UNIVERSIDAD NACIONAL DE CHIMBORAZO

FACULTAD DE CIENCIAS POLÍTICAS Y ADMINISTRATIVAS

CARRERA DE DERECHO

"La eficacia probatoria de la apropiación fraudulenta por medios electrónicos"

Trabajo de Titulación para optar al título de Abogada de los Tribunales y Juzgados de la República del Ecuador

Autora:
Katherine Stefania, Sisa Lema

Tutor:
Abg. Gabriela Yosua Medina Garcés. Mgs.

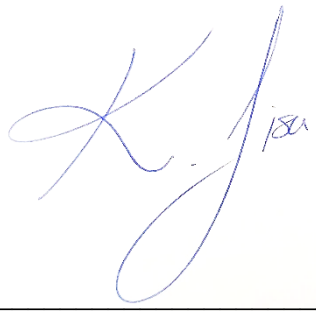
Riobamba, Ecuador. 2024

DECLARACIÓN DE AUTORÍA

Yo, Katherine Stefania Sisa Lema, con cédula de ciudadanía 060484925-7, autor (a) (s) del trabajo de investigación titulado: "**La eficacia probatoria de la apropiación fraudulenta por medios electrónicos"**, certifico que la producción, ideas, opiniones, criterios, contenidos y conclusiones expuestas son de mí exclusiva responsabilidad.

Asimismo, cedo a la Universidad Nacional de Chimborazo, en forma no exclusiva, los derechos para su uso, comunicación pública, distribución, divulgación y/o reproducción total o parcial, por medio físico o digital; en esta cesión se entiende que el cesionario no podrá obtener beneficios económicos. La posible reclamación de terceros respecto de los derechos de autor (a) de la obra referida, será de mi entera responsabilidad; librando a la Universidad Nacional de Chimborazo de posibles obligaciones.

En Riobamba, 20 de noviembre de 2024.



Katherine Stefania Sisa Lema

C.I.: 060484925-7

AUTORA

ACTA FAVORABLE - INFORME FINAL DEL TRABAJO DE INVESTIGACIÓN

En la Ciudad de Riobamba, a los 05 días del mes de agosto del 2024 luego de haber revisado el Informe Final del Trabajo de Investigación presentado por la estudiante **Katherine Stefania Sisa Lema** portadora de la cédula de ciudadanía **060484925-7** de la carrera de Derecho y dando cumplimiento a los criterios metodológicos exigidos, se emite el **ACTA FAVORABLE DEL INFORME FINAL DEL TRABAJO DE INVESTIGACIÓN** titulado ***"La eficacia probatoria de la apropiación fraudulenta por medios electrónicos"***, por lo tanto se autoriza la presentación del mismo para los trámites pertinentes.

Abg. Medina Garcés Gabriela Yosua. Mgs

Tutora

CERTIFICADO DE LOS MIEMBROS DE TRIBUNAL

Quienes suscribimos, catedráticos designados Miembros del Tribunal de Grado para la evaluación del trabajo de investigación **"La eficacia probatoria de la apropiación fraudulenta por medios electrónicos"**, presentado por **Katherine Stefania Sisa Lema** con cédula de ciudadanía **060484925-7,** bajo la tutoría de la Abg. Gabriela Yosua Medina Garcés. Mgs; certificamos que recomendamos la **APROBACIÓN** de este con fines de titulación. Previamente se ha evaluado el trabajo de investigación y escuchada la sustentación por parte de sus autores; no teniendo más que observar

De conformidad a la normativa aplicable firmamos, en Riobamba a los 28 días de noviembre de 2024.

Dr. Segundo Walter Parra Molina
PRESIDENTE DEL TRIBUNAL DE GRADO **Firma**

Dr. Bécquer Flor Carvajal
MIEMBRO DEL TRIBUNAL DE GRADO **Firma**

Dr. Nelson Francisco Freire Sánchez
MIEMBRO DEL TRIBUNAL DE GRADO **Firma**

CERTIFICACIÓN

Que, **SISA LEMA KATHERINE STEFANIA** con CC: **060484925-7**, estudiante de la Carrera **de DERECHO**, Facultad de **CIENCIAS POLÍTICAS Y ADMINISTRATIVAS**; ha trabajado bajo mi tutoría el trabajo de investigación titulado **"LA EFICACIA PROBATORIA DE APROPIACIÓN FRAUDULENTA POR MEDIOS ELECTRÓNICOS"**, cumple con el 6 %, de acuerdo al reporte del sistema Anti plagio **TURNITIN**, porcentaje aceptado de acuerdo a la reglamentación institucional, por consiguiente, autorizo continuar con el proceso.

Riobamba, 11 de noviembre de 2024.

Abg. Gabriela Yosua Medina Garcés. Mgs.
TUTOR(A)

DEDICATORIA

El presente trabajo de investigación en primera instancia se lo dedico a Dios y a mi Virgencita, entes celestiales que guiaron mi devenir, a mis respetados y amados padres que me acompañaron en el proceso de formación profesional, siendo sus abrazos y sus sabios consejos, mi imponente espada; a mi padre Julio, el ser más dulce, consentidor, risueño que conozco, y a mi madre Anita, una mujer lideresa, inteligente, benevolente que ha sembrado en mí virtudes como el altruismo, la honestidad y el trabajo con esfuerzo; personas que se han moldeado como los pilares fundamentales en mi vida.

Los amo y admiro tanto. Gracias por creer en mí. Siempre serán mi mayor inspiración.

Katherine Stefania Sisa Lema.

AGRADECIMIENTO

Agradezco a Dios y la Virgen por ser la luz de mi vida, por bendecirme con una familia que nutre mi alma con apoyo y amor incondicional.

A mis queridos y entrañables padres Julio y Anita, cultivadores de mis más grandes sueños, seres que han prestado su luz para iluminar mi andar en cada tormenta brindando regocijo y cobijo a mi alma, gracias por levantarme cada vez que caigo, acurrucarme en los tiempos de guerra y sobre todo por forjar en mí, la convicción de ser valiente. Todos mis logros se los debo a ustedes

A mi hermana Pamela, por su inquebrantable motivación y su eterna paciencia. A mi hermana Doménica por su terquedad y sapiencia.

A mis mentores Dr. Wilmer y Dr. Israel, profesionales de Derecho que han avivado en mi la llama del autoestudio, la disciplina, y la preparación contante. Personas que creyeron en mi capacidad desde el primer momento.

Katherine Stefania Sisa Lema.

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE ILUSTRACIONES

RESUMEN

La tesis titulada "La eficacia probatoria de la apropiación fraudulenta por medios electrónicos" explora los desafíos jurídicos y técnicos que enfrenta el sistema de justicia ecuatoriano en la investigación y sanción de este delito de naturaleza informática. La investigación se enfoca en el análisis de los elementos de tipicidad del delito establecido en el artículo 190 del Código Orgánico Integral Penal (COIP), complementado con un estudio comparativo de las legislaciones de Ecuador, España y Perú en cuanto al tratamiento de la evidencia digital. Para abordar estos desafíos, se emplearon entrevistas dirigidas a fiscales de las Unidades de Patrimonio Ciudadano, junto con el uso de tablas comparativas y análisis jurídico-doctrinal. Los hallazgos subrayan la falta de protocolos estandarizados para el manejo de la evidencia digital, la escasez de peritos informáticos especializados y las dificultades en la obtención de información bancaria como factores críticos que afectan la eficacia probatoria en estos casos. La investigación concluye que la ausencia de protocolos claros y la insuficiencia de recursos especializados comprometen la admisibilidad y validez de la evidencia digital en los procesos judiciales, lo que frecuentemente conduce a la impunidad en los delitos de apropiación fraudulenta por medios electrónicos. Este estudio resalta la necesidad urgente de mejorar los marcos legales y operativos para asegurar la efectividad en la lucha contra este tipo de criminalidad.

Palabras claves: apropiación fraudulenta, medios electrónicos, admisibilidad, evidencia digital.

ABSTRACT

The thesis entitled 'The evidentiary effectiveness of fraudulent appropriation by electronic means' explores the legal and technical challenges faced by the Ecuadorian justice system in investigating and punishing this computer-related crime. The research focuses on analyzing the elements of the criminality of the offense established in Article 190 of the Comprehensive Organic Criminal Code (COIP), complemented by a comparative study of the legislations of Ecuador, Spain, and Peru regarding the treatment of digital evidence. To address these challenges, interviews with prosecutors from the Citizen Patrimony Units were used, along with comparative tables and legal-doctrinal analysis. The findings highlight the lack of standardized protocols for handling digital evidence, the shortage of specialized computer experts, and difficulties obtaining banking information as critical factors affecting evidentiary effectiveness in these cases. The research concludes that the absence of clear protocols and insufficient specialized resources compromises the admissibility and validity of digital evidence in judicial proceedings, often leading to impunity in crimes of fraudulent appropriation by electronic means. This study highlights the urgent need to improve legal and operational frameworks to ensure effectiveness in the fight against this type of crime.

Keywords: fraudulent appropriation, electronic media, admissibility, digital evidence.

Reviewed by:

Firmado electrónicamente por:
EDUARDO SANTIAGO BARRENO FREIRE

Lic. Eduardo Barreno Freire. Msc.

ENGLISH PROFESSOR

C.C. 0604936211

CAPÍTULO I

1. INTRODUCCIÓN

El siglo XXI es prenombrado como la nueva era digital, el avance rotundo de los sistemas informáticos y la dinamización de redes como el Internet han producido una ola amplia de beneficios vinculados con la optimización y simplificación de actividades humanas, sin embargo, el aparecimiento de potenciales peligros derivados de su mal manejo han generado riesgos a nivel mundial. Por un lado, el sistema de justicia ha sido acechado por la transformación de la delincuencia tradicional por el desarrollo de nuevos modos operandi. La presente investigación, efectúa un análisis de la eficacia probatoria de la apropiación fraudulenta por medios electrónicos.

El delito de apropiación fraudulenta por medios electrónicos tipificado en el artículo 190 del Código Orgánico Integral Penal se configura como un delito contra la propiedad, procura la transferencia no consentida de bienes, valores o derechos en perjuicio de terceros manipulando el funcionamiento de redes electrónicas, programas, sistemas informáticos y equipos terminales de telecomunicación (Asamblea Nacional del Ecuador, 2014) Pero, uno de los mayores retos que afronta la sanción de este ilícito depende de los medios probatorios que demuestren su cometimiento, debido a que al ser efectuados por medios informáticos, su eficacia probatoria tiende a ser limitada por factores como la volatilidad y manipulación de pruebas, restringiendo el convencimiento al administrador de justicia sobre la sanción del delito (Aparicio, 2022).

Actualmente, los delitos de naturaleza informática se configuran como el nuevo fenómeno criminal asociado al abusivo uso de los sistemas informáticos, procesamiento y almacenamiento de datos. Imprimiendo la necesidad de examinar a través del derecho comparado el sistema sancionador de los delitos informáticos y la adoptación de los debidos mecanismos legales para la tutela correcta de los derechos de las personas. Bajo esta línea de pensamiento, la mayoría de las legislaciones mundiales han incorporado en la normativa penal, figuras jurídicas que reprimen y condenan las actividades distorsivas en el uso de sistemas informáticos (Leyva , 2021).

En el caso ecuatoriano, el país actualmente no se halla suscrito a un importante convenio de ciberdelitos, denominado “Convenio de Budapest 2014”, herramienta de dimensión internacional cuyo eje radica en la eliminación de las nuevas modalidades de delitos bajo la incorporación de normativas internas que efectivicen la investigación y la cooperación

internacional. Sin embargo, bajo la emisión del dictamen 1-24-T/24 emitido por la Corte Constitucional, se insta a la emisión de aprobación legislativa del convenio antes mencionado, es decir que el país ecuatoriano, está en proceso de adhesión al instrumento bajo la aprobación del legislativo. El ordenamiento jurídico ecuatoriano, no tipifica en su norma penal los delitos de naturaleza informática tácitamente, pero, en la sección novena denominada "Delitos contra la propiedad" desde el artículo 190 hasta el 195 expone figuras delictivas relacionadas con medios electrónicos, equipos y terminales móviles.

No obstante, la presente investigación se centra especialmente en la eficacia de los medios probatorios del hecho delictivo tipificado en el artículo 190 del COIP prenombrado "Apropiación Fraudulenta por medios electrónicos". En tanto, este delito informático es efectuado bajo diferentes modalidades de comisión a través de las cuales los delincuentes obtienen información confidencial de las víctimas. En este sentido, la tecnología ha dinamizado y transformado el entorno social, cultural y económico que rodea a la sociedad, pero claramente el incorrecto uso de estas ha provocado que los usuarios sean más susceptibles a ser engañados generándoles daños de índole económico, como la clonación de tarjetas y las transacciones ilícitas, son claras referencias sobre como los delincuentes infringen el ordenamiento jurídico con simplicidad por injerencia de la tecnología. Pero la preocupación latente del sistema de justicia recae sobre como actualmente, la impunidad del delito ha proliferado, pues, aparentemente los medios probatorios digitales no son suficientes para probar la materialidad y responsabilidad del ilícito (Aparicio, 2022).

El aspecto metodológico de la investigación se enmarca en el análisis documental de artículos científicos de los últimos cinco años, bajo diferentes métodos como el jurídico-analítico, comparación jurídica y jurídico descriptivo. En consecuencia, para garantizar la obtención de datos empíricos, las técnicas son la aplicación de entrevistas y la tabla de derecho comparado.

La investigación del presente tema, sostiene interés académico, ya que, mediante la difusión del presente trabajo, se contribuirá a la academia en conocimientos empíricos sobre como en la actualidad se manejan procesalmente los delitos de naturaleza informática, su valor probatorio en el proceso penal; y la existencia o no de normas que los regulen y sancionen el cometimiento de dicha infracción. Es decir, se busca ofrecer el conocimiento de la realidad jurídica del delito de apropiación fraudulenta por medios electrónicos.

La investigación se estructura conforme a lo establecido en el artículo 16 numeral 3 del Reglamento de Titulación Especial de la Universidad Nacional de Chimborazo, que comprende: portada; introducción; planteamiento del problema; objetivos; general y específicos; estado del arte, marco teórico; metodología; presupuesto y cronograma del trabajo investigativo; referencias bibliográficas; anexos; y visto bueno del tutor.

Por lo tanto, el objetivo de la investigación radica en analizar la eficacia probatoria de la conducta punible de carácter informático prevista en el artículo 190 del COIP. Esto incluye la ejecución de una evaluación exhaustiva de los desafíos y limitaciones actuales en la recolección, preservación, y análisis de la evidencia digitales. Secuencialmente, la investigación busca identificar las principales dificultades internas y externas que se pueden generar en la investigación y sanción de esta infracción.

1.1 Planteamiento del Problema

El avance tecnológico ha crecido de manera acelerada, convirtiéndose en un factor crucial para el desarrollo de la sociedad actual. Este progreso ha simplificado la comunicación y la interacción digital, pero también ha traído consigo nuevas modalidades delictivas ejecutadas a través de medios informáticos y redes de Internet. Como resultado, el mundo digital presenta desafíos significativos para la protección de los usuarios y facilita la comisión de ilícitos debido al anonimato que proporciona a los delincuentes. Esto ha llevado a que el sistema de justicia enfrente serios problemas asociados con la judicialización de delitos cometidos en este ámbito.

La facilidad de acceso, alteración y destrucción de sistemas informáticos constituye una barrera para la presentación de pruebas que permitan sancionar conductas punibles. Además, la falta de una normativa clara sobre las obligaciones de conservación, protección y exhibición de datos informáticos dificulta las actuaciones urgentes de las autoridades judiciales, convirtiéndose en uno de los mayores obstáculos para llevar a cabo investigaciones digitales (Leyva, 2021).

