UNIVERSIDAD NACIONAL DE CHIMBORAZO
FACULTAD CIENCIAS POLÍTICAS Y ADMINISTRATIVAS
CARRERA DE DERECHO

La construcción del perfil criminológico del ciberdelincuente para la detección oportuna del phishing en Ecuador

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

Autora:
Salguero Muñoz, Sandy Solange

Tutor:
Mgs. Adrián Alejandro Alvaracin Jarrin

Riobamba, Ecuador. 2026

DECLARATORIA DE AUTORÍA

Yo, **SANDY SOLANGE SALGUERO MUÑOZ**. con cédula de ciudadanía **1803985777**, autora del trabajo de investigación titulado: **LA CONSTRUCCIÓN DEL PERFIL CRIMINOLÓGICO DEL CIBERDELINCUENTE PARA LA DETECCIÓN OPORTUNA DEL PHISHING EN ECUADOR**, 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 autora de la obra referida, será de mi entera responsabilidad; librando a la Universidad Nacional de Chimborazo de posibles obligaciones.

En Riobamba, a los 18 días del mes de febrero de 2026.

Salguero Muñoz Sandy Solange

C.I: 1803985777

DICTAMEN FAVORABLE DEL PROFESOR TUTOR

Quien suscribe, **MGS. ADRIÁN ALEJANDRO ALVARACIN JARRIN** catedrático adscrito a la Facultad de Ciencias Políticas y Administrativas, por medio del presente documento certifico haber asesorado y revisado el desarrollo del trabajo de investigación **LA CONSTRUCCIÓN DEL PERFIL CRIMINOLÓGICO DEL CIBERDELINCUENTE PARA LA DETECCIÓN OPORTUNA DEL PHISHING EN ECUADOR**, bajo la autoría de Sandy Solange Salguero Muñoz; por lo que se autoriza ejecutar los trámites legales para su sustentación.

Es todo cuanto informar en honor a la verdad; en Riobamba, a los 18 días del mes de febrero de 2026.

Mgs. Adrián Alejandro Alvaracin Jarrin

C.I: 0604091975

CERTIFICADO DE LOS MIEMBROS DEL TRIBUNAL

Quienes suscribimos, catedráticos designados Miembros del Tribunal de Grado para la evaluación del trabajo de investigación **"LA CONSTRUCCIÓN DEL PERFIL CRIMINOLÓGICO DEL CIBERDELINCUENTE PARA LA DETECCIÓN OPORTUNA DEL PHISHING EN ECUADOR"**, presentado por **Sandy Solange Salguero Muñoz**, con cédula de identidad número 1803985777, bajo la tutoría de **Mgs. Adrián Alejandro Alvaracin Jarrin**; 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 su autor; no teniendo más nada que observar.

De conformidad a la normativa aplicable firmamos, en Riobamba a los 19 días del mes de mayo de 2026.

Mgs. Fernando Peñafiel Rodríguez
PRESIDENTE DEL TRIBUNAL DE GRADO

Mgs. Romero Noboa Wendy Pilar
MIEMBRO DEL TRIBUNAL DE GRADO

Mgs. Freire Sánchez Nelson Francisco
MIEMBRO DEL TRIBUNAL DE GRADO

CERTIFICACIÓN

Que, **SANDY SOLANGE SALGUERO MUÑOZ** con CC: **1803985777**, estudiante de la Carrera **DERECHO**, Facultad de **CIENCIAS POLITICAS Y ADMINISTRATIVAS**; ha trabajado bajo mi tutoría el trabajo de investigación titulado "**LA CONSTRUCCIÓN DEL PERFIL CRIMINOLÓGICO DEL CIBERDELINCUENTE PARA LA DETECCIÓN OPORTUNA DEL PHISHING EN ECUADOR**", cumple con el 2 % similitudes y el 2 % de texto generado por la IA; de acuerdo al reporte del sistema Anti plagio **COMPILATIO**, porcentaje aceptado de acuerdo a la reglamentación institucional, por consiguiente autorizo continuar con el proceso.

Riobamba, 07 de mayo de 2026

Mgs. Adrián Alejandro Alvaracin Jarrin
TUTOR

DEDICATORIA

A Dios, por ser la esencia de mi vida y mi guía constante. A mis abuelos, por ser el origen y el refugio de mi historia. A mi madre, por el amor que impulsó mi vuelo. A mi padre, por la fuerza que siempre me da seguridad. A mi hermano, por ser mi luz y el ritmo de mis pasos. A mi enamorado, por ser mi puerto seguro y el alma en la que encuentro serenidad. A mi familia, a mis amigos, a mis maestros y mentores, por iluminar mi camino con su sabiduría. Y a mis mascotas, por ser la pureza y los compañeros más fieles de mi alma.

Sandy Solange Salguero Muñoz

AGRADECIMIENTO

A Dios, gracias por haber sido el aliento que reavivó mi fe cuando el camino se oscurecía, por haber sido la luz que nunca se apagó en mis noches de insomnio y por haberme llevado en tus brazos cuando las fuerzas me abandonaron.

A mis abuelos, pilares de mi vida, ustedes son mi primer hogar, ese abrazo sagrado donde el amor es infinito y donde mi alma siempre se siente como en casa. Todo lo que logre será para honrar su legado.

A mi madre, mi raíz, este triunfo no es solo mío; es fruto de tu sacrificio, el eco de tu coraje inquebrantable y de la fuerza que me enseñó a volar cuando mis alas aún temblaban. A mi padre, por su apoyo.

A mi hermano, mi alma gemela, este triunfo es la promesa de que siempre apoyaré tus sueños, como tú has apoyado los míos. Te dejo mi camino para que el tuyo te lleve cada vez más lejos.

A mis tíos, tías, primas y primos, gracias por ser la red de seguridad que me salvó del abismo y me recordó que nunca estoy sola.

A mi enamorado, gracias por ser mi dulce refugio, el alma donde siempre encuentro paz, gracias por ser mi calma en la tormenta, por creer en mi camino con tanta ternura y por caminar a mi lado con un corazón tan sincero.

A mis amigos, la familia con la que he elegido compartir mi alma, gracias por no haberme abandonado nunca.

A mis maestros y mentores, gracias por enseñarme que una profesión se construye sobre la pasión.

Y a mis mascotas, mis ángeles silenciosos, gracias por su inquebrantable lealtad, por velar por mí cada mañana y por reconfortar mi alma.

Sandy Solange Salguero Muñoz

ÍNDICE GENERAL

DECLARATORIA DE AUTORÍA
DICTAMEN FAVORABLE DEL PROFESOR TUTOR
CERTIFICADO DE LOS MIEMBROS DEL TRIBUNAL
CERTIFICADO ANTIPLAGIO
DEDICATORIA
AGRADECIMIENTO
ÍNDICE GENERAL
ÍNDICE DE TABLAS
ÍNDICE DE FIGURAS
ÍNDICE DE ANEXOS
RESUMEN
ABSTRACT
CAPÍTULO I 15
INTRODUCCIÓN 15
1.1 Planteamiento del problema 16
1.2 Justificación 17
1.3 Objetivos 18
1.3.1 Objetivo General 18
1.3.2 Específicos 18
CAPÍTULO II 19
2. MARCO TEÓRICO 19
2.1 Estado del arte 19
2.2 Aspectos teóricos 20
2.2.1 UNIDAD 1: Perfil criminológico del ciberdelincuente 20
2.2.2 UNIDAD 2: Phishing 29
2.2.3 UNIDAD 3: Dimensión normativa y casuística 34
CAPÍTULO III 39
3. METODOLOGIA 39
3.1 Unidad de análisis 39
3.2 Métodos 39
3.3 Enfoque de investigación 40
3.4 Tipo de investigación 41

3.5 Diseño de investigación 41
3.6 Población y muestra 41
3.7 Técnicas e Instrumentos de investigación 43
3.8 Técnicas para el tratamiento de información 43
CAPÍTULO IV. RESULTADOS Y DISCUSIÓN 45
4.1. Resultados 45
4.2 Discusión de resultados 58
CAPÍTULO V. CONCLUSIONES Y RECOMENDACIONES 61
5.1 Conclusiones 61
5.2. Recomendaciones 61
ANEXOS 67

ÍNDICE DE TABLAS

Tabla 1. Taxonomía del comportamiento delictivo en el ecosistema digital. 22
Tabla 2. Ficha técnica de especialistas que participarán en la entrevista. 42
Tabla 3. Interpretación del phishing en relación al articulado del COIP..... 55
Tabla 4. Sistematización de las pruebas digitales y físicas incautadas durante la Operación KAERB..... 57

ÍNDICE DE FIGURAS

Figura 1. Tríada criminológica: delito, autor y víctima. 21
Figura 2. Tipología de la cibervictimización. 25
Figura 3. Enfoque inductivo y deductivo en el análisis del comportamiento delictivo. 26
Figura 4. Niveles de ejecución en el modus operandi de los ciberdelincuentes..... 27
Figura 5. Escala de progresión en la sofisticación de las tácticas de phishing..... 31
Figura 6. Mecanismos de gamificación para la retención cognitiva de protocolos de ciberseguridad..... 34

ÍNDICE DE ANEXOS

Anexo 1. Matrices de validación del instrumento "Guía de entrevistas" para la aplicación a expertos. 67
Anexo 2. Guía de entrevistas y consentimiento informado..... 70
Anexo 3. Fotografías con los expertos entrevistados 72
Anexo 4. Consentimiento informado firmado por los expertos. 74

RESUMEN

Esta investigación se justifica por la urgente necesidad de detectar el phishing en Ecuador, una forma de ciberdelincuencia en rápida expansión, impulsada por la inteligencia artificial, dada la ausencia de una tipificación explícita en la legislación y la preocupante centralización operativa. El objetivo principal es establecer el perfil criminológico del ciberdelincuente como un instrumento de prevención esencial para mejorar la detección oportuna del phishing, con el fin de fortalecer la dimensión jurídico-institucional del Estado ecuatoriano. Se emplea un enfoque cualitativo, integrado por el análisis doctrinal-normativo, el criterio de expertos mediante entrevistas y el estudio de la "Operación KAERB 2024". La tesis concluye que el perfil criminal es una herramienta técnica indispensable para transformar las huellas digitales en inteligencia predictiva, lo que permite identificar patrones de comportamiento como la despersonalización de la víctima y la ingeniería social. Los resultados demuestran que, en ausencia de entidades descentralizadas, el análisis del comportamiento criminal del ciberdelincuente es la única estrategia para superar limitaciones jurídico-operativas; a virtud de lo expuesto, el Estado ecuatoriano pasa de una respuesta tardía a una detección oportuna de redes de ciberdelincuencia locales y transnacionales.

Palabras clave: perfil criminológico, ciberdelincuencia, phishing, inteligencia artificial, ciberseguridad

ABSTRACT

This study provides a comparative analysis of presumed donation and family consent systems under opt-out models in Ecuador and Argentina, through a legal examination of regulatory frameworks, legal doctrine, and hospital practices. The opt-out system presumes that every adult is an organ donor, unless they have expressly objected during their lifetime, which must be documented through a notarized record or on their identification document. In Ecuador, the Organic Law on the Donation and Transplantation of Organs, Tissues, and Cells establishes this clear legal presumption. However, in hospital practice, the family veto predominates, nullifying the potential donor's autonomy in most cases due to cultural factors, lack of regulatory awareness, and protocols that consult the family first. Generating constitutional tensions between the right to personal autonomy and the protection of family unity, resulting in persistently low transplant rates that exacerbate waiting lists and ultimately increase patient mortality. The methodology adopts a mixed approach with a comparative, descriptive, and inductive design, integrating an exhaustive documentary analysis of legislation and INDOT clinical protocols, a critical review of legal doctrine, semi-structured interviews with healthcare professionals specializing in organ transplants, and quantitative surveys of legal experts regarding regulatory contradictions. The contrast with Argentina, particularly following the Justina Law, which limits the family to an informational notification without veto power, demonstrates greater effectiveness by simplifying opposition registries and promoting cultural campaigns that reduce refusals. In Ecuador, legal loopholes, institutional weaknesses, and sociocultural barriers limit the system. We propose strengthening legal certainty by prioritizing presumed consent through easily accessible, binding electronic registries; automatic ICU protocols that override unregistered family vetoes; annual training for medical staff with practical simulations; and multisectoral national campaigns to balance individual autonomy with social solidarity.

