal de Lima Norte 2020

ENTREVISTADO: Dr. Fredy Ramírez Bailón

Cargo: Asistente en función Fiscal del Distrito Fiscal de Lima Norte.

Profesión: Abogado

Grado académico: Magister

FECHA: 23/12/2020

INDICACIONES: *El presente instrumento forma parte de una investigación jurídica. Se le ruega contestar de forma objetiva. Recuerde que no hay respuestas correctas o incorrectas, su participación y experiencia es lo que se valorará.*

CATEGORIA N°01

FRAUDE INFORMÁTICO

1. ¿Cuáles son las consecuencias jurídicas de alterar el ingreso de datos de manera ilegal mediante sistemas informáticos en el fraude informático del delito contra el patrimonio? Explique.

   Esta conducta constituye acto de ciberdelincuencia que tiene la finalidad de lograr un objetivo ilícito en perjuicio de los bienes patrimoniales del agraviado a través de los medios informáticos.

2. ¿Considera usted que alterar, destruir, suprimir o robar datos informáticos puede ser difícil de detectar la conducta ilícita del ciberdelincuente en el delito contra el patrimonio? Explique.

   La conducta ilícita es difícil de detectar en la medida que se puede confundir con la conducta del usuario y no se encuentra evidencia de la misma, debido a que los ciberdelincuentes lo realizan por medios informáticos de forma virtual en muchos casos sin dejar rastro de sus actos.

3. ¿Considera usted que alterar o borrar archivos no autorizadas sobre datos almacenados en los medios informáticos lo puede realizar cualquier persona en los delitos contra el patrimonio? Explique.

No, lo puede realizar cualquier persona dado que por la especialidad se requiere de cierto conocimiento informáticos que se encuentran inmersos en los dispositivos tecnológicos para su manipulación y aplicación correcta con fines ilícitas.

4. ¿Considera usted para alterar o dar un mal uso a sistemas o software con propósitos fraudulentos se requiere de un alto nivel de conocimiento informático en los delitos contra el patrimonio? Explique.

   No, necesariamente porque, depende de los actos ilícitos, en algunos casos se requiere de conocimiento básico y en otros más especializados según la magnitud del daño patrimonial causado en perjuicio del agraviado.

CATEGORIA N° 02

PROTECCIÓN PENAL

5. ¿Cuál es el bien jurídico protegido en el fraude informático, desde la perspectiva del derecho a la propiedad del sujeto pasivo en los delitos contra el patrimonio? Explique

   El bien jurídico tutelado es el patrimonio en relación al derecho de propiedad que tiene el sujeto pasivo sobre la base de datos informáticos y su adecuado funcionamiento de un sistema informático.

6. ¿En qué consiste la tipicidad objetiva del fraude informático en el delito contra el patrimonio? Explique

   Consiste en efectuar el análisis si concurren los elementos del tipo penal prescrito de acuerdo a la normatividad vigente en relación a la conducta del sujeto activo y el objeto material del delito.

7. ¿Cuáles son los criterios para establecer la tipicidad objetiva en el fraude informático del delito contra el patrimonio? Explique.

   Al respecto, si la conducta está prevista ley de los delitos informáticos, el cual sea susceptible de, verificar la tipicidad, antijuricidad y la culpabilidad y el reproche penal en contra del sujeto activo.

8. ¿En qué consiste el análisis de la tipicidad subjetiva del fraude informático en los delitos contra el patrimonio? Explique.

   Consiste en establecer el accionar del agente es doloso o culposo es decir se analiza la voluntad y el conocimiento en la realización de la conducta delictiva del fraude

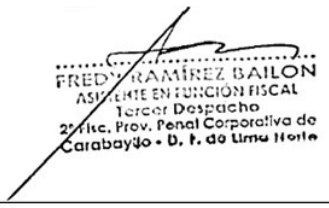
informático a través de medios informáticos o en su defecto si la conducta delictiva es culposa o no del agente.

9. ¿Considera usted que la tipicidad subjetiva en el delito de fraude informático comprende solo el análisis de la conducta dolosa? Explique

   Sí, porque, el dolo excluye la modalidad culposa es decir el agente deberá comprender la falta de autorización para realizar la conducta delictiva con propósito de obtener el provecho económico en perjuicio de un tercero utilizando instrumentos informáticos para efectuar trasferencias electrónicas de fondos o con la utilización de tarjetas en los cajeros automáticos y acceso ilícitos a ordenadores de redes a través del internet.

10. ¿Cuáles son los criterios para establecer la pena y circunstancias agravantes en el delito de fraude informático? Explique

    Que la acción de la conducta cumpla con los elementos de tipicidad en la norma, para establecer la pena a imponer de acuerdo a las circunstancias agravantes esto es según la magnitud del daño provocado, en el patrimonio del Estado y que además dichos patrimonios estén orientados en programas de apoyo social.

Nombre del entrevistado	Sello y Firma
Dr. Fredy Ramírez Bailón	

GUÍA DE ENTREVISTA

TÍTULO: Implicancias jurídicas del fraude informático y la protección penal del delito contra el patrimonio Distrito Fiscal de Lima Norte 2020

ENTREVISTADO: Br. Guillermo Jesús Matallana Lucero

Cargo: Asistente en función Fiscal del Distrito Fiscal de Lima Norte.