Según datos estadísticos de la fiscalía general del Estado, entre 2017 y 2021 se registraron 10,393 denuncias por el delito de apropiación fraudulenta por medios electrónicos. Estos números indican que los delitos de naturaleza informática han ganado terreno en la sociedad ecuatoriana (Fiscalía General del Estado, 2021). Sin embargo, debido a la naturaleza intangible de la prueba, existen limitaciones probatorias que dificultan la sanción de estos delitos, lo que plantea serios desafíos para los fiscales encargados de las investigaciones.

De acuerdo con Aparicio (2022), los delitos informáticos tienden a quedar impunes por la falta de evidencia, lo que ha provocado un crecimiento exponencial de fraudes informáticos. Estos delitos lesionan bienes jurídicos protegidos por el Estado, como la intimidad personal y el patrimonio, a través del robo de datos informáticos y bancarios. Según investigadores como Le Clercq y Sánchez (2020) en su estudio "Escalas de Impunidad en el Mundo", Ecuador ocupa el lugar 55 de 96 países en términos de impunidad, una posición vinculada a la falta de sanción efectiva de los delitos.

1.2 Justificación

La importancia de este trabajo de investigación radica en la necesidad académica de generar una respuesta a la alta tasa de impunidad asociada al delito de apropiación fraudulenta por medios electrónicos. La frecuencia de este delito ha aumentado con el avance acelerado de la tecnología, evidenciando que las leyes penales sustantivas y sus procedimientos aún no están en sintonía con la era digital. Esto provoca que las víctimas no reciban respuestas oportunas del sistema de justicia.

Esta investigación analiza las posibles soluciones legales que pueden integrarse en el marco jurídico del país, con el objetivo de establecer barreras legales que permitan reducir la comisión del delito de apropiación fraudulenta por medios electrónicos y, en consecuencia, disminuir su impunidad. También se identifica la implementación de cuerpos normativos en otras legislaciones para combatir los delitos de naturaleza informática.

La problemática que busca resolverse es la impunidad en los delitos de apropiación fraudulenta por medios electrónicos, evitando que los ciudadanos sufran lesiones a sus bienes jurídicos debido a la deficiencia probatoria en el proceso judicial penal.

En la era digital, los delitos cometidos a través de medios electrónicos, al ocurrir en un entorno intangible, son difíciles de localizar y, por ende, tienden a quedar impunes. Entre estos, el delito de apropiación fraudulenta por medios electrónicos ha incrementado notablemente debido al uso de redes sociales y plataformas digitales. Esto genera inestabilidad en el espacio intangible y plantea grandes retos al sistema de justicia, afectando bienes jurídicos como la intimidad personal y el patrimonio económico. Las personas, al ser víctimas del robo de datos personales y bancarios, corren el riesgo de sufrir clonación de tarjetas y transferencias ilícitas.

1.3 Objetivos

1.3.1 Objetivo General

Realizar un estudio jurídico analítico de la eficacia probatoria de la apropiación fraudulenta por medios electrónicos, tipificada en el artículo 190 del COIP.

1.3.2 Objetivos Específicos

- Analizar los elementos de tipicidad de la conducta punible de apropiación fraudulenta por medios electrónicos a través de una revisión jurídico-legal.
- Examinar a través del derecho comparado el procesamiento de los tipos de prueba en casos de apropiación fraudulenta por medios electrónicos.
- Establecer la eficacia de las pruebas obtenidas en casos de apropiación fraudulenta mediante la ejecución de entrevistas a expertos.

CAPÍTULO II

2. MARCO TEÓRICO

2.1. Estado del Arte

"La eficacia probatoria de la apropiación fraudulenta por medios electrónicos" es un tema propuesto bajo la indagación bibliográfica de fuentes secundarias que se asocian con las variables de estudio, dilucidando las siguientes conclusiones:

Aparicio (2022) en su escrito signado "Delitos informáticos en Ecuador según el COIP: un análisis documental" dilucida que los delitos informáticos se caracterizan por ser conductas ilícitas asociadas con la información y telecomunicaciones, acciones ligadas en efectuar daños relacionados con el ámbito informático, categorías mayores y complejas, que involucran la repotenciación de delitos tradicionales como el robo, fraude, falsificación y chantaje. En consecuencia, el autor resalta que los hechos ilícitos más comunes se vinculan con el fraude informático, un delito tradicional (fraude) repotenciado por la influencia tecnológica, la dinámica delictiva se enfoca en la eliminación de archivos, sustracción de información, bienes o valores que afecten la funcionalidad de un servidor.

De acuerdo a Villanueva y Andrade (2020) en su proyecto de investigación denominado "Ciberdelincuencia, enfocada en la apropiación de información a través de medios electrónicos y su influencia en el cometimiento de delitos informáticos" , plantea que el nacimiento de los ciberdelitos se asocia directamente con el caso llamado "blue box" de John Draper, antecedente histórico que remarcaría el hito del fortalecimiento de los delitos electrónicos, en conjunto de la evolución de estrategias empleadas por los infractores para evitar la detección del ilícito. En concomitante, la apropiación fraudulenta por medios electrónicos reza al acto de adquisición ilícita de información personal y datos financieros por medio de prácticas engañosas o manipulación de sistemas de información y comunicación, involucrando técnicas ilícitas como el phishing, el sniffing y el pharming, por intermedio del cual los ciberdelincuentes contraen información de carácter confidencial a través del Internet, suplantando la identidad de terceros o entidades financieras para engañar a las víctimas.

Remarcando que actualmente, la legislación ecuatoriana sostiene dificultad para investigar delitos de naturaleza informática, por su escaso desarrollo investigativo en este tipo de delitos, la infraestructura y equipos tecnológicos que impiden la óptima investigación. Por un lado, se pensaría que los países con más desarrollado en el ámbito tecnológico sería más

sencillo detectar el cometimiento de estos ilícitos, sin embargo, entre más avance de redes informáticas, los criminales tendrían más facilidad para cometer dichas conductas.

Mientras que Leyva (2021) en él, "Estudio de los delitos informáticos y la problemática de su tipificación en el marco de los convenios internacionales" destaca que la evolución del derecho penal tradicional está direccionada a atender los nuevos delitos efectuados en espacios intangibles, su naturaleza globalizada involucra que los perpetradores traspasen fronteras internacionales, complicando las cuestiones jurisdiccionales, en razón de que a menudo emplean herramientas de anonimización como redes privadas virtuales (VPN) y servidores proxy para enmascarar direcciones IP y ubicación real, lo que dificulta, el rastreo del hecho delictivo, generando una judicialización no exitosa.

Sempertegui (2022) en su investigación prenombrada "Delito de apropiación fraudulenta por medios electrónicos bajo la modalidad de phishing dentro del marco jurídico ecuatoriano" examina que uno de los mayores desafíos que afrontan los titulares de la acción penal pública en la legislación ecuatoriana gira en la investigación del hecho delictivo previsto en el artículo 190, así como, en la identificación de los perpetradores, bajo la bandera de anonimato que emplean los sujetos activos, debido a la facilidad para cometer estos delitos sin un amplio conocimiento técnico. Secuencialmente, fija la importancia de regulación y fundamento jurídico de los delitos de naturaleza informática, enfatizando la necesidad de un marco jurídico más completo que atienda las carencias en la normativa penal vigente, y las mejoras de las medidas de ciberseguridad.

La revista científica jurídica emprendida por la Fiscalía General del Estado (2021) titulada "Perfil Criminológico-Ciberdelitos" explora como la apropiación fraudulenta por medios electrónicos, presentan constantes desafíos para reunir medios probatorios suficientes para procesar eficazmente la participación de los infractores, dificultad que surge por la naturaleza intangible de las transacciones digitales y las complejidades que implica rastrear y probar actividades fraudulentas en el ciberespacio, en consecuencia, se afirma que los métodos tradicionales de recopilación y preservación de pruebas no son los adecuados para el tratamiento de los delitos cibernéticos como la apropiación fraudulenta; la dependencia de evidencia digital, requiere una profunda compresión de ciencias forenses digitales y nuevas metodologías de investigación cibernética, pero, la falta de experiencias y recursos adecuados en el presente campo, dificultan la presentación de pruebas admisibles en los tribunales de justicia.

Por consiguiente, Yendan (2023) en su exploración investigativa jurídica titulada " La no adhesión al convenio de Budapest vulnera los derechos en delitos informáticos" aborda que el Estado ecuatoriano al no estar adherido al principal instrumento internacional contra la ciberdelincuencia, denominado "Budapest" ha incidido en la incompleta legislación que contrarresta los ciberdelitos, debido a que la falta de capacitación en materia de ciberseguridad, la falta de intercambio de información crítica entre naciones y la falta de mejora de técnicas de investigación fiscal, no han reforzado la capacidad del Ecuador para lograr enfrentar amenazas informáticas.

Subsecuentemente "Legalidad de la prueba electrónica en el ámbito penal" redactada por Ashour y Afan (2023) aborda la dinámica asociada con la naturaleza evolutiva de las actividades delictivas provocadas por los avances tecnológicos que involucran el uso de computadoras y sistemas de información para actividades ilegales, en tanto, la legalidad de la evidencia digital en los procesos penales, se consagrada como un tema crítico que requiere que las pruebas se obtengan a través de procedimiento legítimos y que los fiscales se adhieran a las normas y estándares legales.

Seguidamente, GomezJurado (2017) en la investigación nominada " Identificación del sujeto activo en el delito de estafa a través de medios digitales y electrónicos bajo la perspectiva del COIP en el Ecuador" sostiene que algunas de las limitaciones de enjuiciamiento, se asocian con el estancamiento en la etapa de presentación de una denuncia, y muy pocos de los casos avanzan a fases de investigación o enjuiciamiento ulteriores, por la falta de conocimiento de los mecanismos legales o posibles repercusiones si denuncian el delito.

2.2 Aspectos Teóricos

2.2.1 UNIDAD I: FUNDAMENTOS DE LA APROPIACIÓN FRAUDULENTA POR MEDIOS ELECTRÓNICOS

La presente unidad introduce concepciones primarias acerca del delito de apropiación fraudulenta por medios electrónicos, su definición y características de la conducta delictiva; secuencialmente se amplía la data histórica y contexto actual del prenombrado delito, así como las modalidades bajo las cuales actúan los sujetos infractores en el cometimiento de la infracción penal motivo de estudio.

2.2.1.1 Definición y características de la apropiación fraudulenta por medios electrónicos

Para poder definir lo que se comprende por apropiación fraudulenta por medios electrónicos, es indispensable primero aproximarse a la definición de apropiación, y segundo a una definición de fraudulenta, con la intención clara de lograr una mayor delimitación del concepto en conjunto. En este punto, Muñoz (2022) establece que el vocablo "apropiación" en su concepción imperiosa, deviene de hacer propia una cosa privada como si ejerciera el dominio sobre ella, con la plena intención de no restituirla, es decir el sujeto efectúa acciones de disposición o de uso determinado sobre un bien. Mientras que, la Real Academia Española define a la apropiación como el hecho de apoderarse de una cosa o bien, haciéndose dueña de ella. Ambas concepciones destacan que la apropiación implica tomar la posesión de algo bajo el ejercicio de control y dominio sin intención de restitución y que el sujeto se plantee como propietario del mismo.

Por otro lado, el término "fraudulenta" proviene del latín *fraudulentus*, derivada de *fraus, fraudis,* palabras que se vinculan con la mala fe y engaño. En consecuencia, el presente acusativo produce un término de léxico jurídico conocido como fraude. García (1998) destaca que "el fraude es un comportamiento ilícito que atenta contra el patrimonio de las personas, suponiendo el empleo de medios indirectos, ardides, falacias que produzcan apariencias engañosas" (p.10). En cambio, la Real Academia Española (2002) lo define como "Acción contraria a la verdad y a la rectitud, que perjudica a la persona contra quien se comete. Se trata de inducir, mantener o reforzar el error en la víctima, con el designio de lograr de ella una disposición patrimonial". Juicios, que naturalmente afirman que el fraude se asocia con la producción directa de artificios confabulados para el engaño y su plena intención de inducir al error y provocar un daño patrimonial a terceros.

Los medios electrónicos se configuran como aquellos instrumentos que son empleados para almacenar, transmitir y presentar información de manera electrónica como las computadoras destinadas para el procesamiento de datos e información; dispositivos de almacenamiento como discos duros y memorias USB; software de red que facilitan la comunicación como navegadores, servidores web, correos electrónicos, mensajes y fax. Naturalmente la amplia incorporación de recursos tecnológicos como la informática y los avanzados medios de comunicación como las herramientas previamente determinadas se ha configurado como espacios rentables para la comisión de fraudes altamente lucrativos (Universidad de Costa Rica, 2009).

De hecho, bajo las conceptualizaciones realizadas, se logra fijar que la apropiación fraudulenta por medios electrónicos se asocia con la manipulación ilícita realizada a través de

la alteración de base de datos o sistemas informáticos con el objetivo de lucrar indebidamente afectando bienes jurídicos como el patrimonio de terceros. Secuencialmente, la presente conducta presenta características notorias, las cuales son reconocidas y sancionadas por el ordenamiento jurídico.

En primer lugar, se fija que la acción ilícita es por naturaleza fraudulenta, caracterizada por el engaño y uso indebido de determinados equipos. En segundo lugar, se señala el medio a través del cual debe ser efectuada, siendo los equipos tecnológicos como dispositivos móviles, computadores y softwares, herramientas de naturaleza informática. Por último, la finalidad es la ganancia de un lucro injusto, bajo la premisa de un beneficio ilícito, elementos que implica que el sujeto se enriquezca indebidamente (Universidad de Costa Rica, 2009).

2.2.1.2 Evolución histórica y contextual actual de la apropiación fraudulenta

Según lo señalado por Miro (2012), el procesamiento automatizado de información personal por intermedio de los medios informáticos genera consecuencias indudables en el mundo jurídico, desde una perspectiva histórica de la criminalidad informática, la categoría de delitos de naturaleza informática nace como construcciones doctrinales emergentes de legislaciones como la alemana y la española durante los años setenta, ochenta y novena, logrando la agrupación autónoma de conductas delictivas con caracteres sistemáticos.

Las primeras conductas delictivas relacionadas con ordenadores empezaron su auge en la década de los años 70, las infracciones penales de naturaleza informática fueron de tipo económico, en la que deslumbraban delitos como el espionaje informático, la piratería de software, y el sabotaje de datos digitalizados. Por consiguiente, en la década de los 80 surgen los fraudes de tipo financiero, en la que primó la alteración de base de datos de empresas, así como la manipulación de factores de pago.

El modo operandi de los infractores se efectuaba bajo la instalación de dispositivos lectores en los cajeros automáticos y teclados falsos, estos copiaban los datos de las tarjetas de crédito, acto que instó a las entidades bancarias a la adopción de plásticos como medida de seguridad. Precisamente, en esta época iniciaron los países europeos con la protección normativa sobre bienes como el dinero electrónico, regulación que también precedería en el país americana en 1978.

Precisamente en el año 1985 un grupo de expertos convocados a la edición nombrada “Delitos relacionados con ordenadores” por la Organización para la Cooperación y el Desarrollo Económico, efectuó un amplio análisis por primera vez respecto a los delitos

informáticos, definiéndolos como “toda acción dolosa que provoca un perjuicio a personas o entidades, en cuya comisión intervienen dispositivos habitualmente utilizados en las actividades informáticas”. Así también, el Manual de Recursos de Justicia Criminal del Departamento de Justicia de los Estados Unidos en los siguientes años emboza que los delitos informáticos como la estafa informática se configura como un acto ilegal que parte del conocimiento de tecnología computacionales. En tanto, se logra identificar como los países y los Organismos Internacionales iniciaron en identificar las nuevas modalidades de delitos, y brindar el oportuno tratamiento jurídico y la toma de medidas preventivas.