Keywords: Organ donation, opt-out system, family consent, donor autonomy, organ transplants.

Reviewed by:
Marco Antonio Aquino
ENGLISH PROFESSOR
C.C. 1753456134

CAPÍTULO I

INTRODUCCIÓN

Uno de los ataques más comunes de ciberdelincuencia en el país es el phishing. Ciberdelito que se ve potenciado por brechas en el marco institucional centralizado y por la ausencia de unidades técnicas capaces de identificar estos delitos. Asimismo, se observa un desconocimiento en ciberseguridad entre los ciudadanos y los agentes especializados, aunque Ecuador se ha adherido a lineamientos del Convenio de Budapest, la respuesta interna de prevención al phishing e identificación de ciberdelincuentes es débil. Actualmente no se encuentra tipificado en el Código Orgánico Integral Penal, lo cual genera dificultad para conocer esta figura, ante lo expuesto, es necesario efectuar un análisis criminológico completo de los infractores, para reforzar la prevención y por consiguiente su detención.

El trabajo investigativo, se perfila bajo un estudio de tipo criminológico, que profundizará sobre el ciberdelincuente, como una categoría de análisis independiente, cuya finalidad es la determinación de patrones y conductas que se asocian a atacantes digitales. El conocimiento técnico impacta directamente a la categoría de análisis dependiente, encargada de evidenciar estrategias de prevención sólidas que ayuden a su detección oportuna, lo que mejora la capacidad de respuesta del sistema judicial, de seguridad e investigación.

Para la elaboración del presente documento, se considera como unidad de análisis a los agentes del sistema de justicia, seguridad e investigación del Ecuador, expertos en delitos cibernéticos como el phishing, además, determinan rasgos y características de los ciberdelincuentes. La tesis tiene como objetivo establecer mediante un enfoque cualitativo el perfil criminológico del ciberdelincuente como un instrumento de prevención esencial para mejorar la detección oportuna del phishing, con el fin de fortalecer la dimensión jurídico-institucional del Estado ecuatoriano.

El estudio aplicará un paradigma interpretativo con un alcance analítico, método que permitirá profundizar e inspeccionar fenómenos en reglamentos sociales asociados a los ciberdelitos. El análisis, permitirá analizar la norma vigente, así como evaluar cada uno de sus componentes en los establecimientos y patrones criminológicos que reduzcan dichos delitos.

El enfoque aplicado fue de tipo cualitativo, empleando una revisión documental y normativa, que se configura a conceptualizaciones establecidas en el Código Orgánico Integral Penal, así como en normas complementarias internacionales como el Convenio de Budapest y literatura actual. Se utilizará para la recolección de datos entrevistas a funcionarios del sistema de justicia, seguridad, investigación e información, que además podrá integrarse con el estudio del caso “Operación KAERB 2024”, caso que permitirá incluir información necesaria que refuerce mecanismos de protección del phishing y conductas delictivas del ciberdelincuente.

La presente investigación, se plantea en base a un interés jurídico social, que demuestra la necesidad de consolidar al perfil criminológico del ciberdelincuente como un instrumento técnico que perfecciona su detección en el país, fortaleciendo una respuesta jurídico-operativa del Estado y estructura bases para la formación especializada de sus funcionarios.

La relevancia de este enfoque permite abordar limitaciones institucionales al entender rasgos criminógenos del atacante frente a la sofisticación del phishing. A virtud de aquello, se expone una estrategia de prevención integral que incluye al Estado, sus funcionarios y entidades, sean públicas o privadas, nacionales e internacionales.

1.1 Planteamiento del problema

Sánchez (2021), en su estudio, identifica la importancia del perfil criminológico del ciberdelincuente para entender el funcionamiento de la ejecución criminal; por otro lado, destaca la necesidad de conocer cómo los agentes o funcionarios del sistema penal emplean actividades de prevención ante delitos cibernéticos. Los caracteres delictivos de los ciberdelincuentes no poseen pautas definidas con precisión, aunque se especifican consideraciones puntuales como patrones comunes del intelecto.

Es así que Jativa et al. (2025) aluden que, aplicar un análisis criminológico de los ciberdelincuentes, que incluya la motivación de los implicados, no es suficiente, se requiere atenuar la creciente oleada de ciberdelitos generada por avances tecnológicos, así los operadores especializados gestionan de manera eficaz el control cibernético, con apertura a un panorama de cooperación internacional positiva.

Por su parte, Pazmiño et al. (2024) señalan que el constante refinamiento sobre técnicas de programación, que utilizan algoritmos, permite catapultar al phishing como un ciberdelito ágil, indetectable por el escaso intelecto poblacional ante la veracidad o falsedad de portales web; los programas de protección de información no detienen estos ataques, que se fortalecen con ayuda de la inteligencia artificial.

Aunque el Ministerio del Interior, se suma a este criterio, que asevera el crecimiento exponencial de este delito, argumenta que la evolución técnica nace con la utilización de plataformas digitales generadas con inteligencia artificial, factor que actúa como un mecanismo de sofisticación del phishing al crear sitios cibernéticos lesivos, que a primer contacto con sus víctimas, se halla creíble, lo cual, sugiere, que la ingeniería social automatizada, hace más compleja la persecución esta trasgresión (Dirección de ciberdelitos, 2024).

Flores (2024) considera que no existe una especificación clara sobre el tratamiento del ciberdelito “phishing” en la legislación ecuatoriana. El Código Orgánico Integral Penal, en sus artículos 186 y 190, determina que los caracteres conceptuales del crimen cibernético reflejan un entendimiento complejo sobre esta figura. El Decreto Ejecutivo N° 332, que se suscribe en el año 2024, expone una adhesión al instrumento internacional “Convenio de

Budapest", cuyo objetivo es la lucha contra la ciberdelincuencia, componente elemental para la creación de la política penal y la cooperación internacional (Consejo de Europa, 2001).

La jerarquización de agentes, que aborden aspectos de ciberseguridad e investigación de delitos digitales, son una realidad a la que se enfrenta el territorio nacional, mantiene una esfera máxima que confina la cercanía con la víctima y obscurece el proceso de conocimiento preventivo básico en la sociedad, por su parte, el Ministerio de Telecomunicaciones y de la Sociedad de Información (2022), emitió un documento que habilitó estrategias de ciberseguridad, donde la problemática central fue la insuficiente formación y escases de unidades de prevención ante este tipo de delitos. Entidades gubernamentales como la Fiscalía General del Estado (2021), en su artículo "El Perfil criminológico", establece la inexactitud en la definición teórica-pragmática de delitos informáticos y cibercrímenes, lo que demuestra una nula capacitación de funcionarios.

Dado este problema, la viabilidad de la construcción del perfil criminológico del ciberdelincuente se relaciona con técnicas necesarias para la detección del phishing en Ecuador. La investigación sostiene que al implementar esta herramienta se identifican patrones de comportamiento y métodos operacionales de los atacantes, aspecto que la posesiona como un recurso científico capaz de contribuir a la formación de especialistas, su finalidad es reforzar su respuesta institucional, con esto, garantiza una gestión jurídica eficiente que permita la prevención de actividades digitales delictivas, en concordancia con la sensibilización ciudadana y la cooperación internacional.

Surge la interrogante: ¿Es posible que la construcción del perfil criminológico del ciberdelincuente se convierta en una herramienta necesaria para la prevención y detección oportuna del phishing en Ecuador, dadas las limitaciones legales, institucionales y cognitivas en el ámbito de la ciberseguridad?

1.2 Justificación

El perfil criminológico del ciberdelincuente es un componente relevante en la determinación de patrones comunes entre los antisociales que cometen un delito digital, donde se precisan motivos y rasgos que impulsan a los individuos a efectuar estos actos ilícitos; aspecto que permite detectar oportunamente los ataques de phishing y previene el avance de la ingeniería social. De la misma forma, es importante ampliar el conocimiento sobre asuntos cibernéticos conceptuales-pragmáticos a agentes judiciales, investigativos, de seguridad, entes reguladores y la sociedad, con la finalidad de anticiparse al desarrollo criminal.

En el transcurso del tiempo el phishing se ha fortalecido a gran medida, evoluciona con rapidez, por medio de técnicas novísimas como la aplicación de inteligencia artificial, por ende, en Ecuador es relevante emplear una estructuración jerárquica especializada de unidades y dependencias descentralizadas que trabajen en investigar, prevenir y detectar el ciberdelito. También se requiere cumplir con los lineamientos emanados del Convenio de Budapest para obtener una cooperación internacional eficiente, que ayude a superar las

falencias de la legislación penal que no incluye el término phishing y subsume actividades delictivas del ciberespacio en delitos tradicionales.

La metodología se limita a un enfoque cualitativo, apoyado por técnicas como entrevistas congruentes al estudio, para obtener indicadores puntuales sobre ciberdelincuentes, phishing y ciberseguridad, esta información se contrasta con el análisis bibliográfico y normativo derivado de la observación minuciosa de artículos científicos, libros, tesis, esquemas legales, manuales de apoyo, etc.

La temática en estudio es imprescindible debido a que el phishing pone en peligro, los datos personales de las personas, situación que las conlleva a una pérdida de credenciales sensibles, lo que aumenta la desconfianza hacia el uso de tecnologías, no obstante, el diseño de un perfil criminológico, se presenta como un insumo necesario, para la detección efectiva del ciberdelito, esto da lugar a que los de operadores del sistema judicial, investigativo y de seguridad adquieran el conocimiento adecuado sobre seguridad cibernética, para obtener un entorno seguro y consiente.

1.3 Objetivos

1.3.1 Objetivo General

- Establecer mediante un enfoque cualitativo el perfil criminológico del ciberdelincuente como un instrumento de prevención esencial para mejorar la detección oportuna del phishing, con el fin de fortalecer la dimensión jurídico-institucional del Estado ecuatoriano.

1.3.2 Específicos

- Analizar los fundamentos teóricos de la cibercriminología y los elementos constitutivos del perfil criminológico, para identificar los patrones conductuales y el modus operandi del ciberdelincuente especializado en phishing
- Explicar la sofisticación del phishing y las limitaciones jurídico-institucionales para su detección, con la finalidad de establecer un enfoque preventivo como estrategia esencial en el sistema de seguridad ecuatoriano.
- Interpretar la figura del phishing en el Código Orgánico Integral Penal, la ratificación del Ecuador al Convenio de Budapest y la casuística de la 'Operación KAERB 2024', para determinar la utilidad del perfil criminológico del ciberdelincuente como un instrumento técnico que fortalezca la detección oportuna de este ciberdelito.