Profesión: Bachiller en derecho

Grado académico: Bachiller

FECHA: 15/12/2020

INDICACIONES: *El presente instrumento forma parte de una investigación jurídica. Se le ruega contestar de forma objetiva. Recuerde que no hay respuestas correctas o incorrectas, su participación y experiencia es lo que se valorará.*

CATEGORIA N°01

FRAUDE INFORMÁTICO

1. ¿Cuáles son las consecuencias jurídicas de alterar el ingreso de datos de manera ilegal mediante sistemas informáticos en el fraude informático del delito contra el patrimonio? Explique.

   Por definición al tratarse de un ingreso ilegitimo en sistemas informáticos la consecuencia jurídica sería la de una sanción penal o administrativa conforme la conducta especifica se encuentre tipificada en la norma.

2. ¿Considera usted que alterar, destruir, suprimir o robar datos informáticos puede ser difícil de detectar la conducta ilícita del ciberdelincuente en el delito contra el patrimonio? Explique.

   Considero que dichas conductas serian de difícil detección por el usuario por medio de los sistemas informáticos, ya que la mayoría se limitan al uso de programa de ofimática, mientras que conocimiento de redes y encriptación informático necesarios para causar una conducta pasible de ser calificada como delito informático requieren cierto nivel de especialización mínimo.

3. ¿Considera usted que alterar o borrar archivos no autorizadas sobre datos almacenados en los medios informáticos lo puede realizar cualquier persona en los delitos contra el patrimonio? Explique.

   Si bien los delitos informáticos no son delitos especiales, pues en principio pueden ser cometidos por cualquier persona, en la práctica se requiere un nivel de conocimiento y especialización para poder alterar los sistemas informáticos a nivel que puedan causar un perjuicio capaz de subsumirse como delito informático.

4. ¿Considera usted para alterar o dar un mal uso a sistemas o software con propósitos fraudulentos se requiere de un alto nivel de conocimiento informático en los delitos contra el patrimonio? Explique.

   Considero que si es necesario un alto nivel de conocimiento informático, que el usuario promedio no posee.

CATEGORIA N° 02

PROTECCIÓN PENAL

5. ¿Cuál es el bien jurídico protegido en el fraude informático, desde la perspectiva del derecho a la propiedad del sujeto pasivo en los delitos contra el patrimonio? Explique

   El bien jurídico protegido lo configura el patrimonio, el cual es afectado haciendo uso de los sistemas informáticos y digitales.

6. ¿En qué consiste la tipicidad objetiva del fraude informático en el delito contra el patrimonio? Explique

   La tipicidad objetiva es la actividad externa desarrollada por el sujeto activo confines fraudulentos del correcto funcionamiento en el sistema informático o de transmisión de datos con el propósito de lograr una ventaja económica con contenido ilícito.

7. ¿Cuáles son los criterios para establecer la tipicidad objetiva en el fraude informático del delito contra el patrimonio? Explique.

   El criterio sería que el hecho ilícito de la conducta cumpla la configuración del tipo penal y que encuadre dentro del análisis de la tipicidad en el plano informático, es decir las vulneraciones, alteraciones o supresiones de sistema de seguridad informática contravengan la norma teniendo como consecuencia la sanción penal.

8. ¿En qué consiste el análisis de la tipicidad subjetiva del fraude informático en los delitos contra el patrimonio? Explique.

Implica el análisis de la conducta dolosa del sujeto activo el cual se compone de dos elementos él volitivo se refiere al ánimo y la voluntad de querer realizar el hecho ilícito, y el cognitivo este elemento se analiza si el sujeto activo tiene conocimiento respecto del evento delictivo que va a cometer incluso de los alcances o consecuencias jurídicas.

9. ¿Considera usted que la tipicidad subjetiva en el delito de fraude informático comprende solo el análisis de la conducta dolosa? Explique

   Conforme lo define la propia ley de delitos informáticos, el delito de fraude informático solo puede ser a título de dolo porque el agente actúa motivado con animus lucrandi, desde el inicio hasta la consumación de la conducta ilícita.

10. ¿Cuáles son los criterios para establecer la pena y circunstancias agravantes en el delito de fraude informático? Explique

    Como los delitos previstos en el Código Sustantivo los criterios para establecer la pena lo configuran las agravantes genéricas y especificas del artículo 46° de dicho cuerpo legal. Y las circunstancias agravantes se presenta cuando el delito se comete afectando el patrimonio del Estado con fines asistenciales, lo cual tiene coherencia pues dicha conducta tiene un mayor desvalor pues afecta patrimonio dirigido a cubrir una necesidad de la comunidad.

Nombre del entrevistado	Sello y Firma
Br. Guillermo Jesús Matallana Lucero	GUILLERMO JESÚS MATALLANA LUCERO ASISTENTE EN FUNCIÓN FISCAL Tercer Despacho 2° Fisc. Prov. Penal Corporativa de Carabayllo - D. F. de Lima Norte