A nivel de América Latina, las actividades delictivas de naturaleza informática comenzaron a afectar varios países, incluido Chile. El primer hackeo documentado en Sudamérica se realizó contra el Banco de Chile en 1988. Este ataque involucró el acceso no autorizado a sistemas informáticos y la manipulación de datos financieros. Por los bajos sistemas de seguridad, los inicios del siglo XX, se vio azotada por la invasión de redes, robo de información personal, hacking, y fraudes informáticos que se repotenciaron por la invención de herramientas tecnológicas que menoscabaron la privacidad, intimidad y patrimonio de las víctimas. De hecho, es vital enmarcar que el primer país en Sudamérica que reguló específicamente los delitos informáticos fue Colombia, bajo la aprobación de la ley 1273, normativa que creó un nuevo bien jurídico tutelado denominado “la protección de la información y de datos”.

La primera norma asociada con las nuevas tecnologías en el país ecuatoriano, se asocia directamente con la Ley de Comercio Electrónico, Mensajes de Datos y Firmas Electrónicas publicada en el año 2002, consecutivamente, en el año 2011, por iniciativa del Ministerio de Telecomunicaciones se emitió la “Estrategia Ecuador Digital” con el nacimiento de políticas públicas direccionadas en el manejo de tecnologías. Siendo, uno de las innovaciones más relevantes, el desarrollo de infracción de naturaleza informática en el Código Penal y posteriormente el Código Orgánico Integral, publicado el 10 de agosto del 2014.

De esta forma, el delito de apropiación fraudulenta por medio electrónicos, se encuentra actualmente previsto como una infracción informática incorporada en el Art.62 de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de datos, que además consta en la sección “Delitos contra el derecho a la propiedad”, en el artículo 190 del COIP.

2.2.1.3 Modalidades de la apropiación fraudulenta por medios electrónicos

Por lo general, el delito de apropiación fraudulenta por medios electrónicos se lleva a cabo bajo nuevas modalidades de comisión como el *pishing, vishing, smishing, malware.*

Phising

El phishing es el acto criminal en el que se obtiene información confidencial como nombres de usuarios, contraseñas y detalles de tarjetas de crédito pretendiendo ser una fuente confiable, por lo general el modo operandi de los infractores, se focaliza en el envío de correos electrónicos engañosos pretendiendo ser entidades legítimas, con el objetivo de engañar a los sujetos para que compartan información personal que pueda ser utilizada para actividades fraudulentas (Gisin, 2008).

Vishing

El *vishing* implica el engaño a víctimas a través de llamadas de voz para obtener ganancias económicas, comúnmente, los estafadores manipulan a los sujetos utilizando técnicas ingeniería social para inspirar confianza, reclamando autoridad y persuadiendo a las víctimas para que sigan sus instrucciones (Molin, 2021). En el mismo sentido Carriedo (2022), destaca que el *vishing,* es una práctica que consiste en la realización de llamadas telefónicas en las que una grabación, presentada como mensaje institucional de una entidad bancaria, notifica a la víctima sobre un supuesto fraude relacionado con su tarjeta de crédito. La grabación proporciona un número telefónico al que el usuario bancario, sorprendido por el aviso, debe comunicarse de inmediato. Al contactar dicho número, se le solicita proporcionar las claves confidenciales en su tarjeta, permitiendo así a los delincuentes utilizarla y consumar el ciberdelito.

Smishing

Smishing, que significa SMS Phising, es un tipo de ataque en el que los estafadores intentan engañar a las personas para que revelen información personal o financiera mediante mensajes de texto. A diferencia del phishing tradicional, los ataques de smishing implica el envío de mensajes de texto con información mínima y pueden incluir abreviaturas y símbolos para engañar a los destinatarios (Mishra & Soni, 2023).

Malware

El malware, proviene de la abreviatura "*malicious software"*, un prototipo de software malicioso, diseñado directamente para dañar, infiltrar o realizar actos no deseados en los

sistemas informáticos, redes sociales, sin el conocimiento y consentimiento de los sujetos, el modo operandi de los delincuentes se consolida bajo la instalación no conocida de este virus, generalmente a través de descargas o enlaces engañosos, que una vez instalados, acceden a información personal. En ocasiones, supervisan la actividad de equipos móviles, pudiendo forzar a visitar sitios web específicos, enviar correos electrónicos, inclusive proceder con el robo de información personal y bancaria (Universidad de Jaén, 2018).

2.2.2 UNIDAD II: EVIDENCIA DIGITAL Y MEDIOS PROBATORIOS EN CASOS DE APROPIACIÓN FRAUDULENTA

En la presente unidad se ampliará el conocimiento sobre el aporte que efectúa la evidencia digital en los procesos de judicialización; así como los tipos de evidencia que tienden a ser presentados frente a los tribunales de justicia; secuencialmente, se partirá con el estudio comparado del tratamiento de la evidencia digital en legislaciones como la peruana y la española.

2.2.2.1 Estudio comparado del tipo penal por apropiación fraudulenta de los países de Perú y España

El presente estudio comparativo se centra en las legislaciones cuyas figuras delictivas comparten elementos típicos asociados con el delito de apropiación fraudulenta por medios electrónicos. En primer lugar, se analizará la conducta penal tipificada en Perú considerando su relevancia y enfoque particular en la normativa penal. Posteriormente, se llevará a cabo un análisis de la conducta típica de la legislación española. Este esquema tiene como objeto identificar las posibles áreas de mejora en la regulación de este delito en ambos países.

Tabla 1 Elementos constitutivos del fraude informático "Perú"

Elementos constitutivos del fraude informático "Perú"	
Elementos	**Acción del delito:** La conducta delictiva se enfoca en la inferencia de supuestos en los que sujetos transfieren fondos ajenos a una cuenta de su propiedad o de un tercero.
	Sujetos: La persona procesada debe ser mayor de edad (imputable)
	Consentimiento: La conducta delictiva debió ser efectuada sin el consentimiento expreso del titular de los bienes
	Resultado del delito: Perjuicio a un tercero. Afectación al patrimonio

Tipicidad	**Sujeto activo:** El sujeto que efectúa la comisión del delito informático (Cualquier persona) **Sujeto pasivo:** Persona natural o jurídica afectada por la conducta delictiva **Objeto material:** Responde a los dispositivos empleados para materializar el ilícito, siendo estos los sistemas informáticos. **Objeto jurídico:** Asociado con el bien protegido a ser protegido
Antijuridicidad	El bien jurídico protegido es el derecho al patrimonio
Culpabilidad	El autor debe actuar con conocimiento y voluntad de llevar a cabo la conducta ilícita para obtener el provecho ilícito
Ley N ° 30096	**Art.8** El que deliberadamente e ilegítimamente procura para sí o para otro un provecho ilícito en perjuicio de tercero mediante el diseño, introducción, alteración, borrado, supresión, clonación de datos informáticos, o cualquier interferencia o manipulación en el funcionamiento de un sistema informático, será reprimido con una pena privativa de libertad no menor de tres ni mayor de ocho años y con sesenta a ciento veinte días-multa. La pena será privativa de libertad no menor de cinco ni mayor de diez años y de ochenta a ciento cuarenta días-multa cuando se afecte el patrimonio del Estado destinado a fines asistenciales o a programas de apoyo social

Fuente: Ley N° 30096 - Ley de Delitos Informáticos (2013)

Autor: Katherine Sisa. (2024).

Tabla 2 Elementos constitutivos del delito de defraudación "España"

Elementos constitutivos del delito de defraudación "España"	
Elementos	**Acción:** Manipulación o artificios informáticos **Sujetos:** Imputable **Consentimiento:** La conducta delictiva debió ser efectuada sin el consentimiento expreso del titular de los bienes. **Resultado del delito:** La acción debe causar un daño económico o perjuicio a la persona titular de los bienes.
Tipicidad	**Sujeto activo:** Cualquier sujeto que se halle legitimado para acceder a los sistemas o terceros no autorizados **Sujeto pasivo:** Sujeto titular del patrimonio. **Objeto material:** Utilización de medios informáticos.

	Objeto jurídico: Comprende la protección del patrimonio, la integridad y seguridad de sistemas información.
Antijuridicidad	El bien jurídico protegido es el patrimonio
Culpabilidad	El autor debe actuar con conocimiento y voluntad de llevar a cabo la conducta ilícita para obtener el provecho ilícito
Código Penal	**Artículo 249 literal 1.** a) Los que, con ánimo de lucro, obstaculizando o interfiriendo indebidamente en el funcionamiento de un sistema de información o introduciendo, alterando, borrando, transmitiendo o suprimiendo indebidamente datos informáticos o valiéndose de cualquier otra manipulación informática o artificio semejante, consigan una transferencia no consentida de cualquier activo patrimonial en perjuicio de otro. b) Los que, utilizando de forma fraudulenta tarjetas de crédito o débito, cheques de viaje o cualquier otro instrumento de pago material o inmaterial distinto del efectivo o los datos obrantes en cualquiera de ellos, realicen operaciones de cualquier clase en perjuicio de su titular o de un tercero. Serán sancionados con una pena de prisión de seis meses a tres años.

Fuente: Ministerio de la Presidencia, Justicia y Relaciones con las Cortes (2021)

Autor: Katherine Sisa (2024)

2.2.2.2 Concepto, y tipos de evidencia digital en caso de delitos informáticos

Concepto

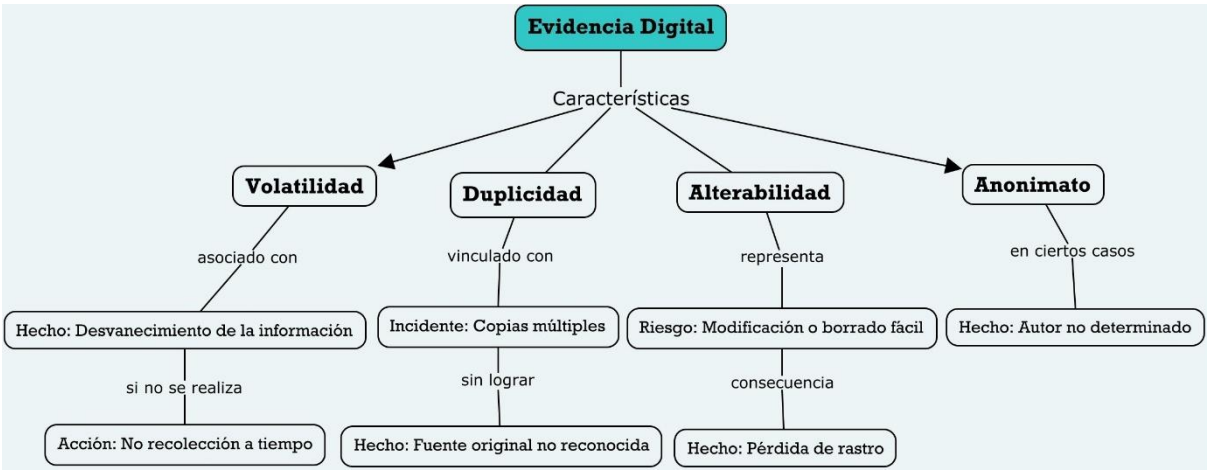
Desde un plano jurídico, la evidencia se define como el mecanismo a través del cual se demuestra la materialidad y responsabilidad de un sujeto frente a un tribunal. Consolidándose como un elemento del cual se figura un supuesto de hecho, y su verdad es investigada en el proceso judicial. Así que, este elemento principal prueba los hechos alegados por las partes, siendo indispensable que la evidencia sea confiable y fiable (Flórez et al., 2016). Consecuentemente, la presentación de evidencia sólida fomenta que los administradores de justicia logren discernir la verdad de manera más efectiva y se conviertan en la base sólida para la toma de decisiones justas y equitativas.

La evidencia digital juega un papel importante en la investigación de conductas delictivas modernas debido a la creciente utilización de medios electrónicos para la comisión de delitos. Casey (2011) asegura que, “la evidencia digital engloba indicios que se vinculan con el almacenamiento de información en un formato digital yacentes en computadoras o redes” (p.23). Así mismo, Osco et al., (2024) señala que la evidencia digital se refiere a la información almacenada en archivos digitales como documentos, chats y metadatos, creados conscientemente por los usuarios o automáticamente por dispositivos sin su consentimiento, proveyendo datos afiliados con los tipos de dispositivos digitales utilizados para la comisión del delito, el origen de transmisión y su almacenamiento.

En la misma línea, conforme la doctrina, Mirzakarimovna (2021) resalta que la evidencia digital se vincula con la información electrónica prevista por computadores, teléfonos inteligentes, correos electrónicos, redes sociales y otras fuentes digitales. Mientras que, Wilson et al., (2023) afirma que la información ayuda a rastrear, interpretar y comprender las acciones de los sujetos involucrados en las actividades delictivas. Indudablemente, la evidencia digital comprende cualquier indicio o prueba que esté relacionado con el almacenamiento de información en formato digital y que esta información se encuentre en computadoras o redes. En consecuencia, permite la reconstrucción de hechos y el análisis de los nuevos modus operandi adoptados por los infractores.

Efectivamente, la evidencia digital contiene características propias que la diferencian de la evidencia tradicional; entre ellas se destaca su volatilidad, rasgo asociado con el hecho de que la información puede o no desvanecerse si esta no es recolectada en un determinado tiempo y forma; por consiguiente, su duplicidad se vincula con el incidente de que pueden o no efectuarse diversas copias sin lograr reconocer la fuente original; además su alterabilidad, representa un factor de riesgo, en razón de que la información digital puede ser fácilmente modificable o borrada sin dejar rastros de las acciones; adicionalmente, el anonimato, una característica que en ciertos casos no permite determinar el autor de las mismas (Sosa, 2023).

Ilustración 1 *Evidencia Digital*



Fuente: Sosa (2023)

Elaborado por: Katherine Sisa (2024)

Tipos de evidencia digital en los delitos informáticos

Según Ochoa (2018), la evidencia digital puede ser categorizada en dos tipos:

A. **Evidencia Volátil:** Se refiere a la información de carácter transitorio, como la que se encuentra en la memoria principal (RAM). Se caracteriza por su temporalidad, en razón de que se pierde cuando el dispositivo se apaga o se reinicia. Como datos de la memoria activa de procesos en ejecución, información de la red, como conexiones activas y tablas de enrutamiento, archivos temporales y datos en caché.
B. **Evidencia No Volátil:** Se refiere a la información almacenada de manera permanente en dispositivos tales como discos duros, unidades, USB, CD, entre otros. Este tipo de información persiste incluso después de que el equipo hay sido apagado, por lo general, este tipo de evidencia es crucial en investigaciones forenses ya que proporciona datos duraderos.

2.2.2.2 Proceso de recolección, y preservación de la evidencia digital

Bajo el marco internacional se han planteado una serie de modelos óptimos para el tratamiento de la evidencia digital, en primer lugar, *"U.S Department of Justice"* fija lineamientos que proporcionan asistencia y orientación sobre quienes, en el ejercicio de sus funciones, son los encargados de llevar a cabo las diligencias preliminares en el ámbito de la evidencia digital. Estas diligencias comprenden la identificación de elementos probatorios de naturaleza digital, su recopilación o adquisición mediante procedimiento técnicos apropiados.

El proceso de recolección de evidencia digital según *"U.S Department of Justice"* deviene con el propósito de salvaguardar la integridad de la evidencia digital, el equipo de primera respuesta tiene la obligación de documental meticulosamente todas las intervenciones realizadas en los equipos informáticos, dispositivos periféricos y demás elementos tecnológicos, estableciendo directrices específicas para el manejo de equipos, diferenciando los procedimientos según su estado operativo. Así también, se dilucida que, dada la naturaleza inherente de la evidencia digital, y se garantice su conservación, se requiere la implementación de protocolos de embalaje que contemple como mínimo, elementos como documentación detallada, etiquetado inequívoco, inventario exhaustivo y utilización de embalajes antiestéticos (Institute of Justice, 2001).

Así también, Ochoa (2018) refiere que el proceso de recolección de evidencia digital comienza con la identificación que incluye un análisis de riesgos, el establecimiento de objetivos e hipótesis, la selección de herramientas y la generación de una lista de evidencia a recolectar. Luego se procede con la fijación fotográfica del lugar y los dispositivos. La adquisición de evidencia se divide en dos etapas: primero la evidencia volátil como la memoria RAM si el dispositivo está encendido, y segundo, la adquisición del almacenamiento permanente, que implica apagar el dispositivo, extraer las unidades de almacenamiento y realizar una copia bit-stream usando bloqueadores de escritura.