CAPÍTULO II

2. MARCO TEÓRICO

2.1 Estado del arte

Sobre el tema, “La construcción del perfil criminológico del ciberdelincuente para la detección oportuna del phishing en Ecuador”, que conlleva una problemática actual evidenciada por la oleada cibernética de los últimos años, no se han documentado estudios; no obstante, se encontraron exploraciones, que se ajustan a lineamientos similares, las cuales han servido de sustento en el presente trabajo de investigación.

Sánchez (2021), en su estudio “Perfiles del ciberdelito: un campo de estudio inexplorado”, expuesto en la revista Central American Journals Online, refleja que la personalidad de los ciberdelincuentes es compleja, con motivaciones variadas. Sin embargo, no se presenta una metodología completamente detallada, pero se describe la aplicación del método teórico-analítico. Concluye que la prioridad en estrategias, para la adaptación de sistemas de investigación, se fundamenta en la incorporación del análisis conductual del ciberdelincuente con un enfoque en la criminología.

El artículo denominado “Análisis de la efectividad de phishing automático”, desarrollado por Pazmiño et al. (2024), publicado en la revista Elite, tiene como finalidad el análisis de la efectividad de la técnica de phishing junto con su impacto en la seguridad de datos obtenidos. Se aplica una metodología que abarca la revisión documental cuyos resultados muestran cómo los ataques se ven impulsados por la inteligencia artificial y el aprendizaje automatizado, que sobrepasan las metodologías tradicionales globales. Concluye que es necesario implementar medidas de protección eficientes a través del fortalecimiento de sistemas de seguridad y colaboración internacional.

Maldonado (2024), en su artículo científico " Análisis sobre la integración de la inteligencia artificial en la lucha contra la ciberdelincuencia en el Ecuador: desafíos y perspectivas” publicado en la Revista de Criminalidad, aplica una metodología cualitativa que se centra en entrevistas, ejercidas a funcionarios expertos en ciberseguridad pertenecientes a la Unidad Nacional de Ciberdelito de la Policía Nacional del Ecuador, cuyos hallazgos determinan que el cibercrimen actualmente, se encuentra posicionado como un exponente, resultado de la vulneración técnica e institucional que amplía su afectación por la ausencia de una legislación completa. Se concluye que el ciberdelito en el Ecuador es altamente sensible por su infraestructura; el Estado fortalece su detección al desarrollar equipos de respuesta.

La investigación titulada “Análisis de los Ataques de Ingeniería Social en Ecuador”, publicada en Ciencia Latina Revista Multidisciplinaria, es el resultado de la labor investigativa de expertos de la Dirección Nacional de Tecnologías de la Información y Comunicación de la Policía Nacional del Ecuador, Garzón et al. (2024). La investigación es de carácter documental con un enfoque cualitativo; los hallazgos determinan la existencia

de un incremento evidente en la ingeniería social; esto se produce por la falta de competencias digitales de los ciudadanos. Finalmente, la conclusión expone que la vulneración de las personas ha potenciado la ciberdelincuencia en Ecuador.

Autores como Jara y Durán (2025), en su artículo "El impacto de la ciberdelincuencia en el Ecuador y los desafíos para la justicia en esta nueva era digital" publicado en la revista MQRInvestigar, aplica el método cualitativo, que se basa en el análisis de evidencia bibliográfica expuesta en documentos, normativas e informes; los resultados refieren que el aumento de ciberdelitos, supera la capacidad de respuesta del Estado, como consecuencia de una obsolescencia legal y tecnológica, que se agrava por el desconocimiento global existente. Las investigaciones sugieren que esta una amenaza mantiene un enfoque coordinado, por ende, es necesario que el Estado priorice la educación digital, la inversión en tecnología y la urgente implementación de normativas judiciales.

Cada uno de estos estudios brinda una base metodológica, teórica y práctica que sirve como sustento en la redacción de esta tesis; los estudios reflejan un análisis profundo del comportamiento criminal digital como una necesidad ante la alta complejidad y actualización continua de ataques de phishing, que dan apertura a la necesidad de diseñar perfiles criminológicos de ciberdelincuentes, como un instrumento que identifique trasgresiones y deficiencias jurídico-operativas en el país. Finalmente, se justifica la selección de un enfoque cualitativo, por medio del uso de entrevistas dirigidas a expertos en el área del sistema investigativo, seguridad y judicial.

2.2 Aspectos teóricos

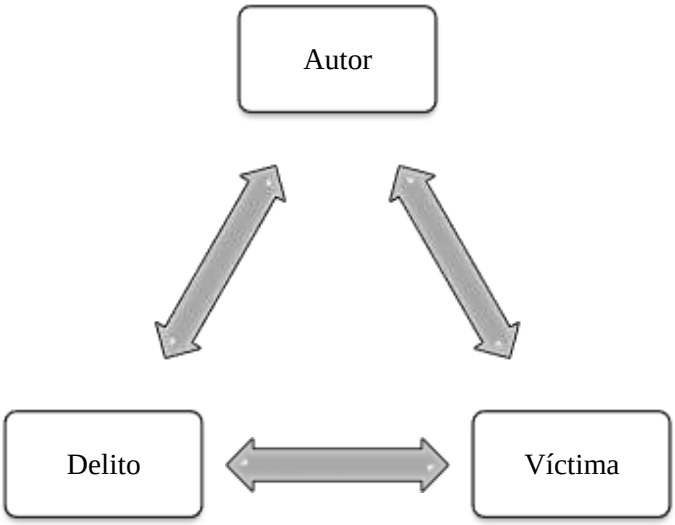
2.2.1 UNIDAD 1: Perfil criminológico del ciberdelincuente

En este apartado, se explora la evolución de la criminología en el mundo digital, y se analiza cómo la ciberdelincuencia es incluida en retos actuales. Es así como se examina la identidad de criminales digitales; se clasifican en base al nivel de conocimiento técnico o motivacional. Asimismo, se estudia el impacto de la cibervictimización en una sociedad hiperconectada. Finalmente, se detalla el uso del perfil criminal como un mecanismo que identifica a autores anónimos en relación al modus operandi y técnicas de ingeniería social, usadas para cometer ciberdelitos.

2.2.1.1 Transición de la criminología a la cibercriminología

Para Cámara (2020), la criminología es una ciencia empírica que posee un enfoque multidisciplinario e interdisciplinario y permite el análisis del fenómeno criminal, al estudiar la tríada criminológica en un sistema de control social. Es así que la cibercriminología investiga la etiología de los delitos generados en el ciberespacio, en conjunto con el análisis de las consecuencias del medio físico. Esta disciplina no solo se encuentra limitada a la indagación del comportamiento antisocial, más bien conforma un equilibrio emocional y técnico entre la interfaz hombre-máquina cuya finalidad es prevenir los delitos que emplean sistemas electrónicos.

Figura 1. *Tríada criminológica: delito, autor y víctima.*



Nota: Elaborado por Salguero, S. (2026). Representación esquemática de la tríada fundamental del derecho penal. El triángulo simboliza la estructura de equilibrio necesaria para el análisis de un caso, en el que el autor y la víctima son, respectivamente, los sujetos activo y pasivo, vinculados por la comisión del delito.

En el pasado, el control era similar al de un topo que operaba en espacios confinados, como fábricas o prisiones, donde el cuerpo permanecía inmovilizado. Hoy, vivimos en una sociedad que parece mucho más libre; el control se asemeja a una serpiente, que se moviliza por todas partes sin límites. Ya no necesitamos ser fiscalizados desde una torre de vigilancia física, ahora existe un panóptico digital. Esto significa que, gracias a la conectividad constante, el poder sabe lo que hacemos, en cualquier parte del planeta, ante aquello, la criminología estudia sistemas digitales que nos controlan a través de la comunicación y datos sensibles (Alvaracin, 2023).

Para abordar la transformación hacia la cibercriminología, es importante recalcar el término ciberdelincuencia, cuyo origen se remonta al desarrollo del sistema de alerta temprana de las fuerzas armadas estadounidenses, diseñado para interceptar bombardeos enemigos, mediante una red de computadoras militares denominada *"ARPANET".* Este paso histórico marcó el inicio de una nueva forma de acceso a la información, a medida que la sociedad exploraba el ciberespacio, los antisociales comenzaron a percibir nuevas oportunidades de delinquir. Sin embargo, es esencial mencionar que no todos los ataques contra un elemento tecnológico constituyen un ciberdelito; su clasificación depende del impacto en las Tecnologías de la Información y Comunicación *"TIC".* No obstante, se reconoce que esta evolución demuestra cómo el mundo digital amplifica los riesgos sociales debido a la ausencia de fronteras digitales (Punín, 2021).

Tabla 1. *Taxonomía del comportamiento delictivo en el ecosistema digital.*

Métodos de ataque	Caracterización técnica
Ciberataques puros	Representan comportamientos completamente nuevos del ciberespacio, como el hacking.
Ciberataques réplica	Corresponden a la adaptación de delitos tradicionales, como el phishing al entorno virtual.
Ataques basados en el contenido	Se centran en la naturaleza ilícita de la información difundida, como la pornografía infantil.

Nota: Elaborado por Salguero, S. (2026) a partir del criterio de Punín (2021). Las categorías distinguen entre el origen de un ataque y su ejecución, lo que ayuda a los criminólogos a determinar si se trata de un comportamiento delictivo específico del mundo digital o de una evolución del delito tradicional.

El avance hacia la digitalización ha abierto una nueva vía denominada tecnocriminología, que actualmente se arraiga como respuesta a los retos que plantea la Inteligencia Artificial *"IA".* Bajo la perspectiva de los miembros del Colegio Profesional de la Criminología de la Comunidad de Madrid (2025), la profesionalización criminológica actual dependerá en gran medida de la integración ética algorítmica del comportamiento del ser humano. Esta evolución le permite al experto en el área de gestión de amenazas sistémicas la interpretación de procesos de victimización automatizada, así como el uso de IA aplicada en la sociedad contemporánea. Esta transformación se integra como parte de una evaluación en el espacio digital, al marco de la fase externa del delito.

La persona considerada como ciberdelincuente sigue un recorrido denominado "iter criminis", que inicia en la fase interna, y a posteriori lo materializa por medio de las Tecnologías de Información y Comunicación. Motivo por el cual, el autor, de un delito, que opera en el ciberespacio, se caracterizará por mantener una presencia en el mundo físico a través de conexiones especializadas, lo que permite darle un seguimiento. Esto obliga a que los criminólogos adopten métodos técnicos y científicos modernos que les permitan identificar e investigar cualquier tipo o forma de ciberdelito (García, 2024).

Poco a poco, el avance de la criminología, con dirección a la cibercriminología y tecnocriminología, representa una evolución que sobrepasa el contexto criminal; esto representa un nuevo paradigma de comunicación entre el ser humano y la web, considerado como el epicentro del análisis de la conducta delictiva. La data vigilancia reemplaza una detección física, y se aplica por medio de algoritmos, los cuales son estudiados como mecanismos de poder y control social. Dicha transformación permite comprender cómo la ausencia de fronteras físicas ha potenciado el aparecimiento de ciberataques.

No obstante, en la actualidad, el auge sobre el uso de la inteligencia artificial exige a los criminólogos la toma de una reorientación en acciones de prevención compleja donde se integre la psicotecnología, para rastrear todo el proceso delictivo por medio del uso de entornos automáticos. Así se unifica el rastro que se deja en el ciberespacio, se detecta la

identidad real del autor en el mundo físico, cuya finalidad es conformar un sistema de control avanzado, necesario en la investigación y prevención de la ciberdelincuencia.