Mientras que, la recolección de dispositivos involucra desconectar fuentes de energía, remover cables y bloquear botones de encendido. Secuencialmente, la preservación de la evidencia digital implica que la evidencia sea embalada y sellada bajo condiciones adecuadas, utilizado contendores antiestéticos y acolchados cuando sea necesario, siendo también crucial mantener una cadena de custodia rigurosa, documentando todo el manejo y almacenamiento de la evidencia, manteniendo un registro detallado de toda persona que ha manejado la evidencia, incluyendo fechas, horas, ubicaciones y propósito del manejo (Ochoa, 2018).

2.2.2.3 Proceso de recolección, preservación y análisis de la evidencia digital en la legislación peruana y española.

Perú

Bajo la Resolución Ministerial No. 848-2019-IN, la legislación peruana aprobó el Manual para el Recojo de la Evidencia Digital, emitido por el Ministerio del Interior en el contexto de la Dirección contra el Delito de Crimen Organizado. Esta valiosa herramienta sirve

como guía para los procedimientos realizados por los miembros de la fuerza pública y los especialistas encargados de recabar, preservar y analizar técnicamente la información de dispositivos tecnológicos y/o registros de la escena del crimen. Su objetivo es evitar la contaminación o alteración de la evidencia, garantizando su validez en el proceso de judicialización.

Específicamente, el manual preestablecido enfatiza que el proceso para la recolección, preservación y análisis de evidencia digital se configura de la siguiente manera:

A. Identificación de la evidencia digital: Para la correcta identificación de la evidencia digital, es fundamental determinar las fuentes de las que proviene la evidencia de naturaleza informática. Estas pueden incluir computadoras personales, servidores, discos duros, discos duros externos, pen drives (USB), tarjetas electrónicas y memorias externas (SD, MicroSD), sistemas de vigilancia, y dispositivos móviles como teléfonos, tarjetas SIM, módems USB, GPS y tabletas (Ministerio del Interior, 2019).

B. Preservación de la evidencia digital: Para la preservación de la información, se asegura el área donde se encuentran los dispositivos involucrados en la comisión del delito, evaluando posibles riesgos y adoptando las medidas de seguridad necesarias. Efectivamente, un mecanismo de seguridad crucial es la imagen forense, una técnica que consiste en crear copias fieles de dispositivos de almacenamiento o sistemas informáticos, incluyendo todos los archivos y datos ocultos, como espacios no asignados y archivos eliminados (Ministerio del Interior, 2019). Según Bill (2018), el uso de imágenes forenses permite a los técnicos examinar los datos e información en un entorno seguro.

Consecutivamente, la cadena de custodia digital es un proceso documental que detalla cómo se realiza la recolección, transferencia y almacenamiento de la evidencia digital, garantizando su autenticidad, integridad y control en todo momento. Los elementos materiales probatorios y la evidencia física se consideran auténticos e intactos, siempre y cuando hayan sido asegurados, fijados, recogidos y embalados técnicamente, y sometidos a la regla de cadena de custodia.

C. Análisis de la evidencia digital: Para el desarrollo del análisis informático forense, el manual peruano de recogida de evidencias digitales establece que es indispensable la emisión de los siguientes documentos: el acta de hallazgo y recogida, el acta de incautación, el acta de entrega y recepción, el acta de lacrado y el acta de cadena de custodia. Finalmente, se requiere la autorización del usuario o una resolución judicial que disponga el análisis informático de los dispositivos (Ministerio del Interior, 2019).

España

En la legislación española, la recolección, preservación y análisis de la evidencia digital están reglamentados por diversas leyes y normativas que establecen directrices claras para la preservación de información digital. En efecto, la Ley de Enjuiciamiento Criminal (LECrim), promulgada por el Gobierno de España bajo la supervisión del Ministerio de la Presidencia, Justicia y Relaciones con las Cortes, se configura como una normativa regulatoria del procedimiento penal. Especialmente en su Capítulo V, denominado "La interceptación de las comunicaciones telefónicas y telemáticas," aborda las disposiciones generales, la incorporación al proceso de datos electrónicos de tráfico o asociados, y el acceso a los datos necesarios para la identificación de usuarios, terminales y dispositivos de conectividad.

Aunque la ISO/IEC 27037 no se consolida como una ley por sí misma, sus directrices y lineamientos son integrados en la legislación y prácticas operativas en España, a través de entidades como el Instituto Nacional de Ciberseguridad (INCIBE) y el Centro Criptológico Nacional (CCN). Esta normativa se focaliza en garantizar que la evidencia digital se maneje de acuerdo con los más altos estándares internacionales, asegurando su autenticidad en los procesos judiciales.

Tabla 3 Normas Españolas que regulan, el proceso de recolección, preservación y análisis de la evidencia digital

	Ley de Enjuiciamiento Criminal **Capítulo V**	**Normativa Internacional ISO/IEC 27037**
Recolección de la evidencia digital	• **Artículo 588 terb: Ámbito** Inspección y Registro de lugares Cerrados: El presente artículo le cede la potestad a los administradores de justicia de ordenar la inspección y registro de lugares cerrados cuando sea indispensable la investigación de un delito La recolección de evidencia incluye la prolija inspección de dispositivos electrónicos y sistemas informáticos presentes en el lugar.	• Una vez asegurada la escena y confirmada la autoridad legal para confiscar la evidencia, se procede a recolectar los dispositivos. Es fundamental obtener contraseñas, códigos o PIN de las personas involucrada cuando sea posible, así como recolectar los cargadores, cables, periféricos y manuales asociados.

	Artículo 588 octies:	
Preservación de la evidencia digital	• El cuerpo normativo español es claro en establecer que las pruebas, e información concreta deben ser aseguradas sin alterar su estado original, bajo la bandera de dar cumplimiento con la cadena de custodia.	• La ISO/IEC 27037 establece que antes de iniciar con el análisis de la evidencia, se crea una imagen o una copia, en tanto proceden a aislar dispositivos inalámbricos e instalar un software de bloqueo de escritura.
Análisis de evidencia digital	• El análisis de la evidencia digital debe ser efectuada en laboratorios forenses acreditados, bajo la aplicación de herramientas y software forenses que incluyan técnicas innovadoras como la recuperación de datos eliminados, análisis de actividades y trazas, y la captura de datos volátiles	• Los sujetos encargados del análisis de la evidencia son: Digital Evidence First Responder (DEFRs) o especialista en evidencia digital de primera intervención, Digital Evidence Specialist (DESs) o especialista en evidencia digital,especialistas en respuestas a incidentes y directores de laboratorios forenses.

Fuente: (Ministerio de la Presidencia Justicia y Relaciones con las Cortes, 2021)
Elaborado por: Katherine Sisa (2024)

2.2.3 UNIDAD III: EFICACIA PROBATORIA Y DESAFÍOS EN CASOS DE APROPIACIÓN FRAUDULENTA POR MEDIOS ELECTRÓNICOS

En esta última unidad se analizará el delito de apropiación fraudulenta contemplado en el Código Orgánico Integral Penal (COIP) de la legislación ecuatoriana, enfocándose en los elementos objetivos y subjetivos que lo componen. Además, se valorará el sistema de obtención, preservación y presentación de pruebas digitales, tal como se establece en los manuales de organismos internos. A continuación, se estudiará la eficacia probatoria de las pruebas digitales en el contexto del delito mencionado. Finalmente, se examinará la actividad probatoria específica del delito de apropiación fraudulenta.

2.2.3.1 El delito de apropiación fraudulenta contemplado en el Código Orgánico Integral Penal

El delito de apropiación fraudulenta por medios electrónicos se encuentra regulado en el Capítulo Noveno, titulado “Delitos contra la propiedad”, artículo 190 del Código Orgánico

Integral Penal (COIP). En esta normativa penal, la conducta delictiva de naturaleza informática se manifiesta de la siguiente manera:

> La persona que utilice fraudulentamente un sistema informático o redes electrónicas y de telecomunicaciones para facilitar la apropiación de un bien ajeno o que procure la transferencia no consentida de bienes, valores o derechos en perjuicio de esta o de una tercero, en beneficio suyo o de otra persona, alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas, sistemas informáticos, telemáticos y equipos terminales de telecomunicaciones, será sancionada con pena privativa de libertad de uno a tres años.

2.2.3.2 Obtención, preservación de pruebas digitales en el delito de apropiación fraudulenta

Según el Manual del Subsistema de investigación técnico científica en materia de medicina legal y ciencias forenses sobre peritajes que se llevan a cabo a nivel nacional, provisto por el Servicio Nacional de Medicina Legal y Ciencias Forenses de la Policía Nacional del Ecuador, se determina qué en el ámbito de la investigación criminal y el procesamiento de pruebas digitales, la disciplina de Ingeniería Informática Forense desempeña un papel fundamental. Esta especialidad emplea metodologías y tecnologías forenses de vanguardia para la extracción, análisis y preservación de evidencia digital, con el propósito de coadyuvar en la resolución de hechos presuntamente delictivos.

Para la ejecución lícita y válida de estas diligencias periciales como la obtención de la evidencia digital, se requiere cumplir con ciertos presupuestos procesales: la emisión de un mandamiento por parte de la autoridad competente que ordena la pericia, la determinación precisa de la ubicación de los indicios digitales y la disponibilidad de recursos técnicos y metodológicos actualizados para su análisis. Estas pericias especializadas se llevan a cabo primordialmente en dependencias judiciales designadas como Jefaturas Zonales “Tipo 1”, las cuales se presume cuentan con la infraestructura y capacidad técnicas necesaria para abordar casos de complejidad en el ámbito de la informática forense (Jácome et al., 2022).

Mientras, que para el efecto de preservar las evidencias de naturaleza digital es imprescindible la aplicación de la cadena de custodia, misma que constituye un conjunto de procedimientos estandarizados cuyo propósito fundamental es garantizar la autenticidad e integridad de los elementos probatoria obtenidos en el curso de una investigación penal. Este proceso se inicia en el momento y lugar de la recolección de los indicios o evidencias. Su

implementación implica el registro detallado de cada persona que tiene contacto con los elementos probatorias, así como la documentación de cualquier manipulación, traslado o análisis realizado sobre estos. El objetivo primordial es asegurar que los elementos de prueba presentados ante un tribunal de justicia sean los mismos que fueron recolectados inicialmente y que no hayan sufrido alteraciones que pudieran comprometer su valor probatorio (Fiscalía General del Estado, 2016)

La responsabilidad de mantener la cadena de custodia recae sobre diversos actores del sistema de justicia, incluyendo personal de investigación, peritos forenses, custodios de centros de acopia y cualquier otro servidor público o particular que tenga acceso a los elementos probatorios durante el proceso investigativo y judicial (Fiscalía General del Estado, 2016).

2.2.3.4 Eficacia probatoria de las pruebas digitales en el delito de apropiación fraudulenta

El artículo 76 de la Constitución de la República del Ecuador, en su numeral 4, establece que "las pruebas obtenidas o actuadas con violación de la Constitución o la ley no tendrán validez alguna y carecerán de eficacia probatoria". Este artículo es claro en señalar que los medios probatorios en el proceso penal deben ser practicados con estricto apego y observación a la norma constitucional para que gocen de plena validez dentro del proceso penal.

La eficacia probatoria se refiere a la capacidad o aptitud de una prueba para demostrar un hecho relevante en un proceso penal y generar convicción en el juzgador. Es la fuerza o valor probatorio que tiene un medio de prueba para acreditar un hecho controvertido. Según López (2015), su utilidad en el procedimiento penal radica principalmente en los siguientes aspectos:

A. **Permite determinar la verdad de los hechos:** Las pruebas eficaces ayudan a reconstruir lo sucedido y esclarecer los hechos materia de investigación
B. **Fundamenta la decisión del juzgador:** Proporciona elementos para que el juez pueda motivar adecuadamente su sentencia, sea condenatoria o ratificatoria de inocencia.
C. **Garantiza el debido proceso:** La valoración de pruebas eficaces asegura que la decisión judicial se base en elementos objetivos y no en meras presunciones.
D. **Desvirtúa la presunción de inocencia:** Pruebas con alta eficacia probatoria permiten destruir el estado de inocencia del acusado más allá de toda duda razonable.

E. **Individualiza la pena:** Ayudan a determinar el grado de participación y responsabilidad del acusado

La eficacia probatoria es fundamental para cumplir la finalidad del proceso penal de esclarecer los hechos y determinar responsabilidades de manera justa y apegada a derecho. Una adecuada valoración de la eficacia de las pruebas es esencial para una correcta administración de justicia penal.

Admisibilidad y valoración de pruebas en el proceso judicial

La admisibilidad probatoria está intrínsicamente vinculada a la legalidad de los elementos de convicción. En este sentido, los medios probatorios deben ajustarse estrictamente a las disposiciones normativas que regulan su incorporación al proceso judicial. Adicionalmente es importante que los elementos probatorios cumplan requisitos de pertinencia, mismos que implican la relación directa y sustancial con el hecho típico, antijurídico y culpable que es objeto de la controversia jurídica en cuestión.

En consonancia con lo establecido en el Código Orgánico Integral Penal (COIP), se han instituido diversos principios rectores en materia probatoria, los cuales tienen como finalidad orientar los procesos de obtención, valoración y aplicación de elementos probatorios en el marco del procedimiento penal. Estos principios han sido concebidos con el propósito de salvaguardar la equidad y justicia procesal.

En este contexto, el principio de legalidad, consagrado en el artículo 5 del mencionado cuerpo normativo, estipula que la producción y presentación de pruebas deben ajustarse estrictamente a los preceptos legales vigentes. En consecuencia, aquellos elementos probatorios que sean obtenidos mediante procedimientos que contravengan la ley o que vulneren derechos fundamentales, serán considerados inadmisibles en el proceso penal, careciendo de toda eficacia jurídica.

En el marco del ordenamiento jurídico procesal penal, el principio de necesidad de la prueba está implícito en varias disposiciones del código, rigiéndose como un precepto fundamental que exige la presentación de elementos probatorios indispensables para el esclarecimiento de los hechos materia de investigación y la determinación de la responsabilidad penal del procesado. Este principio implica que la actividad probatoria debe ser proporcional y pertinente en relación con el objeto del proceso.

Concomitantemente, el principio de pertinencia probatoria previsto en el artículo 454 del COIP, establece que los elementos de convicción deben guardar una relación directa y

lógica con los hechos que son objeto de la investigación penal. En virtud de este principio, se admiten únicamente aquellas pruebas que revisten relevancia sustancial y demuestran una conexión racional con las circunstancias fácticas.

Así también principio de exclusión probatoria, previsto en el artículo 454 del COIP, establece que cualquier elemento de convicción o prueba que haya sido obtenido mediante la transgresión de derechos fundamentales reconocidos en la constitución, en tratados internacionales de derechos humanos o en la legislación vidente, será considerado carente de eficacia probatoria en el proceso penal. Esta disposición normativa se encuentra íntimamente ligada al principio de necesidad en materia probatoria, por cuanto establece un criterio de admisibilidad basado en la licitud de la obtención de la prueba.

En efecto, estos principios, en conjunto tienen como finalidad garantizar la eficacia y economía procesal en la actividad probatoria, evitando la incorporación de elementos probatorios inconducentes que pudieren dilatar innecesariamente el proceso penal o desviar la atención de los hechos jurídicamente relevantes.

Por otro lado, el Código Orgánico General de Procesos (COGEP), como norma supletoria, en su Título II denominado "Prueba", artículo 160, enfatiza que para que la prueba sea admitida debe reunir los requisitos de pertinencia, utilidad y conducencia.