2.2.1.2 Ciberdelincuentes

El ciberdelincuente se define como un individuo que posee un alto conocimiento técnico y una considerable capacidad de adaptación en entornos digitales, cuya finalidad es llevar a cabo actos delictivos considerados no lícidos, por medio del aprovechamiento de su anonimato y ausencia de fronteras físicas en el ciberespacio. Este tipo de delincuente indaga vulneraciones técnicas que demuestran la agilidad en migrar sus tácticas a entornos nuevos utilizados por la sociedad como plataformas digitales y redes sociales. Es decir, el perfil delictivo del ciberdelincuente es dinámico y transnacional (Gutiérrez et al., 2025).

Según el criterio de Castillo (2021), la motivación e impacto de los ataques se alinean con criterios técnicos y criminológicos del tipo de delincuente, expuestos a continuación:

- ***Newbie:*** Se caracteriza por ser novato en actividades de piratería informática, no posee altos conocimientos ni experiencia, aplica su conocimiento adquirido de manera autónoma
- ***Lamer:*** Corresponde a un individuo que aparenta ser un experto en el área, solo porque usa herramientas prediseñadas por otras personas.
- ***Script Kiddie:*** Es una persona que tiene una intención maliciosa, pero que no posee un conocimiento profundo y especializado, motivo por el cual se dedica a hacer modificaciones no autorizadas en sitios web.
- ***Phreake:*** Es considerado un pirata en información, el cual interactúa por medio de la evasión de mecanismos de facturación en operaciones telefónicas.
- ***Sneaker:*** Posee las habilidades necesarias, que le permiten infiltrarse dentro de un sistema no autorizado, motivado por un contexto económico, es decir, suele ser contratada por una tercera persona con el fin de obtener secretos industriales o comerciales.
- ***Cracker:*** Se vincula a la piratería informática y ciberdelincuencia, emplea su conocimiento con el objetivo de ejercer prácticas antiéticas o ilícitas.
- ***Hacker***: Individuo ya especializado en superar obstáculos tecnológicos que mejoran los sistemas; estos se clasifican en dos grupos:
    - ***Hacker* de sombrero blanco - *white hat:*** Mejora la ciberseguridad al detectar vulnerabilidades.
    - ***Hacker* de sombrero negro - *black hat*:** Actúan por incentivo económico o venganza. Dentro de la categoría se incluye:
        - ***Phisher:*** Engloba a un novato o erudito en tecnología, donde no siempre necesita un alto nivel de especialización para burlar sistemas digitales.
- **Hacktivistas:** Comunidad que lanza un ataque con el fin de expandir una idea o mensaje dentro de cualquier ámbito a fin de defender su libertad en el internet.

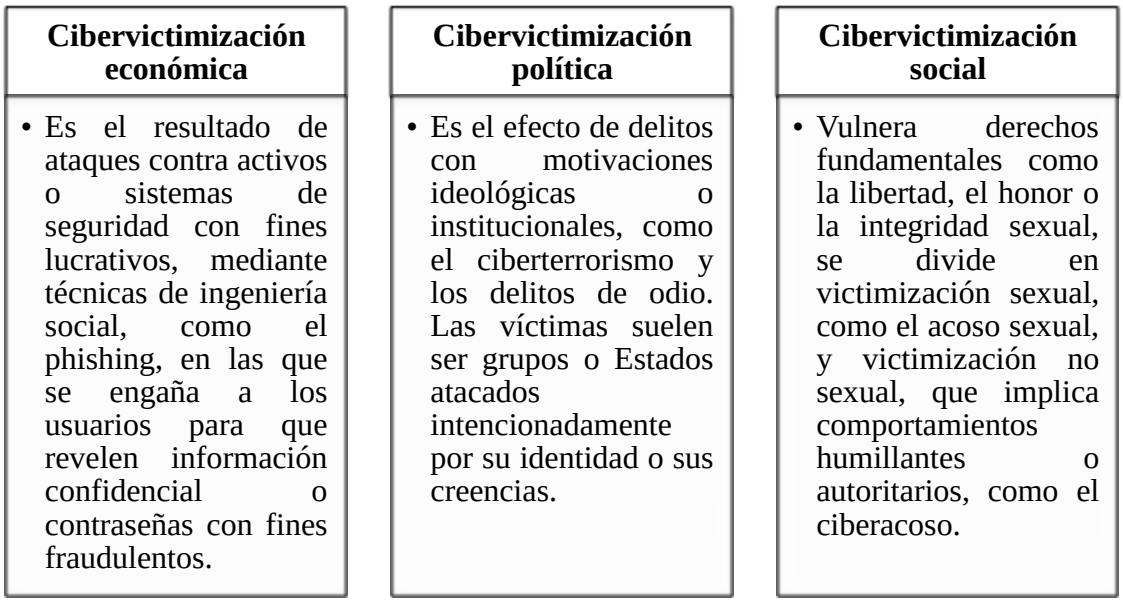
- **Cybercrime as a service – CaaS**: Le faculta a la persona la compra de kits criminales, que serán usados en ataques, sin necesidad de poseer conocimiento técnico

Estudiar cada una de las modalidades de los ciberdelincuentes, mediante sus rasgos internos y mecanismos de regulación social, en base al ámbito de la psicología criminal, se incluye una marcada falta de empatía, con la existencia de un sentido frágil de responsabilidad, así como una elevada capacidad de ingeniería social. Esto se sustenta en la manipulación de relaciones interpersonales que le permite obtener beneficios ilícitos, al utilizar la deslocalización digital, con el objetivo de mantener un riesgo mínimo en operaciones tecnológicas que facilita la vulneración de derechos de protección de datos, en escala mundial (Díaz et al., 2023).

Los ciberdelincuentes mantienen una facilidad de adaptación, que les permite operar de forma anónima dentro del espacio digital. El nivel de amenaza varía por su experiencia, va desde principiantes que usan herramientas de terceros hasta personas con un nivel de conocimiento más profundo, que comprometen la seguridad de las grandes empresas con fines lucrativos o por venganza. Un criterio relevante es la manipulación psicológica, del atacante a la víctima, para obtener sus credenciales sensibles y datos. Los individuos muestran una carencia de consideración por el daño que causan, al no mantener un contacto directo con las víctimas, motivo por el cual perciben un menor riesgo de ser detectados. Se identifica que la tecnología es un medio que le permite al ciberdelincuente manejar un peligro que se sustenta en su capacidad de explorar la confianza humana y la vulnerabilidad del sistema con la finalidad de beneficiarse ilícitamente.

Es necesario mencionar a las personas afectadas en el plano digital. El concepto de cibervictimización se ha transformado de un incidente aislado a un sujeto de vulnerabilidad permanente, como consecuencia de una conexión y exposición continua en la red. La persona considerada víctima posee un papel importante en su protección, si interactúa desmedidamente en la web y carece de herramientas de defensa, potencia el riesgo de ser un blanco fácil para estos criminales digitales (Montiel, 2020).

Figura 2. *Tipología de la cibervictimización.*



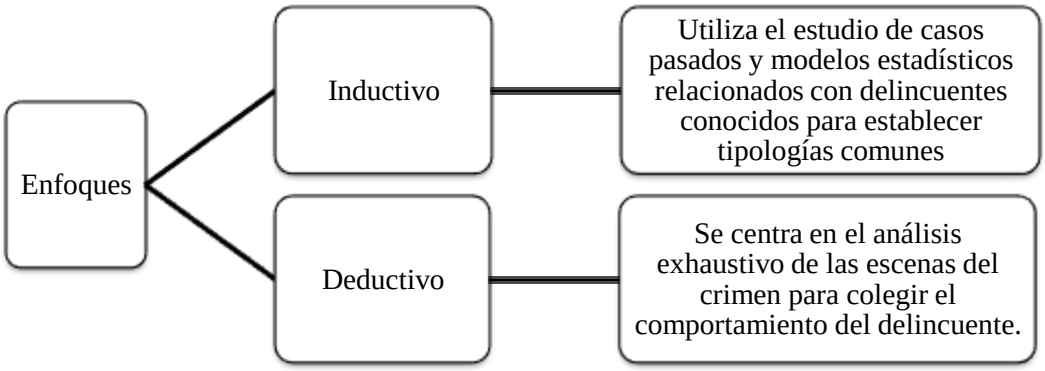
Nota: Elaborado por Salguero, S. (2026) a partir del criterio de Montiel (2020). El diagrama presenta una taxonomía de la cibervictimización dividida en tres categorías independientes. Cada categoría se distingue por la motivación del agresor y por el daño causado, ya sea pecuniario, institucional o relacionado con los derechos fundamentales.

En base al criterio de López (2020), la ciberdelincuencia posee un nivel de afectación mayor que la delincuencia tradicional, esto debido a que un solo ataque impacta de forma notoria a varios usuarios. Causa daño al patrimonio de las personas por medio de fraudes que son considerados insignificantes, pero que conforman una victimización económica de gran escala. Este deterioro no se limita al ámbito económico solamente, también se ven afectados bienes jurídicos como la privacidad de la persona, su honor, propiedades intelectuales, etc. Según la naturaleza de los ataques cibernéticos, las cibervíctimas sufren vulneraciones sin identificarlas; esto indica que la tecnología ha trascendido la seguridad personal en un estado de exposición constante, que obliga a los usuarios a dejar su pasividad, la carencia de acciones de prevención y la existencia de una confianza en exceso, dentro de plataformas digitales.

2.2.1.3 Perfilación criminal

Márquez (2022) en su estudio indica que el perfil criminal es una técnica multidisciplinaria, usada en investigaciones penales, con el objetivo de estudiar la evidencia conductual. Esta metodología permite deducir de forma sistemática los rasgos bibliográficos, motivaciones y estilos de vida de delincuentes desconocidos, al establecer procesos analíticos en base a la dicotomía metodológica que incluye al método inductivo y deductivo.

Figura 3. *Enfoque inductivo y deductivo en el análisis del comportamiento delictivo.*



Nota. Elaborado por Salguero, S. (2026) con relación a la perceptiva de Márquez (2022). Comparación de los procesos lógicos aplicados a la criminología. El enfoque inductivo tiene como objetivo establecer caracteres frecuentes de los criminales, mientras que el enfoque deductivo establece la actuación del antisocial a partir de la observación meticulosa del lugar de los hechos.

Dentro del área de la cibernética, el perfilamiento criminal se entiende como un instrumento criminológico, necesario para la recopilación y el análisis de las características conductuales, las cuales se ven influenciadas por la evolución tecnológica, la hiperconectividad y el anonimato del ciberespacio. Para esto es relevante diferenciar si los sitios tecnológicos son el objetivo de la acción o el medio del cometimiento de otros delitos, con el fin de identificar patrones criminógenos (Sánchez, 2021). Se incluye la postura de la Fiscalía General del Estado (2021), en donde la elaboración de perfiles criminales es considerada una herramienta que permite reducir actos de delincuencia digital, desafiantes al derecho penal tradicional por su naturaleza transnacional y el modo incógnito que otorga el cifrado de identidad.

Actualmente, se determina que una persona, aunque no sea parte de un grupo social marginado, aprovecha las oportunidades delictivas que le brinda el internet, desde un enfoque sociodemográfico, el delincuente digital, presenta características distintivas, que identifican a hombres jóvenes o nativos digitales como los principales sospechosos, debido a que disponen de un tiempo amplio en la indagación de la web (López, 2022).

El perfil criminológico de los ciberdelincuentes se asocia a tres factores: la superioridad técnica, el anonimato estratégico y la manipulación. Dominar las funciones informáticas confiere una ventaja operativa sobre el sistema de seguridad, modifica la percepción de riesgo, como respuesta al uso de herramientas de ocultamiento, que conduce a la protección ante la ley. Su estructura es dinámica y deshumanizada; el entorno digital incita un efecto de despersonalización, donde la cibervíctima se comprime a un dato o a un objeto abstracto, por ello, el ciberdelincuente actúa con un impacto multidimensional que incluye estímulos de tipo económico, poder, venganza, hostigamiento y pensamiento intransigente (Jativa et al., 2025).

El estudio del comportamiento del ciberdelincuente, permite al funcionario especializado, el identificarlo, pese a que, en el ciberataque, su identidad, se encuentra

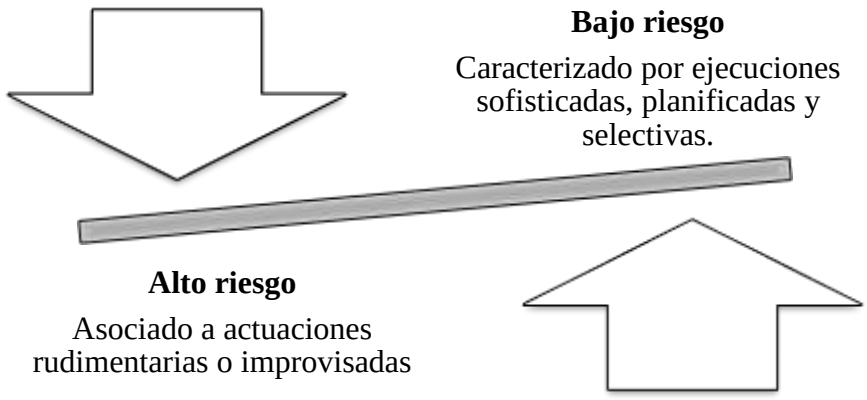
oculta, así podrá operar sin un límite geográfico, que se enfoque en el estudio de este dentro del ciberespacio: dicha técnica, analizará delitos que se presentan en entornos digitales. Eso indica que un delincuente cibernético, no mantiene una sapiencia prolongada: muchos de estos, emplean técnicas sencillas como el uso de un engaño, mientas que otras personas podrían obtener una competencia más técnica y compleja. Actúan de forma remota, por medio de acciones que les permiten considerar al afectado como un objeto.

El perfil criminológico del ciberdelincuente se transcribe a operaciones generadas en línea. La utilización de tecnología reduce el temor del ciberdelincuente, al ser detenido, sin embargo, al aplicar un análisis criminógeno, se rompe la barrera invisible, donde la actividad digital se encuentra vinculada a la vida real, lo que facilita su localización y permite sancionar su accionar.

2.2.1.4 Modus operandi del ciberdelincuente especializado en phishing

El modus operandi hace referencia a todo el proceso que conlleva un delito, cuyo objetivo principal es lograr un resultado deseado, ocultar la identidad del autor y facilitar su huida. Es un método que se trasforma en el tiempo, deteriora o evoluciona la capacidad física y mental del agresor, con un nivel de bajo o alto riesgo (Arciniegas et al., 2022). Fundamento que se ajusta al criterio de la Organización Internacional de Policía Criminal "INTERPOL" (s.f.), institución que establece la ejecución del phishing por medio de correos electrónicos, llamadas telefónicas o mensajes de texto, donde el ciberdelincuente se hace pasar por una entidad legítima, ya sea un banco o plataforma de comercio electrónico, para obtener información personal o financiera del afectado, esto demuestra la adaptabilidad de trasgresor y fallas de comunicación.

Figura 4. *Niveles de ejecución en el modus operandi de los ciberdelincuentes*



Nota: Elaborado por Salguero, S. (2026) en contraste con el argumento de Arciniegas et al. (2022). Esta figura ilustra cómo la sofisticación técnica reduce los riesgos para el delincuente, mientras que la improvisación aumenta la vulnerabilidad de su identidad, lo que influye en el éxito de ataque y ocultación.

El phishing describe el modus operandi, como una combinación entre el uso de herramientas tecnológicas y técnicas sociales, las cuales, son manifestadas por medio de:

- ***Phishing* engañoso:** Incluye el método clásico de suplantación de identidad por medio de correos electrónicos de gran escala, donde se utilizan enlaces fraudulentos que guían a la víctima a sitios web falsos.
- ***Software* malicioso:** Requiere una invasión en el sistema por medio del uso de un software malicioso, se encuentra clasificado en:
    - ***Key-loggers y Screen-loggers*:** Mecanismo que registra pulsaciones del teclado y se capturan pantallas.
    - **Secuestradores de sesión*:*** Invasión que causa una desviación de la sesión activa del usuario luego de la autenticación
    - **Troyanos *web*:** Incluyen mecanismos que modifican la configuración del sistema para redirigir el tráfico de datos hacia el atacante.
    - **Ataques de reconfiguración de sistema*:*** Son ataques que se caracterizan por obtener una modificación en la configuración de ordenadores de las víctimas, desvían la información.
    - **Robo de datos:** En este aspecto, se puede acceder a ellos por medio de un código malicioso, el cual puede desarrollarse en el ordenador, cuya meta es la recopilación de información personal, que será compartida en con el ciberdelincuente.
- **DNS o "*Pharming*":** Es un método de mayor impacto, que puede cambiar el nombre del dominio, redireccionando a usuarios a entornos web no verídicos, que se observan en el navegador, así se evitará que el ciberdelincuente adquiera una directa con la persona afectada.
- **Introducción de contenidos:** Compromete los servidores legítimos por medio de inyectables de códigos maliciosos, que extraen datos de la entidad suplantada.
- **Técnica del intermediario:** Mecanismo en el cual, la persona agresora, se coloca de manera estratégica entre el usuario y el sitio web, para modificar la información en tiempo real, promueve el robo de cuentas o secuestro de sesiones.
- **Motor de búsqueda*:*** Crea sitios web que ofrecen productos o servicios falsos con un precio bajo, en este sentido, los motores de búsqueda se unen a otros sitios, los usuarios acceden a ellos y proporcionan información personal al intentar ejercer una compra.

El modus operandi incluye el antes, durante y después de un evento delictivo, es decir, abarca desde la planificación hasta el encubrimiento del ataque. La habilidad del ciberdelincuente determina si la ejecución fue de manera improvisada o con preparación y sofisticación. En el phishing, el infractor suplanta la identidad de terceras personas o instituciones por medio de redes sociales, llamadas telefónicas o mensajes de texto. Es un método que armoniza la manipulación psicológica, así como herramientas digitales. Se evidencian ataques masivos que usan enlaces falsos o ataques aplicados como consecuencia de la instalación de programas que registran pulsaciones o secuestro de sesiones. Existen técnicas avanzadas que modifican las direcciones de IP, con el fin de redirigir a víctimas a sitios web engañosos sin su consentimiento.

2.2.2 UNIDAD 2: Phishing

En la unidad 2, se analiza el phishing como un delito cibernético, cuya evolución ha incluido mecanismos manuales de la ingeniería social, hasta sistemas automatizados. Permite examinar sus modalidades y técnicas de funcionamiento, así como las limitaciones jurídicas e institucionales en el país, que dificultan una detección eficaz. Asimismo, contribuye a la prevención por medio de estrategias basadas en una cultura digital y cooperación internacional, propone un cambio de paradigmas que impulsa el empoderamiento de usuarios y la protección de sus derechos en contraposición a los métodos punitivos tradicionales.

2.2.2.1 El phishing como ciberdelito

Alvaracin (2023) indica que el poder en la época contemporánea no requiere aplicar fuerza física ni actos vinculados al castigo; ahora se usan mecanismos como la seducción, que actúa en la psiquis e incita a entregar información personal de manera voluntaria. Por ende, los dispositivos inteligentes son considerados un confesionario moderno frecuentemente usado, que contiene información sobre gustos, emociones, hábitos, materia prima de grupos delictivos que controlan la tecnología a través de engaños silenciosos.

La divulgación de datos personales construye un espacio útil para efectuar ataques de phishing; es un fenómeno delictivo complejo que aplica técnicas sociales y plataformas digitales, aprovecha la vulnerabilidad sistémica, donde la víctima revela información personal, motivada por fines lucrativos. Este ciberdelito se consuma por medio de la suplantación no autorizada, usa dispositivos visuales que obligan al destinatario a realizar acciones específicas (Benavides et al., 2020).

La terminología phishing tiene su origen en el año de 1996, descrita en el foro de "*hackers alt.2600"*, cuya referencia se asocia a personas involucradas en el ataque de cuentas *AOL* al suplantar empleados. Posteriormente, evolucionó a servicios de correo electrónico con mensajería fraudulenta. Al transcurrir el tiempo, se diversificaron tácticas de uso de mensajes instantáneos; en la pandemia de COVID-19, se evidenció un despunte de ataques y actualmente se centra en la falsificación de bancos en línea, servicios de logística y organismos gubernamentales (Cano, 2021).

Por esto, es considerado un delito refinado, cuyo éxito dependerá del malware y del aprovechamiento social, ejercido como consecuencia de sesgos cognitivos y la sobreconfianza de la víctima. En la estructura operativa, las acciones ejercidas le permiten al agresor mantener el anonimato; en este caso, la persona violentada no tiene conocimiento sobre quién cometió el acto. El engaño no tiene por objeto inducir a la persona a realizar una transacción financiera, busca obtener las credenciales necesarias (Torres et al., 2021).

Según la percepción de Díaz (2020), este ciberdelito se clasifica en cuatro tipos según el método de contacto, la técnica empleada y el perfil de la víctima.

- **Phishing tradicional:** Usa el correo electrónico para suplantar la identidad de empresas o establecimientos y robar credenciales.
- ***Smishing:*** Mecanismo en el cual, se usa mensajes para robar información
- ***Vishing:*** Llamadas telefónicas o mensajes de voz.
- ***Malware-based* phishing*:*** El agresor envía archivos o URL maliciosos que se adjuntan a correos electrónicos para que la víctima descargue un software malicioso.
- **Phishing mediante mensajería instantánea**: Utiliza direcciones de internet de carácter malicioso por medio de salas de chat o mensajería instantánea.
- ***Banners* de anuncios falsos:** Emplea sitios web que ofertan productos con descuentos elevados; las víctimas son trasladadas a páginas diseñadas para insertar información y así robar sus datos.
- ***Spear* phishing:** Agresiones generadas en contra de personas u organizaciones específicas, donde el infractor tiene un conocimiento extenso del objeto.
- **CEO: E**l ciberdelincuente engaña a empleados con acceso a finanzas para solicitar movimientos bancarios, a nombre de ejecutivos altos.

El phishing es un tipo de ciberdelincuencia, que se sustenta en la ingeniería social, cuyo fin es engañar a las personas afectadas para que estas les brinden información personal. El éxito de sus operativos depende de su actividad delictiva, así como de la manipulación del usuario por medio de instrumentos informáticos, elementos clave en esquemas delictivos. Los métodos utilizados son los mensajes de texto, las llamadas telefónicas o correos que se caracterizan por ser personalizados, así como anuncios ficticios en motores de búsqueda o suplantación de identidad de altos ejecutivos. En sí, el phishing es una amenaza adaptable que aprovecha un canal de comunicación digital para comprometer la seguridad informática del afectado con el objetivo de obtener beneficios.