Pertinencia

Según la doctrina, la pertinencia se vincula con el hecho de que la prueba es adecuada para demostrar los hechos que son objeto del proceso. El medio probatorio debe tener una conexión, directa o indirecta, con los hechos en litigio, y efectivamente aportar al debate que se desarrolle en el juicio (Mazón, 2021). La base legal que acredita la pertinencia de la prueba se sitúa en el segundo inciso del artículo 161 del COGEP, que dispone: "La prueba deberá referirse directa o indirectamente a los hechos o circunstancias controvertidos".

Conducencia

La conducencia se relaciona con la idoneidad legal del medio para demostrar un hecho específico en el proceso judicial. Implica que no exista una norma legal que prohíba el uso de este medio para probar un hecho determinado. Como ha señalado Parra (2007), "La conducencia es una comparación entre el medio probatorio y la ley, con el fin de determinar si el hecho puede ser demostrado en el proceso mediante el uso de este medio probatorio" (p.153).

Utilidad

Un medio probatorio se considera útil cuando contribuye a establecer un hecho controvertido que aún no ha sido demostrado por otros medios de prueba. La utilidad es complementaria e intrínseca a la prueba, vinculada a la eficacia del medio probatorio, cuyo objetivo central es persuadir al juez sobre los hechos alegados (Mazón, 2021). Para que una prueba sea admitida y tenga validez en el proceso penal en Ecuador, debe cumplir con los requisitos de pertinencia, conducencia y utilidad, siempre observando el estricto apego a la Constitución y las leyes vigentes.

2.2.3.3 Factores que inciden en la actividad probatoria del delito de apropiación fraudulenta

Los delitos de naturaleza informática, como el delito de apropiación fraudulenta, enfrentan una serie de desafíos significativos relacionados con la obtención de medios de prueba para demostrar su materialidad y establecer responsabilidades penales. Estos delitos han complicado considerablemente las investigaciones digitales. Algunos de los desafíos clave incluyen: la falta de planeación y técnicas adecuadas para la obtención de evidencia digital, escasa adopción de tecnologías legales (legal tech), carencia de mecanismos de cooperación regional.

A. Falta de planeación y técnicas adecuadas para la obtención de evidencia digital

La falta de planeación adecuada y de técnicas especializadas para la obtención de evidencia digital constituye uno de los principales obstáculos en las investigaciones digitales. Estas investigaciones requieren una meticulosa planificación y el uso de técnicas especializadas para garantizar la integridad y validez de la evidencia digital. La carencia de capacitación y recursos adecuados en este ámbito puede dificultar significativamente la recolección y preservación efectiva de la evidencia.

Además, en el proceso investigativo, la duplicación innecesaria de información entre entidades de investigación y otras instituciones, como entidades financieras u organismos gubernamentales, genera datos contradictorios y obstaculiza la fase de investigación. Además, los vacíos regulatorios existentes y las restricciones impuestas por empresas privadas de telecomunicaciones o sistemas financieros complican aún más la recolección y tratamiento de información relevante (Iuliana, 2020).

El tiempo prolongado desde la generación hasta la recolección de la evidencia digital también contribuye a su volatilidad, ya que los datos almacenados se actualizan y modifican

rápidamente. Esta dinámica dificulta mantener la integridad de la evidencia a lo largo del proceso investigativo, afectando su utilidad y validez en el contexto judicial.

B. La escasa adopción de tecnologías legales (legal tech)

La falta de iniciativas y avances en tecnologías legales (legal tech) limita la capacidad de los investigadores y fiscales para manejar eficientemente grandes volúmenes de datos digitales y aplicar métodos avanzados de análisis forense. Adicionalmente, la ausencia de desarrollo en tecnología legal también restringe el acceso y la utilización de equipos y software especializados de código abierto. Esta limitación impide que las investigaciones se ajusten adecuadamente a los estándares legales e internacionales relacionados con la identificación y la seguridad de la evidencia digital. La falta de adopción de tecnologías innovadoras y de código abierto en este campo deja a los investigadores en desventaja para enfrentar los desafíos cada vez más complejos de la ciberseguridad y los delitos informáticos (Bedner et al., 2009).

C. Carencia de mecanismos de cooperación regional

La cooperación efectiva entre países y regiones juega un papel fundamental en la investigación y persecución de delitos informáticos, los cuales frecuentemente trascienden fronteras nacionales. La falta de mecanismos claros y eficaces de cooperación recíproca entre las autoridades judiciales y policiales de diferentes países puede significativamente obstaculizar los esfuerzos para combatir estos delitos de manera efectiva (Council of Europe, 2001).

Especialmente relevante es la ausencia de la ratificación del Convenio de Budapest por parte de Ecuador, lo cual constituye un factor crítico en este contexto. El Convenio de Budapest es un instrumento fundamental en la lucha contra la ciberdelincuencia, ya que establece un marco para la cooperación internacional en la prevención y persecución de amenazas cibernéticas y actividades delictivas en línea. Facilita la armonización de leyes y reglamentos entre los países signatarios, lo cual es crucial para el enjuiciamiento transfronterizo de infractores y la mejora de las medidas de ciberseguridad a nivel global.

La adhesión de Ecuador al Convenio de Budapest no solo promovería una cooperación más eficaz en la investigación de delitos informáticos, sino que también fortalecería la capacidad del país para enfrentar los desafíos cada vez más complejos del ciberespacio. Además, fomentaría la confianza internacional en los sistemas judiciales y de seguridad digital del país, contribuyendo así a un entorno más seguro y protegido contra las amenazas cibernéticas transnacionales.

CAPÍTULO III

3. METODOLOGÍA

3.1 Unidad de análisis

El objetivo fundamental del presente estudio investigativo consiste en la realización de un análisis jurídico-doctrinario exhaustivo sobre la eficacia probatoria en casos de apropiación fraudulenta a través de medios electrónicos. La investigación, dada su naturaleza, se enmarca en un diseño no experimental, sustentándose primordialmente en el examen pormenorizado del marco normativo vigente y la literatura jurídica especializada.

Subsecuentemente, se procederá con el análisis de un proceso judicial vinculado a la conducta típica objeto de estudio, complementado por un estudio de derecho comparado entre las legislaciones peruanas y española en la materia. Finalmente, se llevarán a cabo entrevistas estructuradas a los titulares de la acción penal pública adscritos a las III Unidades de Patrimonio Ciudadano, así como a un perito informático de la Policía Nacional del Ecuador con competencia en la Zona 3.

3.2 Métodos

Para realizar el análisis de la problemática derivada por la eficiencia probatoria en el delito de apropiación fraudulenta por medios electrónicos, se utilizarán los siguientes métodos de investigación:

- Método dogmático
- Método analítico
- Método histórico- lógico
- Método jurídico
- Método de comparación jurídica

3.2.1 Método dogmático

El presente método evalúa la sistematización e interpretación de la normativa positiva que aborda el estudio de fuentes de derecho como la jurisprudencia, la dogmática; en conjunto de sus precedentes (Bernaconi, 2021). Método a ser aplicado bajo la examinación de normativa como el artículo 190 del COIP, en conjunción de la revisión doctrinaria jurídica relevante sobre la prueba digital y doctrina sobre derecho procesal penal, derecho informático que estén asociados con la prueba digital y a su vez con su validez procesal.

3.2.2 Método analítico

El método analítico se empleará para dilucidar el alcance y sentido de las disposiciones normativas pertinente al objetivo de estudio, realizando una interpretación sistemática. Mediante la aplicación de este método, se procederá al análisis pormenorizado de las dos variables que conforman el núcleo de la presente investigación: la variable dependiente, constituida por la eficacia probatoria; y la variable independiente, representada por la conducta típica de apropiación fraudulenta a través de medios electrónicos.

3.2.3 Método histórico-lógico

Se consolida como un método teórico enfocado en la evolución histórica, matizando los aspectos generales de su desarrollo, las tendencias de progreso, sus conexiones causales y secuenciales, posibilitando la comprensión histórica del delito informático configurado como "Apropiación fraudulenta por medios electrónicos" (Villabella, 2020). Método que incorporará el estudio de la evolución de la leyes y normativas relacionadas con los delitos informáticos y la evidencia digital, así como la examinación de normativas reformadas vinculadas con los avances tecnológicos.

3.2.3 Método jurídico

De conformidad con lo expuesto por Clavijo et al. (2017) , el método jurídico se rige como un instrumento metodológico que centra su aplicación en el establecimiento de procedimiento lógicos- deductivos, los cuales implican el estudio de las fuentes formales del derecho como la ley en calidad de fuente primaria, la jurisprudencia como interpretación vinculante emanada por los órganos jurisdiccionales competentes; y la doctrina, como fuente auxiliar del derecho. El propósito fundamental de este método radica en la valoración jurídica de las normas positivizadas vinculadas con la conducta punible a ser estudiada, tipificada en el artículo 190 del COIP, en conjunto del artículo 76 de la Constitución de la República de la República. Permitiendo así una aproximación hermenéutica integral al ordenamiento jurídico penal.

3.2.4 Método de comparación jurídica

El método de comparación jurídica se focaliza en la comparación de sistemas jurídicos que involucran la comprensión de los diferentes modelos o sistemas legales preexistentes en el mundo (Morán, 2002). En efecto, se realizará la comparación jurídica entre dos países con marcos legales avanzados en regulación de delitos informáticos como España y Perú, estudio que evaluará los procedimientos de recolección, preservación de las pruebas electrónicas de las legislaciones previamente señaladas.

3.3 Enfoque de la Investigación

Por las características de la investigación, se asumirá un enfoque mixto, porque se apoya de una estudio cuantitativo y cualitativo, compuesto por la integración dinámica de revisión bibliográfica, el estudio de caso y la ejecución de entrevistas.

3.4 Tipo de Investigación

Por los objetivos que se pretende alcanzar, la presente investigación es de tipo dogmática, histórica jurídica, jurídica correlacional y jurídica descriptiva.

3.4.1 Dogmática

La presente investigación empleará la investigación dogmática que aboca el análisis sistemático y crítico de la estructura del Derecho positivo aplicable. Este estudio comprenderá un examen exhaustivo de las normas jurídicas vigentes y doctrina imperante. En efecto, este análisis dogmático permitirá dilucidar la configuración normativa del delito, sus elementos constitutivos y los desafíos probatorios en el ámbito procesal de la apropiación fraudulenta por medios electrónicos.

3.4.2 Histórica jurídica

El presente tipo de investigación se centrará en la comprensión de la génesis y evolución del fenómeno delictivo en cuestión. Conforme lo expuesto Tantaleán (2016), se ajustará la investigación en la ejecución del análisis diacrónico del derecho, examinando su desarrollo y transformación a lo largo del tiempo.

3.4.3 Jurídica correlacional

Tiene como fin medir o determinar la influencia, impacto o incidencia de una variable sobre otra. Es decir que se valorará como la eficacia probatoria influye sobre el delito de apropiación fraudulenta por medios electrónicos. Efectuando correlaciones o conexiones significativas entre las variables dependiente e independiente.

3.4.4 Jurídica descriptiva

La investigación descriptiva en el ámbito jurídico tiene por objeto la caracterización pormenorizada de las cualidades y atributos inherentes al problema, fenómeno o hecho jurídico objeto de estudio, adhiriéndose a los protocolos metodológicos preestablecidos y consensuados por la comunidad científica jurídica, conforme a lo expuesto por Carruitero Lecca (2014) En el contexto específico de la presente investigación, se procederá a realizar una exégesis exhaustiva de la normativa aplicable, así como un análisis dogmático de los elementos

constitutivos del tipo penal de apropiación fraudulenta perpetrada mediante medios electrónicos.

3.5 Diseño de Investigación

Debido a la complejidad inherente de la investigación, los objetivos a alcanzar, los métodos a utilizar en el análisis del problema jurídica y la naturaleza del estudio, el diseño es no experimental. Este enfoque metodológico permitirá efectuar un análisis exhaustivo de las fuentes jurídicas y doctrinales vinculadas al delito de apropiación fraudulenta, con el propósito de determinar los factores exógenos y endógenos que inciden en la eficacia probatoria de la conducta típica objeto de estudio.

La investigación tiene como fundamentos, bases doctrinales, y legales. Reconociendo como actores principales de la investigación a los fiscales de las unidades de patrimonio ciudadano y peritos informáticos. Todos los sujetos antes mencionados conforman una estructura para fijar los factores que intervienen en la investigación de delitos de naturaleza informática. Aplicando técnicas de investigación como análisis doctrinas, y entrevistas, entre otros.

3.6 Población y muestra

a) **Población:** La población de estudio que participará en la investigación será la siguiente:

Tabla 4 Población

POBLACIÓN	UNIDAD DE ANÁLISIS	NÚMERO
Fiscalía General del Estado	Fiscales de las Unidades de Patrimonio Ciudadano	3
Perito	Perito informático Zona 3	1

Elaborado por: Katherine Sisa Lema

b) **Muestra:** A efectos de la determinación de la muestra representativa, se procederá a la inclusión de la totalidad del universo poblacional objeto de estudio.

3.7 Técnicas e instrumentos de investigación

Para la recopilación de la información se aplicaron las siguientes técnicas e instrumentos:

3.7.1 Técnicas para el tratamiento de información

El desarrollo de la investigación se efectuará bajo la empleabilidad de dos técnicas de estudio; la prima enfocada en la realización de entrevistas, la segunda que se configura bajo la ejecución de una técnica análisis documental comparado

Entrevistas: Se instituirá de manera verbal en la población descrita en la tabla N°5

Análisis comparado: Comparación jurídica efectuada entre la legislación peruana y española.

3.7.2 Instrumento de investigación

Guía de entrevista

Tabla de derecho comparado

3.8 Hipótesis

Hipótesis positiva: La eficacia probatoria de la apropiación fraudulenta por medios electrónicos se garantiza por la adecuada implementación de protocolos de manejo de evidencia digital.

Hipótesis negativa: La deficiencia probatoria de la apropiación fraudulenta por medios electrónicos se halla incidida por la falta de estandarización de protocolos de manejo de evidencia digital.