2.2.2.1.1 Sofisticación del phishing

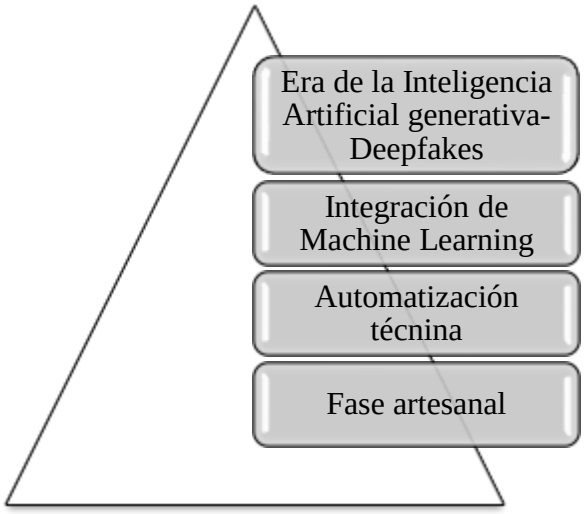
El uso actual de la tecnología crea un espacio de sofisticación para ciberataques, los cuales, cada vez, son más prolijos, evolucionan con el fin de adaptarse a nuevas condiciones y optimizar su efectividad. El refinamiento de los ciberdelitos surge por el aparecimiento de IA, que permite desarrollar técnicas más avanzadas como la utilización de *deepfakes*, que facilitan al agresor imitar la voz o la forma de escritura de la víctima. El progreso de las técnicas y procedimientos indica que la ciberdelincuencia ya no se encuentra limitada a afectaciones locales; actualmente se ha transformado en operaciones altamente especializadas (Aguilar y Balseca, 2024).

Por esto, la Dirección de Ciberdelitos (2024) aplica un análisis sobre la ciberdelincuencia y su transformación, menciona que la IA es una fuerza motriz en la sofisticación del crimen. Sus diferentes plataformas crean espacios en la creación de mensajes y correos electrónicos que son convincentes, eliminan errores lingüísticos y adaptan el tono de la comunicación. Es decir, los agresores aprovechan la capacidad de estas herramientas tecnológicas para procesar información y datos a gran escala cuyo fin es estafar a la víctima sin un esfuerzo manual. Permite generar contenidos sintéticos, como archivos

de audio y vídeo falsos, que aumentan la credibilidad al suplantar con precisión a las personas.

El phishing, poco a poco, ha trasmutado a un sistema automatizado y extremadamente preciso, donde se aplican *scripts*, algoritmos y *software* especializado, como *kits* de phishing, para llevar a cabo ataques masivos. La evolución se induce con mayor fuerza por medio de la Inteligencia Artificial y el Aprendizaje automático (*Machine Learning*), que causa que el agresor personalice su mensaje falso incluso a escalas mayores. En el país, este problema se ha evidenciado con más fuerza en provincias de Guayas y Pichincha, donde la automatización facilita el robo de credenciales y datos financieros, aprovecha el error humano, responsable del 95 % de las vulnerabilidades en materia de ciberseguridad (Pazmiño et al., 2024).

Figura 5. *Escala de progresión en la sofisticación de las tácticas de phishing.*



Nota: Elaborado por Salguero, S. (2026). La escala ilustra la transición del phishing desde métodos manuales a sistemas automatizados, gracias al aprendizaje automático y IA, lo que permite ataques masivos personalizados y la creación de contenidos sintéticos convincentes.

La evolución del phishing en la época actual indica la importancia de renovar sanciones y mecanismos que las frenen, donde además se modifiquen los alcances de la IA, en realización de este tipo de delitos, puesto que, al no basarse en mecanismos lentos y manuales, transgreden a una mayor proporción de habitantes. Por otro lado, las deepfakes, neutralizan las defensas psicológicas de la víctima al presenciar un escenario digital que no distingue la realidad, por ende, la ciberdelincuencia, ha dejado de ser una actividad localizada, para entenderse como un sector tecnológico especializado que aprovecha el error humano como principal vía de ataque

2.2.2.1.2 Limitaciones jurídico-institucionales en la detección del phishing

El estudio sobre la ciberdelincuencia en el país indica el confrontamiento del phishing con las limitaciones jurídico-institucionales, evidenciadas en la falta de una

legislación actual y específica que defina los comportamientos delictivos del ciberespacio. A nivel institucional, la eficiencia de los procesos investigativos se ve afectada por problemas de coordinación entre los organismos clave como la Fiscalía General del Estado, el Ministerio del Interior, ARCOTEL, así como otras instituciones gubernamentales y privadas. Además de la ausencia de una estructura de colaboración, comunicación y competencia, las medidas de respuesta se limitan por la ausencia de recursos humanos y tecnológicos destinados a la formación especializada (Solano et al., 2023).

Juca y Medina (2023) recalcan un aumento de casos de phishing en Ecuador, que supera de manera desmedida la capacidad de respuesta estatal, mientras que la falta de recursos tecnológicos, el desconocimiento del personal y el anonimato de los ciberatacantes conforman una limitante para la administración de justicia. Por su lado, el Ministerio de Telecomunicaciones y Sociedad de Información (2022) destaca dimensiones operativas que recaen en la necesidad de capacitar a expertos para robustecer las unidades especializadas.

León et al. (2024) consideran que, aunque el país se adhirió al Convenio de Budapest, el Código Orgánico Integral Penal presenta deficiencias que vulneran el principio de legalidad. Potenciadas por la rápida evolución de las transgresiones cibernéticas, que supera la capacidad de la legislación para anticiparse, lo que crea vacíos que permiten la impunidad al intentar clasificar comportamientos digitales como delitos tradicionales. Flores et al. (2024) determinan una carencia en la definición jurídica, precisa del phishing, problema que impide categorizar de manera exacta el ciberdelito, obliga a interpretar la actividad delictual en los artículos 186 y 190 del COIP, sin embargo, no refleja la naturaleza técnica del delito mencionado.

La detección de este ciberdelito mantiene un desfase entre la sofisticación del ciberdelito y la capacidad de respuesta estatal, causa una fragmentación operativa que se acompaña de la carencia de protocolos de coordinación entre las entidades especializadas. El sistema institucional actualmente se encuentra sobrecargado, debido a que los ataques de phishing superan los recursos tecnológicos y la formación técnica de los recursos humanos. La normativa actual, posee retos legales que obligan a los agentes del sistema penal a calificar comportamientos digitales como delitos tradicionales que son relativos al phishing, esto impide el ejercicio de sanciones eficientes y fomenta impunidad

2.2.2.1.3 Prevención del phishing como enfoque estratégico

Según el criterio de Zaffaroni (2011), con base en la prevención, indica que esta inicia desde el sistema de justicia penal, donde intervienen acciones posteriores a los conflictos. Menciona que el conocimiento criminológico y las estrategias primarias permiten limitar el poder punitivo. Es decir, necesita abordar condiciones sociales y niveles de vulnerabilidad entre organismos estatales y la reinserción social. No se previenen situaciones desconocidas, por lo mismo, la reducción de la delincuencia depende de la capacidad de la sociedad para neutralizar riesgos por medio del conocimiento genuino.

Para la conformación de estrategias de prevención, es relevante considerar el criterio de Castro (2009), quien estudia la criminología de los derechos humanos. Determina que

existe un control de justicia penal que evita el castigo, promueve la protección del desarrollo progresivo de la paz mental y espiritual de la sociedad. En la percepción de prevención, permite analizar y limitar el control social, donde el sistema penal no se convierta en un instrumento que trasgreda la dignidad y la libertad de los ciudadanos.

Alvaracín (2023) propone la criminología de la liberación, que critica la tendencia a resolverlo todo mediante sanciones dictadas por los poderosos, lo que afecta a la población con mayor grado de vulnerabilidad y deja impunes a grupos influyentes. Una verdadera estrategia de prevención no crea más leyes o prisiones, reclama autonomía, al comprender que el control de los algoritmos nos esclaviza. Es así que la idea principal de la prevención sirve para transformar una realidad injusta en una de protección de derechos.

La toma de medidas de prevención estratégica necesita de modelos proactivos, que otorguen relevancia a la implementación de la autenticación y empleo del "*https*" cifrado como barreras esenciales contra el acceso no autorizado. Asimismo, se considera útil el refuerzo de información, por medio de la ciberseguridad que mitiga la vulnerabilidad relacionada con la ingeniería social; además, el monitoreo continuo refleja un análisis de comportamiento y aplicación de IA capaz de identificar patrones delictivos en tiempo real. Su eficacia depende de la colaboración de entidades y ciudadanos (Morales, 2025).

El sistema judicial del Ecuador necesita un cambio de percepción que transforme el enfoque punitivo en una estrategia integral de seguridad. Aunque en el COIP, se establecen sanciones, se estima un desconocimiento poblacional de 8,2 %; agravado por el número significativo de delitos no denunciados, como respuesta a la falta de desconfianza en autoridades vigentes y desconocimiento de protocolos de denuncia. En base a esto, se emplea un enfoque estratégico, que incluye temas de seguridad cibernética y parámetros de cooperación internacional como el "Convenio de Budapest", de modo que las regulaciones sirvan como mecanismo de gestión de riesgos (Campos et al., 2025).

Al comprender que los delincuentes cibernéticos explotan factores psicológicos y cognitivos de sus víctimas, los métodos preventivos priorizan la formación continua de usuarios. Los individuos con facilidad olvidan las alertas de seguridad, motivo por el cual el asesoramiento no es estático; aplica mecanismos como la gamificación para mejorar la memorización. También, se requieren políticas organizativas que identifiquen a grupos con mayor vulnerabilidad y concientizarlos (Camacho et al., 2024).

Figura 6. *Mecanismos de gamificación para la retención cognitiva de protocolos de ciberseguridad.*

Nota: Elaborado por Salguero, S. (2026) en relación a lo expuesto por Camacho et al. (2024). Ilustra el proceso de aprendizaje interactivo a través de programas y juegos, destaca su capacidad para superar la naturaleza estática de la formación tradicional. Esta metodología promueve el aprendizaje continuo, mejora significativamente la memorización del usuario y su capacidad de respuesta ante posibles amenazas.

La prevención del phishing prioriza los derechos del ser humano por encima de la represión, evidencia que la eficacia no solo se encuentra en sanciones severas, sino que abarca una reducción de la vulneración social mediante el conocimiento propio, que limita la toma de acciones restrictivas. Una herramienta digital, puede explicarse como una evolución de un paradigma jurídico en el país, cuya meta es luchar en contra del desconocimiento digital, la desconfianza en establecimientos gubernamentales y otras instituciones. Una metodología preventiva podrá dirigir una estrategia de cada establecimiento, alineada a una formación constante en el usuario, así se obtendrá una adecuada cibereducación: asimismo, mostrará el compromiso colectivo por una vida más libre en entornos digitales.

2.2.3 UNIDAD 3: Dimensión normativa y casuística

En este apartado, se considerarán lineamientos jurídicos fácticos del phishing, en donde se analizarán diferentes limitaciones del Código Orgánico Integral Penal, los cuales tienen una descripción exacta que, les obliga a tipificar al delito en categorías clásicas. El apego al Convenio de Budapest por parte de Ecuador establece la necesidad de equilibrar la legislación en el país, con normas interinstitucionales. Finalmente, la operación KAERB 2024, profundizará como el desmantelamiento de una red atracadora refleja la necesidad de que en el país se ejerza una gran operación entre instituciones que permitan frenar las tácticas automáticas del phishing.

2.2.3.1 Preceptos legales implícitos en el Código Orgánico Integral Penal

Con base en los delitos informáticos, tipificados en el marco jurídico ecuatoriano, la estructura legislativa se muestra frágil, en el Código Orgánico Integral Penal, no se encuentran secciones que se vinculen a la estipulación exacta de ciberdelitos, esto causa una brecha jurídica. La legislación actual se encuentra limitada por sanciones descritas en el artículo 232 del COIP que hace referencia a ataques en la integridad de sistemas informáticos; no obstante, la respuesta jurídica es insuficiente (Ponce, 2024).

- **Art. 232 "Ataque a la integridad de sistemas informáticos"** (Asamblea Nacional, 2014): Abarca la mayoría de los delitos que se ejercen de forma informática, caracterizados por penalizar daños físicos o lógicos que nacen como resultado de alteraciones en datos y acciones que producen comportamientos indeseados en el funcionamiento normal de redes y dispositivos electrónicos. Se persiguen todas las fases de la cadena delictiva desde su inicio, programación, distribución hasta la ejecución final de un comportamiento delictivo digital que compromete a los sistemas informáticos.

En base al criterio de Conforme y Vela (2023), el phishing no se encuentra tipificado dentro del COIP, aunque posee una aproximación normativa, configurada dentro de los delitos de falsificación informática (art. 234.1) y estafa (art. 186). Flores et al. (2024) respaldan el criterio que argumenta que el phishing no posee una manifiesta estipulación, motivo por el cual encaja en el artículo 190 (Apropiación fraudulenta por medios electrónicos). Finalmente, Suarez (2024) adiciona la figura jurídica del acceso no consentido a un sistema informático, telemático o de telecomunicaciones (art. 234).

Ante lo expuesto, es importante, considerar que el phishing, se interpreta mediante (Asamblea Nacional, 2014):

- **Art. 186 "Estafa":** Incluye hechos fácticos como la creación de sitios web, de carácter fraudulento, para engañar a la víctima. El phishing no tiene como objetivo la infiltración del sistema informático, sino que se corrompe el consentimiento del usuario, para que este divulgue su credencial de acceso. Esto se considerará un prejuicio financiero, donde se logra tramitar transferencias no autorizadas. Esta acción se agrava en el apartado 1, debido a que el ataque de phishing se ejecuta por medio del uso de datos obtenidos sin consentimiento.
- **Art. 190 "Apropiación fraudulenta por medios electrónicos":** Parte técnica del phishing, sanciona el uso del sistema informático y redes de telecomunicación que faciliten transferencias no autorizadas. Esto causa que se origine una alteración dentro de la funcionalidad de sistemas informáticos, al vulnerar la seguridad informática.
- **Art. 230 "Interceptación ilegal de datos":** En este artículo, se establecen lineamientos técnicos de este ciberdelito; se aplica el manejo de flujos de información. Sanciona la interceptación de contenidos digitales dentro de cualquiera de las fases en ejecución. Logra penalizar el diseño de estafas, que se encuentran en páginas web, enlaces o ventanas emergentes, y elementos que inducen a una persona a acceder a sitios web no verídicos. En el numeral 3, 4 y 5, se establece la responsabilidad penal de las personas que distribuyen insumos o herramientas que facultan clonar información,
- **Art. 234 "Acceso no consentido a un sistema informático, telemático o de telecomunicaciones":** El phishing es un mecanismo de carácter engañoso, donde el atacante obtiene la información que no es de libre acceso. El ciberdelincuente

usa medios de navegación falsa para redirigir datos y conseguir credenciales de acceso para acceder al sistema informático.

- **Art. 234.1 "Falsificación informática":** El phishing es considerado un acto en donde se falsifica la información; el autor genera datos o documentos falsos como correos electrónicos fraudulentos o interfaces bancarias clonadas, cuyo fin es netamente causar un engaño. El apartado 1 castiga la alteración o introducción de contenidos de plataformas considerados engañosos o suplantación de una entidad legítima. El siguiente apartado penaliza el uso de la información adquirida con el objetivo de obtener un beneficio ilícito.

Zaffaroni (1998) considera que los discursos jurídicos penales han deslegitimado su función garantista como resultado de una carencia de definiciones jurídicas exactas. El sistema judicial ecuatoriano recurre a interpretaciones análogas o expansivas; es aquí donde los juristas se encargan de limitar medidas de respuesta punitiva que evitan las deficiencias técnicas del legislador, así no se dará lugar a una arbitrariedad judicial que ignore la realidad tecnológica y vulnere el derecho del ciudadano.

El COIP, es un instrumento normativo que penaliza delitos, sin embargo, se evidencia que esta norma mantiene vacíos legales, que limitan su aplicabilidad, al momento de ejercer sanciones penales causadas por una falta de definiciones jurídicas que sean definidas claramente en delitos digitales. Se observa en el artículo 232, que existe una imprecisión en conceptos donde solo se alinean en el atracador, contra los sistemas informáticos, demostrando una respuesta jurídica ineficaz. El phishing se ha asociado a delitos tradicionales, por su parte el art. 186 lo considera al engaño como un mecanismo, que permite obtener beneficios de tipo monetario: mientras que el artículo 190, describe a la transferencia fraudulenta de información gracias al uso de instrumentos tecnológicos: el artículo 230 y 234, consideran que un delito es existente cuando se limita una interpretación de datos o se presenta un acceso no autorizado; y el artículo 234.1 se indica pertinente que el ciberdelincuente reemplace la identidad de un tercero con el uso de una interfaz o documento digital.

2.2.3.2 Cooperación internacional "Convenio de Budapest"

El Convenio de Budapest fue suscrito en el año 2001; es un tratado internacional que influye en la armonización de legislaciones nacionales y promueve la creación de una política penal ante la amenaza digital. Su finalidad es el fortalecimiento de la cooperación internacional, mediante acciones vinculadas a la confidencialidad, disponibilidad e integridad de los sistemas y datos informáticos; estos elementos se adecuan al derecho para enfrentar los retos de la digitalización. Incluye definiciones que detectan, indagan y persiguen ciberdelitos, al tiempo que garantiza el respeto de los derechos humanos y la protección de la información (Consejo de Europa, 2001).

El Convenio de Budapest es el mayor referente contra la ciberdelincuencia. En el cual participan varios Estados, uno de estos, Ecuador, que ratificó su cooperación como el 77. ° integrante, por lo tanto, el país alinea sus leyes con normas internacionales, proporciona

intercambios de información y recolecta evidencia digital (Coronel & Argüello, 2025). La adhesión formal del Estado ecuatoriano a este Convenio se consolidó oficialmente en el Decreto Ejecutivo N° 332, suscrito el 12 de julio del año 2024, posterior al dictamen favorable de la Corte Constitucional y la aprobación de la Asamblea Nacional (Presidencia de la República del Ecuador , 2024).

La ratificación del país al Convenio de Budapest constituye un evento importante en la modernización del marco jurídico nacional como refuerzo de la ciberseguridad. Entre las ventajas de este proceso se encuentran: la mejora del funcionamiento institucional, el acceso a instrumentos tecnológicos especializados en investigaciones y el establecimiento de una clasificación detallada de delitos cibernéticos en el Código Orgánico Integral Penal. No obstante, su ejercicio aún se confronta con limitantes estructurales, que recaen en la necesidad de una reforma legislativa, en la escasez de profesionales especializados en todas las regiones del país y en la insuficiente capacitación sobre seguridad cibernética (Iñiguez et al., 2025).

El instrumento internacional descrito permite combatir ciberataques como el phishing. En el Ecuador, esta norma sobrepasa limitantes que se asocian a la soberanía del territorio, intercambio de información y pruebas volátiles recopiladas en tiempo real gracias a la red de apoyo internacional. Es decir, en el Convenio de Budapest, se exponen reglas que permiten detectar delitos digitales, por medio de una simbiosis entre la eficacia de las investigaciones y el respeto de los derechos del ser humano. Representa un aspecto importante en la ciberseguridad nacional, debido a que permite el acceso a instrumentos tecnológicos especializados y a una política penal, de forma indirecta, refuerza la capacidad operativa y la formación continua de profesionales.

2.2.3.3 Análisis de la operación KAERB 2024, Ecuador.

El estudio se fundamenta en criterios de pertinencia y relevancia, obtenidos del boletín de prensa FGE N° 1048-DC-2024, de la Fiscalía General del Estado, junto con la sección de noticias del portal oficial de la Policía Nacional, y medios de comunicación como El Diario (2024), La Hora (2024) y Primicias (2024) que redactan detalles específicos sobre la operación.

La operación KAERB evidencia un paso importante en la lucha contra la ciberdelincuencia transnacional, desmanteló una red en Europa y América, que operaba por cinco años bajo el modelo de crimen como servicio. El proceso investigativo tuvo una duración aproximada de dos años, descubrió la compleja estructura criminal que combina delitos físicos con ciberdelitos. El diseño delictivo incluye el uso de la plataforma "*iServer*", que según información pública, era manipulada desde Argentina, por una persona encargada de brindar soporte técnico a más de 2.000 usuarios, denominados "desbloqueadores", quienes empleaban dicha plataforma para comprometer la seguridad de los dispositivos móviles de gama alta, robados, afectaron a cerca de 483.000 víctimas a nivel mundial, de las cuales, 42.000 fueron registrados en el Ecuador.

El modus operandi de los ciberdelincuentes se sustenta en el uso de diferentes dominios web con métodos de pago anónimos, que permitían alcanzar campañas de phishing automatizado a través de mensajes de texto y correos electrónicos fraudulentos; las víctimas recibieron falsas promesas ante la recuperación de dispositivos móviles robados; sin embargo, los enlaces los redirigieron a interfaces diseñadas para apoderarse de usuarios y contraseñas. Al obtener esta información, los delincuentes cibernéticos desbloqueaban de forma ilegal sus dispositivos, accedían a información sensible que permitía el ingreso a su cuenta de "Binance". El alcance de las acciones de esta red criminal fue demostrado por la operación ejercida en septiembre del año 2024, que dejó un total de 28 allanamientos en Ecuador, España, Argentina, Chile, Perú y Colombia, la detención de 17 personas y el cierre del servicio web.

Gracias a la Unidad Nacional del Ciberdelito de la Policía Nacional y la Fiscalía General del Estado, pudo encarcelar a dos personas quienes operaban en la provincia de Santo Domingo de los Tsáchilas. Una operación policial, de registro domiciliario, ha facultado a las personas a que se logre incautar un total de 921 dispositivos como elementos de prueba, permitiendo determinar además un total de 23 dispositivos celulares, 11 discos duros y 30 dispositivos de USB. Por otro lado, se decomisaron *tablets*, computadoras y un arma de fuego con un total de 62 cartuchos y criptomonedas. Estas acciones, han permitido conseguir una destrucción de un ente digital que se ha dado inicio a un proceso judicial que se sustenta en el artículo 234 del Código Orgánico Integral Penal, cuyo éxito recalca la necesidad de una cooperación efectiva entre fiscales, cuerpos policiales y servicios de inteligencia como la Europol, Ameripol y PACCTO 2.0, junto con empresas privadas "Group-IB".

La operación KAERB 2024 ha permitido obtener una comprensión profunda sobre la ciberdelincuencia. Al desmantelar la plataforma "*iServer*", se demostró que los actos criminales son modelos automáticos. El caso indica un robo físico de un dispositivo móvil, como una acción preparatoria ante un delito de gran magnitud. La utilización de interfaces fraudulentas, bajo bosquejos de suplantación de identidad, no incluye solo acciones de engaño, sino que se transforma en manipulación técnica del consentimiento, donde el atacante induce a la víctima a proporcionar sus credenciales de acceso.