CAPÍTULO IV

4. RESULTADOS Y DISCUSIÓN

4.1 Resultados

4.1.1. Análisis de los elementos del delito prescrito en el artículo 190 del COIP

4.1.2 Análisis del procesamiento de los tipos de prueba en casos de apropiación fraudulenta por medios electrónicos: España, Perú y Ecuador

Tabla 4 Tabla comparativa del procesamiento de los tipos de prueba en casos de apropiación fraudulenta

	España	**Perú**	**Ecuador**
	Código Penal	**Ley N° 30096**	**COIP**
Tipificación penal del delito	**Art. 249 literal 1 Fraude Informático** Los que, con ánimo de lucro, obstaculizando o interfiriendo indebidamente en el funcionamiento de un sistema de información o introduciendo, alterando, borrando, transmitiendo o suprimiendo indebidamente datos informáticos o valiéndose de cualquier otra manipulación informática o artificio semejante, consigan una transferencia no consentida de cualquier activo patrimonial en perjuicio de otro. **b)** Los que, utilizando de forma fraudulenta tarjetas de crédito o débito, cheques de viaje o cualquier otro instrumento de pago material o inmaterial distinto del efectivo o los datos obrantes en cualquiera de ellos, realicen operaciones de cualquier clase en perjuicio de su titular o de un tercero.	**Art.8 Fraude Informático** El que deliberadamente e ilegítimamente procura para sí o para otro un provecho ilícito en perjuicio de tercero mediante el diseño, introducción, alteración, borrado, supresión, clonación de datos informáticos, o cualquier interferencia o manipulación en el funcionamiento de un sistema informático, será reprimido con una pena privativa de libertad no menor de tres ni mayor de ocho años y con sesenta a ciento veinte días-multa. La pena será privativa de libertad no menor de cinco ni mayor de diez años y de ochenta a ciento cuarenta días-multa cuando se afecte el patrimonio del Estado destinado a fines asistenciales o a programas de apoyo social	**Art. 190** La persona que utilice fraudulentamente un sistema informático o redes electrónicas y de telecomunicaciones para facilitar la apropiación de un bien ajeno o que procure la transferencia no consentida de bienes, valores o derechos en perjuicio de esta o de una tercero, en beneficio suyo o de otra persona, alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas, sistemas informáticos, telemáticos y equipos terminales de telecomunicaciones, será sancionada con

	Serán sancionados con una pena de prisión de seis meses a tres años.		pena privativa de libertad de uno a tres años
Normas que regulen el proceso de recolección, preservación y análisis de la evidencia digital	Ley de Enjuiciamiento Criminal- Capítulo V Normativa Internacional ISO/IEC 27037	Manual para el Recojo de la Evidencia Digital	Manual del Subsistema de investigación técnica científica en materia de medicina legal y ciencias forenses
Recolección de evidencia digital	Asegura la escena, se procede con la identificación del tipo de evidencia volátil o no volátil y se efectúa con la confiscación de las contraseñas, códigos o PIN de personas involucradas, actuaciones que deben debidamente autorizadas según las normas previstas.	Se procede con la identificación de la evidencia digital, sus fuentes y naturaleza informática.	Emisión de la autorización judicial para la recolección de los indicios digitales, la ubicación precisa de los indicios.
Preservación de la evidencia digital	Antes de iniciar con la cadena de custodia se genera una copia o imagen, bajo el aislamiento de dispositivos e instalación de software de bloqueo.	Empleo del mecanismo de seguridad imagen forense; así como el sometimiento de la evidencia a la cadena de custodia	Los tipos de pruebas volátiles y no volátiles se someten a la cadena de custodia
Análisis de la evidencia digital	La evidencia es remitida y analizada en centros de acopio especializados como laboratorios forenses acreditados.	Para que la evidencia sea analizada, los peritos informáticos deben contar con el acta de hallazgo, recogida, acta de incautación, el acta de entrega y la autorización del usuario o judicial que dispongan el análisis informático.	Los indicios digitales son evaluados en la Jefaturas Zonales “Tipo 1”

Elaborado por: Katherine Sisa (2024)

4.1.3 Análisis de entrevistas sobre la eficacia de las pruebas obtenidas en casos de apropiación fraudulenta por medios electrónicos

A continuación, se detalla los resultados de las entrevistas efectuadas a 4 expertos, 3 fiscales de las Unidades de patrimonio ciudadano y un perito informático de la Zona 3. La primera sección divida en resúmenes de los entrevistados y la segunda compuesta por cinco categorías vinculadas con el objeto de estudio.

Resumen de entrevistas

Entrevista 1 dirigida al Agente Fiscal de la I Unidad de Patrimonio Ciudadano

La entrevistada se desempeña como Agente Fiscal de la I Unidad de Patrimonio Ciudadano en el cantón Riobamba, con una destacada trayectoria de 13 años en el campo. La fiscal matiza la importancia de probar la existencia de un sujeto activo que utiliza redes o medios de telecomunicaciones para generar un perjuicio patrimonial, enfatizando que estas apropiaciones pueden involucrar no solo dinero, sino también valores, derechos y activos digitales. En cuanto a la eficacia probatoria, la fiscal señala la crucial importancia de la originalidad y la "virginidad" de las pruebas digitales. Destaca el papel fundamental de los peritos informáticos en la recolección y análisis de evidencias, así como la necesidad de preservar la integridad de los datos para su admisibilidad en los tribunales.

Entrevista 2 dirigida al Agente Fiscal de la II Unidad de Patrimonio Ciudadano

La entrevistada se desempeña como Titular de la acción penal pública de la mencionada unidad en el cantón Riobamba, con una amplia trayectoria de 18 años en el campo. En efecto, la fiscal destaca la complejidad de los delitos de naturaleza informática debido al avance de la ciberdelincuencia y la sofisticación de las técnicas empleadas, como el uso de malware y el hackeo de sistemas bancarios. La fiscal enfatiza la importancia crucial de las pericias informáticas para establecer la materialidad del delito, identificando direcciones IP y patrones de acceso fraudulento. Destaca la importancia de mantener una adecuada cadena de custodia para las pruebas digital, en función de evitar la impunidad en este tipo de delitos, por la falta de prueba que demuestre la materialidad de la conducta punible. Concluye que es imperativo mejorar las capacidades técnicas y de investigación, la correcta aplicación de la cadena de custodia, así como fortalecer la cooperación internacional para enfrentar eficazmente estos delitos en un mundo cada vez más digitalizado.

Entrevista 3 dirigida al Agente Fiscal de la III Unidad de Patrimonio Ciudadano

El entrevistado cuenta con una amplia trayectoria de 17 años en la unidad referida en la ciudad de Riobamba. Su formación académica se focaliza en la obtención de una maestría en Derecho Digital, Derecho Procesal penal, Derecho Constitucional y actual docente universitario. El fiscal enfatiza la importancia de las pruebas digitales y periciales informáticas para establecer la existencia de transferencias no autorizadas y la manipulación de sistemas informáticos. Sin embargo, señala obstáculos asociados con la escasez de peritos especializados en fiscalía, y la falta de unidades técnicas de respuesta inmediata para la

obtención de la evidencia digital. Secuencialmente enfatiza la necesidad de seguir protocoles estrictos en el manejo de evidencia digital, desde su recolección hasta su presentación como prueba. Además, menciona dificultades en la obtención oportuna de información de entidades bancarias y la importancia de la cooperación internacional en casos que involucran delincuencia cibernética transnacional. Finalmente, sostiene la difícil investigación de los delitos de naturaleza informática y su alta tasa de impunidad.

Entrevista 4 dirigida al Perito Informático de la Zona 3

La entrevista efectuada al único perito informático con competencia en la Zona 3, ingeniero informático de profesión. Proporciona una visión detallada sobre los desafíos y procesos involucrados en la recolección y análisis de evidencia digital en casos de apropiación fraudulenta por medios electrónicos. Enfatiza la necesidad de documental meticulosamente cada paso del proceso para mantener la integridad de la cadena de custodia. El perito reconoce que los manuales internacionales y normas ISO para guiar sus procedimientos no son suficientes debido al rápido avance de la tecnología. Se señala la necesidad de una mejor comunicación entre los abogados, fiscales y peritos para definir claramente los objetivos de las investigaciones, y menciona que, a pesar de estar bien capacitados, el número insuficiente de peritos informáticos representa una barrera significativa en el manejo eficaz de estos casos.

Categorías de las entrevistas efectuadas a fiscales

- Categoría 1. Elementos claves del delito de apropiación fraudulenta por medios electrónicos
- Categoría 2. Modalidades de apropiación fraudulenta
- Categoría 3. Admisibilidad de los medios probatorios digitales
- Categoría 4. Retos que afronta la investigación y procesamiento del delito prescrito en el artículo 190 del COIP

Tabla 5 Análisis de las categorías previstas en las entrevistas dirigidas a Fiscales de la ciudad de Riobamba

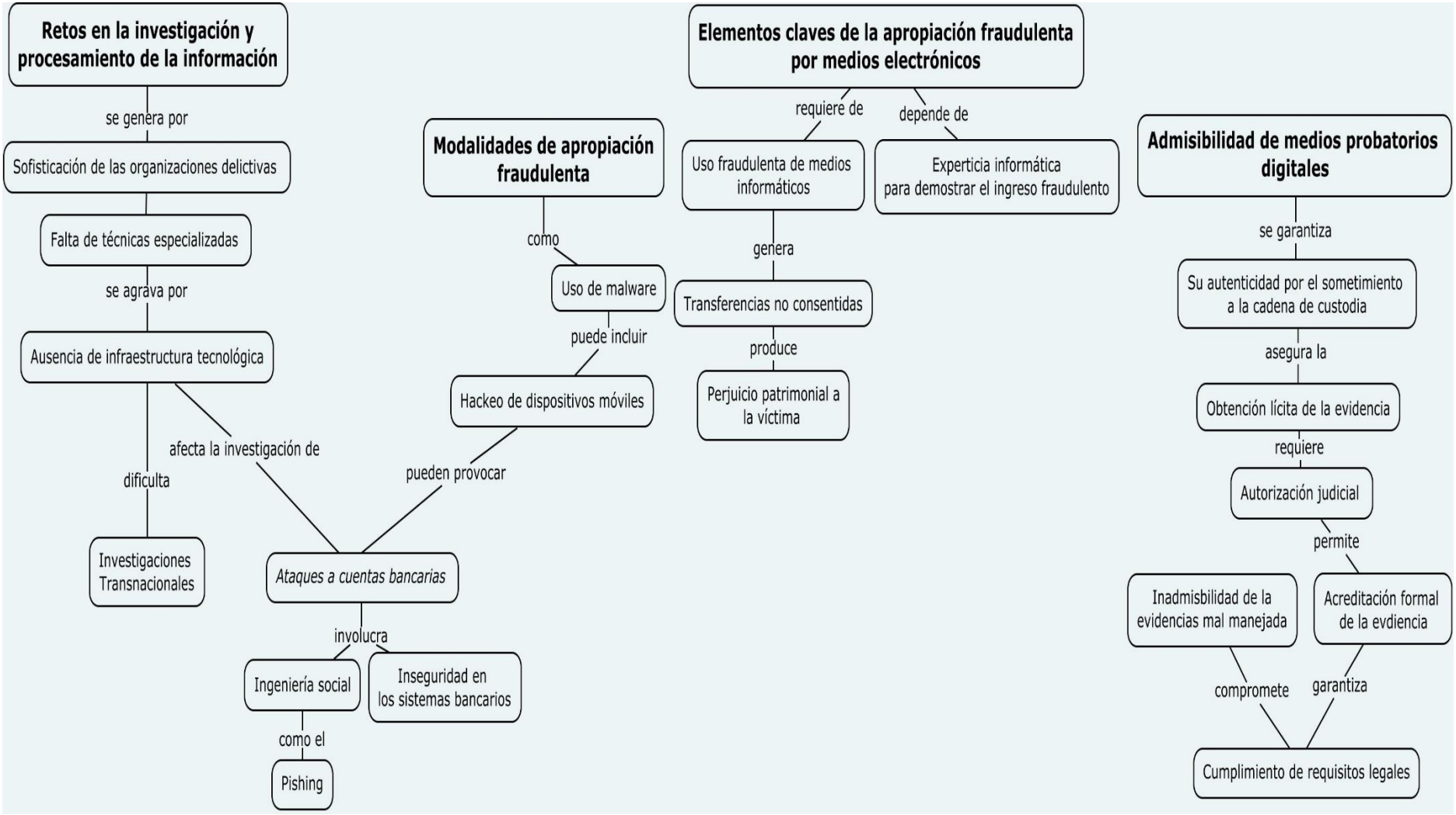
Categoría 1: Elementos claves en el delito de	De las entrevistadas efectuadas se concluye que el delito de apropiación fraudulenta por medios electrónicos, tipificado en el artículo 190 del COIP, se caracteriza por la utilización fraudulenta y dolosa de sistemas informáticos, redes electrónicas o de telecomunicaciones por parte de cualquier sujeto activo, con el fin de facilitar una apropiación ilícita de recursos ajenos. Este ilícito no requiere acceso físico directo al dispositivo y se consuma mediante transferencias no consentidas que perjudican el patrimonio de la víctima. La

apropiación fraudulenta por medios electrónicos	eficacia probatoria en estos casos depende crucialmente de la experticia informática para establecer direcciones IP y demostrar el ingreso fraudulento a los sistemas.
Categoría 2: Modalidades de apropiación fraudulenta	Asimismo, los expertos sostienen que las modalidades más comunes bajo las cuales se efectúa la apropiación fraudulenta por medios electrónicos en el contexto nacional se clasifican en tres: la primera focalizada en el uso de malware, softwares maliciosos que infiltran los sistemas informáticos de las víctimas. Igualmente, el hackeo de dispositivos móviles, que implica el acceso no autorizado a teléfono celulares bajo la clonación y replicación de los mismos. Así también, los ataques dirigidos a cuentas bancarias, modalidad que involucra técnicas de ingeniería social, phishing o explotación de vulnerabilidades en aplicaciones bancarias móviles.
Categoría 3: Admisibilidad de los medios probatorios digitales	Además de las entrevistas se analizó que la eficacia probatoria en casos de apropiación fraudulenta por medios electrónicos está supeditada a una serie de elementos jurídicos ineludibles que determinan la admisibilidad y valoración de las pruebas digitales. En primera instancia, la autenticidad del elemento probatorio digital debe garantizarse mediante la correcta aplicación de la cadena de custodia. Esta medida asegura la inalterabilidad de la prueba desde su obtención hasta su incorporación al proceso, salvaguardando su integridad y valor probatorio. Además, la adquisición de pruebas digitales debe realizarse de manera lícita, lo que implica la obtención de una autorización judicial previa. Esto es particularmente crucial cuando se trata de acceder a información sensible, como aquella proveniente de entidades financieras, asegurando así el respeto a los derechos fundamentales y al debido proceso. Adicionalmente, la evidencia digital debe ser formalmente acreditada ante el tribunal, demostrando su procedencia, desde su origen hasta su presentación en juicio. Finalmente, el cumplimiento riguroso de estos requisitos es esencial para que las pruebas digitales sean admisibles y efectivas en el proceso judicial. Secuencialmente, se manifiesta que la inadmisibilidad de la prueba representa un desafío significativo en casos de apropiación fraudulenta por medios electrónicos. Como lo señalan los expertos "no siempre se manejan los protocolos adecuados en el tratamiento de los indicios digitales o son

	erróneamente recogidos". Esto puede resultar en que evidencia crucial sea declarada inadmisible en el proceso judicial, debilitando la capacidad de la fiscalía para demostrar la culpabilidad del acusado. La complejidad técnica de los delitos cibernéticos exige una meticulosa recolección y manejo de pruebas digitales, siguiendo protocolos forenses estrictos para garantizar su admisibilidad y eficacia probatoria en el tribunal.
Categoría 4: Retos que afronta la investigación y procesamiento del delito prescrito en el artículo 190 del COIP	Baja la ejecución de las entrevistas se dilucida que la investigación y procesamiento del delito tipificado en el artículo 190 del COIP enfrentan desafíos multifacéticos que comprometen la eficacia de la justicia penal en el ámbito cibernético. En primer lugar, la sofisticación de las organizaciones delictivas transnacionales sobrepasa las capacidades investigativas actuales. En segundo lugar, aunque la legislación ecuatoriana no reconoce la especificidad de los delitos informáticos, carece de un desarrollo robusto de técnicas investigativas especializadas. Esta deficiencia se agrava por la ausencia de una infraestructura tecnológica adecuada, evidenciada en la falta de plataformas de conexión directa con proveedores de internet. Adicionalmente, la resistencia institucional por parte de las entidades bancarias y financieras obstaculizan la obtención de pruebas fundamentales para el esclarecimiento de los hechos delictivos. Finalmente, la falta de convenios con ciertos países dificulta las investigaciones transnacionales.

Elaborado por: Katherine Sisa (2024)

Ilustración 2 Análisis de Categorías de las entrevistas efectuadas a Fiscales de la ciudad de Riobamba



Elaborado por: Katherine Sisa (2024)

Análisis de categoría de la entrevista efectuada al perito informático

- Categoría 1: Recolección de evidencia digital
- Categoría 2: Preservación de evidencia digital
- Categoría 3: Manuales de recolección de evidencia digital
- Categoría 4: Cadena de Custodia digital
- Categoría 5: Principales desafíos en el manejo y tratamiento de la evidencia digital en casos de apropiación fraudulenta por medios electrónicos

Categoría 1: Recolección de evidencia digital

De lo mencionado por el entrevistado se determinó que el proceso de recolección de evidencia digital es frecuentemente un desafío, ya que desde el principio es fundamental determinar si la evidencia es volátil o no. Dependiendo de esta característica, se procede con la utilización de herramientas específicas. En algunos casos, se emplean herramientas de acceso libre, a las que cualquier persona puede acceder. Para el análisis más avanzado, se utilizan herramientas licenciadas como *Action*, entre otras.

Categoría 2: Preservación de evidencia digital

Así también, de la información recopilada se estableció que la preservación de la evidencia digital se efectúa a través de la documentación de cada uno de los procesos realizados para la obtención de evidencia digital, se ha llevado a cabo un análisis de las bases de datos y sistemas web utilizados en este tipo de delitos. Con un manejo adecuado de la cadena de custodia, se puede asegurar la preservación de dicha evidencia digital.

Categoría 3: Manuales de recolección de evidencia digital

Ante la ausencia de un manual claramente definido para el tratamiento de la evidencia digital, se recurre a la aplicación de manuales internacionales, como los estándares ISO.

Categoría 4: Cadena de custodia digital

La cadena de custodia en el manejo de evidencia digital es similar a la utilizada para indicios físicos. Su propósito es preservar y garantizar la integridad de la información o evidencia digital desde su obtención hasta su análisis. Para ello, la evidencia digital se almacena en contenedores, como dispositivos de almacenamiento masivo (CDs, memorias flash, entre otros), donde se guarda la información relevante para el caso. Estos dispositivos se gestionan cuidadosamente dentro del proceso de cadena de custodia, individualizándolos con códigos de serie y aplicando códigos hash, que son cruciales para identificar y verificar la integridad de la información durante su análisis.

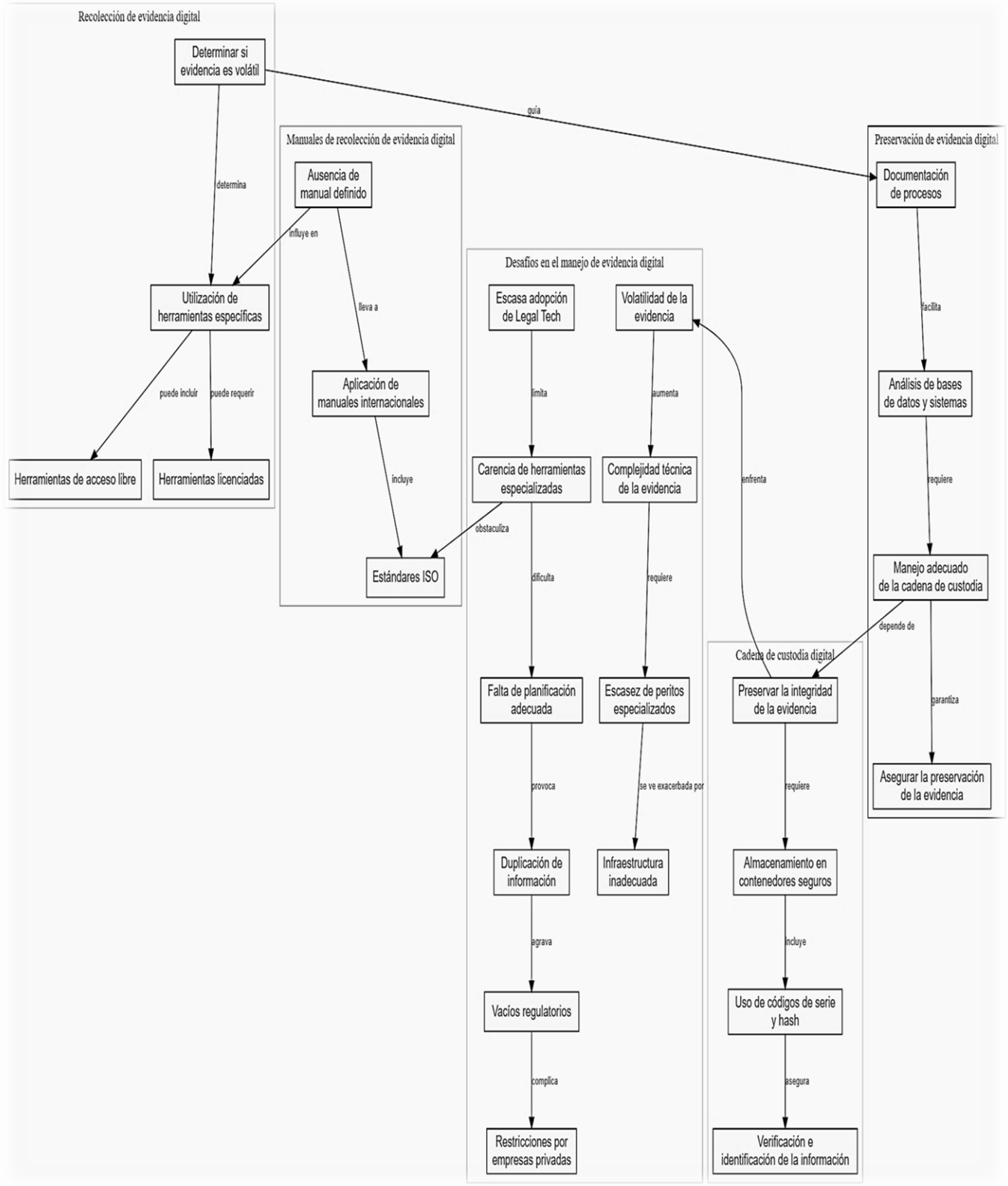
Categoría 5: Principales desafíos en el manejo y tratamiento de la evidencia digital en casos de apropiación fraudulenta por medios electrónicos.

La eficacia probatoria de la evidencia digital en casos de apropiación fraudulenta por medios electrónicos enfrenta múltiples desafíos interconectados. La escasa adopción de tecnologías legales (Legal Tech) limita significativamente la capacidad de los peritos para manejar eficientemente grandes volúmenes de datos digitales y aplicar métodos avanzados de análisis forense. Esta carencia de herramientas especializadas, particularmente de código abierto, obstaculiza el cumplimiento de estándares legales e internacionales en la identificación y seguridad de la evidencia digital.

La falta de planificación adecuada y de técnicas especializadas para la obtención de evidencia digital constituye otro obstáculo crítico. La duplicación innecesaria de información entre entidades, los vacíos regulatorios y las restricciones impuestas por empresas privadas complican aún más este panorama. Además, el tiempo prolongado entre la generación y recolección de la evidencia aumenta su volatilidad, comprometiendo su integridad y validez judicial. Estos factores, combinados con la complejidad técnica inherente a la evidencia digital, como los datos cifrados y las sofisticadas técnicas de ocultamiento utilizadas por los delincuentes, plantean desafíos significativos para su identificación y análisis efectivo.

En el contexto ecuatoriano, según la entrevista efectuada a un perito informático experto, se estima que la situación se agrava por la escasez de peritos especializados, con solo ocho profesionales concentrados en Quito para atender las necesidades de todo el país, y uno designado a la Zona 3 (Chimborazo, Tungurahua, Cotopaxi). Esta limitación se ve exacerbada por una infraestructura inadecuada, manifestada en la carencia de centros de acopio específicos para evidencias digitales y la insuficiencia y desactualización de los protocolos.

Ilustración 3 Análisis de categorías



Elaborado por: Katherine Sisa (2024)

4. Discusión de resultados

De los resultados obtenidos de la investigación vinculada con la eficacia probatoria de la apropiación fraudulenta por medios electrónicos se logró evidenciar que en la valoración de los elementos de tipicidad de la conducta delictiva prevista en el artículo 190 del COIP, se determinó que la materialidad del delito de apropiación fraudulenta por medios electrónicos se vincula estrechamente con el uso indebido de sistemas informáticos para la obtención ilícita de bienes, derechos o servicios. En el proceso penal, la demostración de esta materialidad exige la presentación de pruebas concretas que evidencien la manipulación indebida de dichos sistemas.

En este contexto, la evidencia digital se configura como un elemento crucial, cuyo valor probatorio depende en gran medida de la calidad del informa pericial elaborado por expertos en informática forense. En efecto esta prueba debe ceñirse a los estándares de los Principios de Legalidad, Necesidad, Pertinencia y Exclusión Probatoria previsto en el COIP. Según Molina Granja et al. (2019), el cumplimiento de principios como el de legalidad, así como la pertinencia, confidencialidad, autenticidad e integridad de la prueba digital en conjunto del respeto a los derechos fundamentales de terceros, respeto a las normas de protección de datos; son elementos que no solamente garantiza la admisibilidad de la prueba digital en el proceso judicial, sino que también asegura su valoración efectiva y, por ende, su eficacia probatoria.

La correcta aplicación del principio de legalidad se constituye como un pilar esencial para asegurar la validez y eficacia probatoria de la evidencia digital en el proceso penal. Este principio, consagrado en el artículo 76 de Constitución de la República del Ecuador (CRE), exige que las actuaciones procesales se ciñan estrictamente a los procedimientos establecidos en la ley. En el contexto de recolección, preservación y análisis de pruebas digitales, la observancia del principio de legalidad es indispensable para asegurar la obtención de la evidencia no vulnere derechos fundamentales como el de la privacidad, el del debido proceso y la defensa. El principio de legalidad demanda que los peritos en informática forense, como actores clave en la recolección y análisis de evidencia digital, actúen con estricta adherencia a los estándares técnicos y normativos vigentes. Cualquier desviación de estos estándares puede comprometer la validez de la prueba.

En el marco de esta investigación, se identificó que uno de los factores recurrentes que comprometen la eficacia probatoria es el manejo inadecuado de la evidencia digital. Esta problemática resalta la necesidad de realizar un análisis comparativo de la normativa

relacionada con el procesamiento de pruebas digitales en tres legislaciones: España, Perú y Ecuador; donde se observaron diferencias significativas. España, con su normativa avanzada, que incluye la Ley de Enjuiciamiento Criminal y la adopción de estándares internacionales como la ISO/IEC 27037, ofrece un marco sólido para la gestión de la evidencia digital. En contraste Perú, aunque con un marco menos desarrollado ha implementado un Manual para el Recojo de la Evidencia Digital, que proporciona directrices claras y prácticas. Por su parte, Ecuador se basa en un manual de subsistema de investigación técnica científica más general, lo cual según, según Montecé (2020), resulta insuficiente para abordar las particulares de la evidencia digital en casos complejos de ciberdelito.

No obstante, la sanción de las conductas delictivas de naturaleza informática se ha vuelto cada vez más compleja. Los expertos entrevistados destacan que las técnicas empleadas por los delincuentes se han sofisticado progresivamente, dificultando su investigación, y, en consecuencia, incrementando la impunidad asociada a estos delitos. Según lo señalado por la Universidad de Huánuco (2024), las causas recurrentes de dicha impunidad en este tipo de conductas ilícitas se debe a la falta de equipos tecnológicos indispensables para el procesamiento de evidencia digital. En el contexto nacional, la situación se agrava debido a que únicamente se cuenta con 8 peritos informáticos para atender 271 puntos de atención de Fiscalía a nivel nacional, lo que resulta claramente insuficiente para enfrentar el creciente desafío que representan los delitos informáticos.

Además, otros de los factores visibles que inciden de forma directa en la eficacia probatoria es la carencia de manuales específicos y procedimientos claros en la recolección, preservación y análisis de la evidencia digital en el contexto ecuatoriano. Ecuador puede llevar a la inadmisibilidad de pruebas, como lo destacan autores como Rodríguez y Pérez (2019), quienes señalan que la falta de estandarización en la recolección y preservación de evidencia digital puede resultar en la contaminación de la misma, comprometiendo su validez y fiabilidad en el proceso judicial.

Las entrevistas, la revisión doctrinal y jurídico-legal, revelan preocupaciones significativas respecto a la autenticidad y admisibilidad de las pruebas digitales en el proceso judicial. En las que se han identificado dificultades en la obtención oportuna de información de entidades bancarias, lo que complica aún más la labor de demostración de la materialidad del delito. Según García y Fernández (2021), la coordinación entre las entidades bancarias y las autoridades judiciales es clave para asegurar que la evidencia digital sea preservada y presentada de manera oportuna y conforme a los estándares legales. Más, sin embargo, las

entidades bancarias muchas veces no están prestas a suministrar información, accionar que genera problemas directos en la investigación, pues la prueba al ser volátil, puede desaparecer fácilmente.

Finalmente, en el presente proyecto de investigación se analizaron dos hipótesis relacionadas con la eficacia probatoria de la apropiación fraudulenta por medios electrónicos. Una vez concluida la investigación, se ha comprobado la hipótesis negativa, la cual sostiene que "la deficiencia probatoria de la apropiación fraudulenta por medios electrónicas es producida por la falta de estandarización de los protocolos de manejo de evidencia digital".

Esta conclusión se sustenta en las entrevistas realizadas a expertos y en la revisión jurídico-doctrinal, que revelaron la ausencia de un proceso adecuado para la preservación de los elementos digitales, los cuales deben fungir como medios de prueba durante la etapa de audiencia de juicio. La deficiencia probatoria de estos elementos conlleva a su admisibilidad, lo que, a su vez, dificulta demostrar la materialización del delito tipificado en el artículo 190 del COIP, generando en muchos casos la impunidad de la conducta delictiva.

CAPÍTULO V.
CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

- La tipicidad del delito de apropiación fraudulenta por medios electrónicos, según el artículo 190 del COIP, se caracteriza por el uso fraudulento de sistemas informáticos para obtener ilícitamente bienes, derechos o servicios. La materialidad de este delito depende crucialmente de la presentación de evidencias digitales que demuestren la manipulación indebida de dichos sistemas. No obstante, la falta de protocoles estandarizados para el tratamiento de la evidencia digital, así como un manejo inadecuado, han debilitado significativamente la eficacia probatoria, lo que ha llevado a que la conducta delictiva tipificada en el artículo 190 del COIP, quede en muchos casos en la impunidad.
- En el análisis comparativo entre España, Perú y Ecuador se revelan diferencias significativas en el marco normativo para el procesamiento de pruebas digitales. España cuenta con un marco más avanzado, incluyendo la adopción de estándares internacionales. Perú con un manual especifico, mientras que Ecuador se basa en un manual más general y subsidiariamente aplica las normas ISO, lo cual resulta insuficientes para abordar las particulares de la evidencia digital en casos de delitos de naturaleza informática.
- La admisibilidad y valoración efectiva de la prueba digital depende del cumplimiento de principios como legalidad, pertinencia, confidencialidad, autenticidad e integridad, así como del respeto a los derechos fundamentales y normas de protección de datos. Así también, la eficacia probatoria en casos de apropiación fraudulenta por medios electrónicos enfrenta desafíos significativos en Ecuador, que incluye la escasez de peritos informáticos especializados, la falta de manuales específicos y procedimientos claros para la recolección, preservación y análisis de evidencia digital, dificultades en la obtención oportuna de información de entidades bancarias, y la sofisticación creciente de las técnicas empleadas por los delincuentes.

5.2 Recomendaciones

- Para mejorar la eficacia probatoria en casos de apropiación fraudulenta por medios electrónicos en Ecuador, es imperativo desarrollar e implementar un manual específico para el manejo de evidencia digital. Este manual debe abordar las particularidades de los delitos informáticos y establecer procedimientos claros para la recolección,

preservación y análisis de pruebas digitales. Paralelamente, es crucial aumentar significativamente el número de peritos informáticos especializados en el sistema de justicia ecuatoriano, asegurando una distribución adecuada en todo el territorio nacional.

- En el ámbito normativo y de estandarización, se recomienda promover la adopción de estándares internacionales en el manejo de evidencia digital, como la norma ISO/IEC 27037, adaptándolos al contexto legal ecuatoriano. Esto debe ir de la mano con impulsar reformas legislativas que actualicen el marco jurídico ecuatoriano para abordar de manera más efectiva los desafíos presentados por los delitos informáticos, incluyendo disposiciones específicas sobre la obtención y manejo de evidencia digital.
- La infraestructura tecnológica del sistema de justicia requiere una mejora sustancial. Esto incluye la creación de centros de acopio específicos para evidencias digitales y la adquisición de herramientas forenses avanzadas. Además, es fundamental fortalecer la cooperación entre entidades bancarias y autoridades judiciales mediante la creación de protocolos específicos para el intercambio ágil y seguro de información en casos de delitos informáticos. Esta colaboración interinstitucional es clave para abordar eficazmente la complejidad de los delitos cibernéticos.

BIBLIOGRAFÍA

Aparicio Izurieta, V. V. (2022). Delitos informáticos en Ecuador según el COIP: un análisis documental. *Sapienza: International Journal of Interdisciplinary Studies*, *3*(1), 1057–1063. https://doi.org/10.51798/sijis.v3i1.284

Ashour, A. J., & Afan, H. A. (2023). Legalidad de la prueba electrónica en el ámbito penal "Evidencia." *Namibian Studies*, *1*, 219–231.

Bedner, P., Vasilios, K., & Hennell, C. (2009). On the complexity of collaborative cyber crime investigations. *Digital Evidence and Electronic Signature Law Review*, *6*(0), 214–219. https://doi.org/10.14296/deeslr.v6i0.1894

Bernaconi, A. (2021). El carácter científico de la dogmática jurídica. *Revista de Derecho*, *1*, 9–37.

Carriedo, L. (2022). "Delitos informáticos frente a estándares de derechos humanos y libertad de expresión en México." *Infotec*. https://infotec.repositorioinstitucional.mx/jspui/bitstream/1027/518/1/SOLUCIONESTRATEGICA_LMCT.pdf

Carruitero Lecca, F. (2014). *La investigacíon Jurídica*. *16*, 173–186. https://revistasinvestigacion.unmsm.edu.pe/index.php/derecho/article/download/10937/9861/

Casey, E. (2011). *Digital Evidence and Computer Crime*. 26.

Clavijo, D., Guerra, D., & Yánez, D. (2017). Método, Metodología y Técnicas de la Investigación Aplicada al Derecho. *Universidad de Pamplona"Programa de Derecho"*, *4*(1), 9–15.

Código Orgánico Integral Penal, 256 (2014).

Convenio de Budapest, 11 Analytical Biochemistry 1 (2001).

Fiscalía General del Estado. (2016). *Protocolo del centro de Acopio*. *0*, 1–23.

Fiscalía General del Estado. (2021). Perfil Criminológico. *Вестник Росздравнадзора*, *4*(1), 9–15.

Flórez, G., Montenegro, D., & Bernal, D. (2016). *Evidencia digital*.

García, S. (1998). *El delito de fraude* (Porrúa (ed.); Cuarta edi).

Gisin, M. (2008). Phishing. *Kriminalistik*, *62*(3), 197–200. https://doi.org/10.46647/ijetms.2022.v06i05.092

GomezJurado, J. D. (2017). Identificación del Sujeto activo en el delito de estafa a través de medios digitales y electrónicos bajo la perspectiva del COIP en Ecuador. In *Angewandte Chemie International Edition*, *6(11)*, *951–952.* http://repo.iain-tulungagung.ac.id/5510/5/BAB 2.pdf

Institute of Justice, N. (2001). *Special REPORT Electronic Crime Scene Investigation: A Guide for First Responders*. www.ojp.usdoj.gov/nij

Iuliana, A. (2020). Cybercriminals and the Victims of Cybercrime. *Journal of Law and Administrative Sciences*, *14*, 127–136.

Jácome, Cáceres, Pazmiño, E. (2022). *Manual Del Subsistema De Medicina Legal Y Ciencias Que Se Llevan a Cabo a Nivel Nacional*. 88.

Ley de Enjuiciamiento Criminal (2021).

Ley N° 30096 - Ley de Delitos Informáticos, Diario Oficial El Peruano 1 (2013). https://www2.congreso.gob.pe/sicr/cendocbib/con5_uibd.nsf/C5F98BB564E5CCCF05258316006064AB/$FILE/6_Ley_30096.pdf

Leyva Serrano, C. (2021). Estudio de los delitos informáticos y la problemática de su tipificación en el marco de los convenios internacionales. *Lucerna Iuris et Investigatio*, *1*, 29–47. https://doi.org/10.15381/lucerna.v0i1.18373

López, Y. (2015). ¿Cómo trata la Prueba el Código Orgánico Integral Penal de Ecuador? *UNIANDES EPISTEME: Revista de Ciencia, Tecnología e Innovación*, *2*(1), 26–46. https://revista.uniandes.edu.ec/ojs/index.php/EPISTEME/article/view/89/72

Manual Para El Recojo de Eviencia Digital (2019). www.mininter.gob.pe

Mazón, J. L. (2021). *Pertinencia, conducencia, utilidad y otros requisitos que deben reunir los medios probatorios*.

Miro, F. (2012). *El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio*.

Mirzakarimovna, R. (2021). Ciudadanos con comportamiento desviado. *Ilmiy-Amaliy Journal*, 3–12.

Mishra, S., & Soni, D. (2023). DSmishSMS-A System to Detect Smishing SMS. *Neural*

Computing and Applications, *35*(7), 4975–4992. https://doi.org/10.1007/s00521-021-06305-y

Molin, E. (2021). *The Development of Vishing Fraud During the Covid Pandemic*. *June*, 6.

Molina Granja, F. T., Santillán Lima, J. C., Luna Encalada, W., Lozada Yañez, R., & Guaiña Yungán, J. (2019). Preservación digital y la admisibilidad de las evidencias. *Ciencia Digital*, *3*(1.1), 118–130. https://doi.org/10.33262/cienciadigital.v3i1.1.364

Morán, G. M. (2002). El derecho comparado como disciplina jurídica: La importancia de la investigación y la docencia del derecho comparado en el ámbito jurídico. *Anuario de La Facultad de Derecho*, *6*, 501–530. http://www-isdc.unil.ch/divers/Rapp-

Muñoz, E. (2022). Apropiación Indebida. Un Abuso de Confianza. *Anuario de Derecho*, 94–108.

Ochoa, P. (2018). El tratamiento de la evidencia digital, una guía para su adquisición y/o recopilación. *Revista Economía y Política*, *XIV*(28), 35–46. https://doi.org/10.25097/rep.n28.2018.03

Osco, A., Chipana, Y., Quiñones, L. A., Díaz, J., Calvo, D., & García, G. (2024). Digital Evidence As a Means of Proof in Criminal Proceedings. *Russian Law Journal*, *18*(4), 96–105. https://doi.org/10.24857/rgsa.v18n4-028

Parra, J. (2007). *Manual de Derecho Probatorio* (Décima Sex).

Sempertegui, M. P. (2022). *Delito de Apropiación Fraudulenta por medios electrónicos bajo la modalidad de phising dentro del marco jurídico ecuatoriano*.

Sosa, M. E. (2023). Evidencia Digital. *Columna de La Revista Pensamiento Penal*, *466*, 1–4.

Tantaleán, R. (2016). Tipología De Las Investigaciones Jurídicas. *Derecho y Cambio Social*, *2224–4131*, 1–32. https://dialnet.unirioja.es/servlet/articulo?codigo=5456267

Universidad de Costa Rica. (2009). *Fraude Informático*. 1–28.

Universidad de Huánuco. (2024). *La impunidad en los delitos informáticos. Una problemática de poco interés para legisladores, jueces y fiscales*. *7*(9), 91–115. https://doi.org/10.35292/iusVocatio.v7i9.928

Universidad de Jaén. (2018). *Software malicioso*. 3.

Villabella, C. (2020). Los métodos en la investigación jurídica. In *Universidad Nacional*

Autónoma de México (pp. 161–177). https://webcache.googleusercontent.com/search?q=cache:czIATCpEvboJ:https://archivos.juridicas.unam.mx/www/bjv/libros/13/6226/12a.pdf+&cd=1&hl=es&ct=clnk&gl=co

Villanueva, & Andrade, M. (2020). *Ciberdelincuencia, enfocada en la apropiación de información a través de medios electrónicos y su influencia en el cometimiento de delitos informáticos*.

Wilson, D., Helm, R., Growns, B., & Redfern, L. (2023). Digital evidence in defence practice: Prevalence, challenges and expertise. *International Journal of Evidence and Proof*, *27*(3), 235–253. https://doi.org/10.1177/13657127231171620

Yendan, R. (2023). La no adhesión al convenio de Budapest vulnera los derechos en delitos informáticos. *Angewandte Chemie International Edition, 6(11), 951–952.*, 5–24.

ANEXOS

1. Guías de entrevistas

UNIVERSIDAD NACIONAL DE CHIMBORAZO

FACULTAD DE CIENCIAS POLÍTICAS Y ADMINISTRATIVAS

CARRERA DE DERECHO

CONSENTIMIENTO INFORMADO

Título del estudio: La eficacia probatoria en la apropiación fraudulenta por medios electrónicos

Investigador Principal: Katherine Stefania Sisa Lema

Propósito del estudio: Analizar y evaluar la eficacia de las pruebas digitales en los casos de apropiación fraudulenta utilizando medios electrónicos, conforme al artículo 190 del COIP, con el fin de identificar desafíos y desarrollar recomendaciones para su mejor aplicación en la fiscalía.

Procedimiento: Se llevará a cabo una entrevista estructurada con duración aproximada de 30 minutos. Durante la entrevista, se abordarán temas relacionados con la conducta típica, la admisibilidad de la prueba digital y los retos en el procesamiento de este delito.

Confidencialidad: La información proporcionada será tratada con la máxima confidencialidad y utilizada exclusivamente para fines académicos y de investigación. Los datos serán anonimizados para proteger la identidad de los participantes.

Voluntariedad: Su participación en esta entrevista es completamente voluntaria. Si tiene interrogantes y dudas, puede efectuarlas en este preciso momento.

Declaración de Consentimiento: He leído y comprendido la información proporcionada anteriormente. He tenido la oportunidad de hacer preguntas y todas mis preguntas han sido contestadas satisfactoriamente. Entiendo que mi participación es voluntaria. Al firmar este documento, doy mi consentimiento para participar en la entrevista.

_____

FIRMA DEL PARTICIPANTE

ENCUESTA DIRIGIDA A FISCALES

Guía de Entrevista: La Eficacia Probatoria en la Apropiación Fraudulenta por Medios Electrónicos según el Artículo 190 del COIP

Objetivo de la Entrevista

El objetivo de esta entrevista es obtener información detallada sobre la eficacia probatoria en casos de apropiación fraudulenta por medios electrónicos, específicamente en el contexto de la conducta típica prevista en el artículo 190 del Código Orgánico Integral Penal (COIP).

Introducción y Contexto

Por favor, describa su experiencia y especialización en la fiscalía, específicamente en casos relacionados con delitos informáticos

Categoría 1: Elementos claves del delito de apropiación fraudulenta por medios electrónicos

¿Cuáles son los elementos clave que deben probarse y que tipo de pruebas digitales son esenciales para probar la conducta típica de apropiación fraudulenta por medios electrónicos según el artículo 190 del COIP?

Categoría 2: Modalidades de apropiación fraudulenta

¿Cuáles son las modalidades de apropiación fraudulenta más recurrentes?

Categoría 3: Admisibilidad de los medios probatorios digitales

¿Qué criterios se utilizan para evaluar la admisibilidad de pruebas digitales en casos de apropiación fraudulenta? ¿Ha enfrentado situaciones en las que las pruebas digitales fueron inadmisibles? Si es así, ¿cuáles fueron las razones?

Categoría 4: Retos que afronta la investigación y procesamiento del delito prescrito en el artículo 190 del COIP

¿Cuáles son los principales retos que enfrenta en la investigación y procesamiento de delitos de apropiación fraudulenta por medios electrónicos?

¿Qué papel juega la cooperación con otras agencias y entidades (nacionales e internacionales) en la recolección y validación de pruebas digitales?

Finalmente ¿Cuáles son sus apreciaciones finales respecto al tema?

ENCUESTA DIRIGIDA A PERITOS INFORMÁTICOS

Objetivo de la Entrevista

El objetivo de esta entrevista es obtener información detallada sobre el tratamiento de la evidencia digital en los casos de en los casos de apropiación fraudulenta por medios electrónicos, conducta tipificada en el artículo 190 COIP.

Introducción y Contexto

¿Podría proporcionar una breve descripción de los casos de apropiación fraudulenta por medios electrónicos que ha manejado?

Sección 1: Recolección de Evidencia Digital

¿Qué métodos, herramientas y proceso que utiliza para la recolección de evidencia digital en casos de apropiación fraudulenta?

Sección 2: Preservación y Análisis de Evidencia Digital

¿Cómo asegura la preservación de la evidencia digital desde el momento de su recolección hasta su análisis?

¿Qué técnicas utiliza para analizar la evidencia digital y cuáles son las dificultades más comunes que enfrenta durante el análisis de evidencia digital?

Sección 3: Manuales de Recolección de Evidencia Digital

¿Existen manuales o guías establecidos para la recolección de evidencia digital en su organización?

En caso afirmativo, ¿podría describir su contenido y aplicación?

¿Considera que estos manuales son adecuados y suficientes? ¿Por qué o por qué no?

Sección 4: Cadena de Custodia Digital

¿Cómo maneja la cadena de custodia de la evidencia digital?

Sección 5: Retos en el Tratamiento de Evidencia Digital

¿Cuáles son los principales retos que enfrenta en el manejo y tratamiento de evidencia digital en casos de apropiación fraudulenta?

Conclusión

¿Considera que los peritos informáticos están suficientemente capacitados para manejar y evaluar pruebas digitales? ¿Qué tipo de formación adicional sería útil?

2. Validación de Guías de entrevistas

MATRIZ DE VALIDACION DE INSTRUMENTOS POR ESPECIALISTAS
GUÍA DE ENTREVISTA A PERITOS INFORMÁTICOS

Nombre de Especialista Validador:
Especialidad: Mgs. Investigación
Título de la investigación: La eficacia probatoria en la apropiación fraudulenta por medios electrónicos
Objetivo del instrumento: El objetivo de la presente entrevista se focaliza en la obtención de información detallada sobre la eficacia probatoria en casos de apropiación fraudulenta por medios electrónicos, específicamente en el contexto de la conducta típica prevista en el artículo 190 del COIP

	2larida den la redacción		Coherencia interna		Introducción a la respuesta (Sesgo)		Pertinencia		Calificación de las preguntas			Observaciones (Por favor indique si debe eliminarse o modificar algún ítem)
Preguntas	Si	No	Si	No	Si	No	Si	No	Esencial	Util pero no esencial	No Importante	
1	✓		✓		✓		✓		✓			
2	✓		✓		✓		✓		✓			
3	✓		✓		✓		✓		✓			
4	✓		✓		✓		✓		✓			
5	✓		✓		✓		✓		✓			
6	✓		✓		✓		✓		✓			
7	✓		✓		✓		✓		✓			
8	✓		✓		✓		✓		✓			
9	✓		✓		✓		✓		✓			
10	✓		✓		✓		✓		✓			

Firma de Validador
Nombre: EDISON BOLAÑOS
Cédula: 0605032169

MATRIZ DE VALIDACION DE INSTRUMENTOS POR ESPECIALISTAS
GUÍA DE ENTREVISTA A FISCALES

Nombre de Especialista Validador: Edison Bonifaz

Especialidad: Mgs. Investigacion

Título de la investigación: La eficacia probatoria en la apropiación fraudulenta por medios electrónicos

Objetivo del instrumento: El objetivo de la presente entrevista se focaliza en la obtención de información detallada sobre la eficacia probatoria en casos de apropiación fraudulenta por medios electrónicos, específicamente en el contexto de la conducta típica prevista en el artículo 190 del COIP

	Claridad en la redacción		Coherencia interna		Introducción a la respuesta (Sesgo)		Pertinencia		Calificación de las preguntas			Observaciones (Por favor indique si debe eliminarse o modificar algún item)
Preguntas	Si	No	Si	No	Si	No	Si	No	Esencial	Util pero no esencial	No Importante	
1	/		/		/		/		/			
2	/		/		/		/		/			
3	/		/		/		/		/			
4	/		/		/		/		/			
5	/		/		/		/		/			
6	/		/		/		/		/			
7	/		/				/		/			

Firma de Validador

Nombre: EDISON BONIFAZ

Cédula: 0003032269