El modus operandi de los ciberdelincuentes indica que esta modalidad de phishing usa mensajes y correos electrónicos que redirigen a los usuarios a interfaces duplicadas. Ante esto, el actuar de las personas responsables se pone en manifiesto dentro de un sistema piramidal con un soporte técnico, que brinda desde el extranjero los insumos necesarios a terceros para gestar ataques en el país. Al aplicar el artículo 234 del Código Orgánico Integral Penal, se evidencia cómo el sistema judicial adecúa a delitos existentes la compleja realidad tecnológica. La incautación de diferentes pruebas digitales demuestra que en Ecuador se aplican actividades delictivas simultáneas en el ciberespacio.

CAPÍTULO III

3. METODOLOGIA

El presente estudio aplica una metodología sustentada en el paradigma interpretativo, cuya finalidad es comprender e interpretar fenómenos sociales complicados; el conocimiento nace de la interacción con el entorno, la cual se acompaña de un enfoque cualitativo, que contribuye a la recolección de fuentes consultadas, y desarrolla hipótesis en relación con la realidad investigada (Martínez, 2013). Se utiliza un alcance de tipo analítico, el cual permite descomponer los cuerpos jurídicos (Villabella, 2020); la estrategia dual se apoya en la triangulación de la información para establecer medidas de prevención que fomenten una detección adecuada de ataques de phishing y conviertan el perfil criminológico del ciberdelincuente en un instrumento práctico.

Según el criterio de Guamán et al. (2021), la investigación se estructurará en base a dos dimensiones:

- **Dogmático-jurídico:** Valida e interpreta de manera formal la legislación, tras el análisis del Código Orgánico Integral Penal y el Convenio de Budapest.
- **Socio-jurídico:** Examina la influencia de la realidad social, que causa una metamorfosis dentro del sistema jurídico, por lo tanto, la presente tesis utiliza experiencias empíricas, donde se estudien componentes delictivos y falencias institucionales.

3.1 Unidad de análisis

Gramajo (2012) describe la unidad de análisis como un elemento que da respuesta a los objetivos, así como a las preguntas de indagación. En el plano jurídico, dichas unidades hacen referencia a fenómenos normativos, donde la información es obtenida por medio de documentos, entrevistas o encuestas, con sujetos de investigación. Adicionalmente, es importante considerar que la información obtenida se contextualiza en la República del Ecuador, al centrar su panorama en un contexto operativo-jurídico.

El estudio coloca como fuentes informativas principales a los agentes del sistema de justicia, investigación y seguridad, en conjunto con el material bibliográfico y normativo; estos son los recursos de conocimientos teóricos-fácticos que permiten identificar patrones criminales de ciberdelincuentes y validar estrategias que promuevan una detección eficaz; a lo expuesto se suma el estudio de la “Operación KAERB 2024 Ecuador” que contrasta la información recopilada.

3.2 Métodos

En base al criterio de Lara (2022), se considera al método como la estructura seleccionada por el investigador, que engloba un tema a profundidad para obtener nuevos conocimientos, incluye pasos que garantizan la veracidad del discernimiento, comprende mecanismos seleccionados cuidadosamente, que al combinarlos, permiten tanto el análisis

normativo como la identificación de patrones comportamentales del ciberdelincuente, al sintetizar datos cualitativos proporcionados por profesionales y fuentes consultadas:

- **Método inductivo:** El método inductivo examina hechos o sucesos específicos, los cuales son definidos en base a elementos generales, el proceso permite recopilar conocimiento por medio de la identificación de tendencias marcadas (Villabella, 2020), el estudio, emplea este método con el objetivo de desarrollar entrevistas dirigidas a expertos, incluye la exploración de la "Operación KAERB", para generar características que definan al ciberdelincuente y aspectos referentes a la respuesta institucional del phishing.
- **Método jurídico-analítico:** Separa de manera desglosada un tema, cuya finalidad es comprender principios o componentes e identificar interrelaciones. Son herramientas necesarias que permiten reconstruir teóricamente el fenómeno en estudio (Zenteno y Osorno, 2016). Al emplear un análisis meticuloso del Código Orgánico Integral Penal, se determina qué delitos se aplican al razonamiento analógico ante la nula definición jurídica del phishing, además, destaca la cooperación internacional, que se prevé en el Convenio de Budapest para el fortalecimiento institucional.
- **Método jurídico-doctrinal:** Realiza un estudio técnico de documentos jurídicos y fuentes bibliográficas, cuyo objetivo se sustenta en el establecimiento del significado y alcance del fenómeno de estudio (Celis, 2024), se aplica en la tesis, con la finalidad de brindar una explicación del porque el phishing no se comprende con precisión en Ecuador, proporciona una base teórica necesaria para identificar a los ciberdelincuentes, su enfoque permite la caracterización de limitantes en el área jurídica-operacional, establece un marco doctrinario que justifica la construcción del perfil criminológico como mecanismo de detección oportuno.
- **Método jurídico-descriptivo:** Analiza un tema jurídico, con un enfoque profundo (Aldaz, 2023). Se aplica en el estudio de caso "Operación KAERB 2024" y la información recopilada durante las entrevistas. Cada una de estas acciones identifica técnicas operativas del ciberdelincuente, la utilización de nuevas tecnologías y la fragmentación de unidades especializadas, en base a la comprensión del phishing en el país.

3.3 Enfoque de investigación

Witker (2014) manifiesta que el enfoque cualitativo en la investigación jurídica es una perspectiva que pone en primer plano el contexto y el funcionamiento de las normas e instituciones, considera el derecho como un fenómeno social, para obtener una comprensión profunda y completa de los patrones criminológicos asociados con el phishing. Examina el problema dentro de su realidad natural, tiene en cuenta la experiencia de los participantes en relación a los ciberdelitos y las deficiencias institucionales, incluye el análisis del caso "Operación KAERB 2024". Se entiende que el estudio cualitativo permite recopilar

información única sobre rasgos de ciberdelincuentes desde una perspectiva específica orientada a la detección temprana del phishing.

3.4 Tipo de investigación

Se ha considerado pertinente, incluir algunos tipos de estudio, los cuales permitirán que la investigación no solo se restrinja al detalle de la deficiencia de entres gubernamentales y estatales, permitiendo dotar de soluciones de ciberdelincuencia, generando una guía innovadora, que se manifiesta con un impacto clave en la forma comportamental del ciberdelincuente, que refuerza la capacidad de detección adecuada del phishing, esta tipología son seleccionados en base a lo sustentado por antaleán (2015):

- **Investigación jurídica descriptiva:** Esta forma de investigación facilita la identificación de rasgos y propiedades de una entidad o fenómeno jurídico. En su forma actual, se describe y precisa, que servirá como sustento en la fase inicial, que justificará su partida, para esto, se detallarán tres dimensiones necesarias. Los rasgos actuales, grado de actualización del phishing en el país, fortalezas, debilidades, así como un estudio profundo del marco normativo y de cada entidad existente que podrá relacionarse, que se vincule con el comportamiento del ciberdelincuente.
- **Investigación jurídica exploratoria:** Emplear este tipo investigativo, sustentará una indagación inicial que considerará un temario poco estudiado en la comunidad jurídica, su meta es brindar una familiarización de un fenómeno, determinando características fundamentales, sentando un pilar para el diseño de nuevos estudios y si es necesario, se podrá brindar una contextualización por región en el país. Cuando se constituye el perfil criminológico, el ciberdelincuente, podrá detectarse de manera adecuada, aquí el phishing, podrá profundizarse a mayor escala, su carácter, exploratorio, facultará un análisis de la problemática, considerando además entrevistas de tipo semiestructuradas, que fueron aplicadas en profesionales con conocimiento en la materia, permitiendo consolidar información, tendencias, procesos, así como un análisis de la "Operación KAERB 2024 Ecuador" para obtener un soporte pragmático.

3.5 Diseño de investigación

Se aplica un estudio de tipo trasversal no experimental, que permite explorar cada una de las categorías de análisis en su propio entorno, no se manipula ninguna, solamente se observa los fenómenos según su realidad, el diseño trasversal permite recolectar información por una sola vez en un momento determinado, proporciona un entorno instantáneo de los acontecimientos actuales (Arias, 2021).

3.6 Población y muestra

Según la percepción de Castro (2019), la población hace referencia al universo completo de elementos, de quienes se obtiene la información, a diferencia de la muestra, que es considerada un subconjunto de la población, derivada de un proceso de selección en base

a su pertinencia o relevancia, con el fin de adquirir información que permita extraer conclusiones.

- **Población:** Se compone de agentes del sistema de justicia, seguridad e investigación especializados en delitos digitales y ciberdelincuentes, lo que constituye el aspecto pragmático.
- **Muestra:** Selección de expertos que cumplen características específicas en especialización del phishing junto al análisis criminológico de ciberdelincuentes.

Tabla 2. *Ficha técnica de especialistas que participarán en la entrevista.*

CARGO	CONTRIBUCIÓN	NÚMERO DE PARTICIPANTES
Jefe de la Unidad Nacional de Ciberdelito de la Policía Nacional del Ecuador	Su aporte se sustenta en la detección, prevención, procesamiento técnico y el análisis comportamental del ciberdelincuente.	1
Criminólogo_ Perito Acreditado por el Consejo de la Judicatura	Faculta de conocimiento científico y sustento teórico, que permite establecer rasgos importantes del ciberdelincuente.	1
Agente Fiscal_ Unidad Especializada de Patrimonio Ciudadano	Aporta información en base a competencias fiscales de procedimientos penales, con un análisis de la clasificación de ciberdelitos, especialmente el phishing.	1
Juez_ Presidente de la Corte Provincial	Permite obtener un contexto actual sobre las brechas procesales, así se justifica la necesidad de aplicar un análisis criminológico como mecanismo de apoyo.	1
Abogada_ Especialista en Ciberseguridad	Brinda información sobre ciberseguridad, que combate al phishing mediante un análisis criminológico, con emisión de estrategias legales que se adaptan a la realidad actual.	1
	Total:	5

Nota: Elaborado por Salguero, S. (2026). La tabla describe detalladamente las áreas de especialización de los participantes, abarca aspectos científicos, operativos, investigativos y legales. Esto proporciona una visión completa del fenómeno del phishing y la ciberdelincuencia en el contexto ecuatoriano.

Por otro lado, se ha considerado pertinente incluir el estudio de un caso práctico, necesario para recopilar datos sobre métodos empleados por ciberdelincuentes, la respuesta institucional, los factores criminógenos y los riesgos sistémicos del phishing:

- Operación KAERB 2024.

3.7 Técnicas e Instrumentos de investigación

Las técnicas e instrumentos, que se han considerado en el presente estudio, brindan datos relevantes, que serán recopilados en base al conocimiento de los investigadores, por medio de entrevistas, que actúan como un mecanismo poderoso en la interacción directa entre el entrevistador y el entrevistado, así se obtendrá información confiable (Guanoluisa et al., 2023).

- La técnica principal dentro de la recolección de información primaria es la entrevista semiestructurada, la cual será aplicada a expertos de la materia, que determinan patrones delictivos, estrategias de operación, identificación de ataques de phishing y retos existentes en el sistema jurídico e instituciones.

Asimismo, se apoyará con la información obtenida en la revisión documental-normativa y con el análisis del caso "Operación KAERB 2024", como evidencia empírica para la triangulación de los datos de las entrevistas.

3.8 Técnicas para el tratamiento de información

Calle y Gil (2015) las definen como el conjunto de fases continuas que permiten la obtención de información, por medio del establecimiento de un orden, que facilita su interpretación; son necesarias en la conservación de información de datos, confirmación de fiabilidad y transmutación a conclusiones:

3.8.1 Elaboración del instrumento de investigación

En esta etapa, se aplica un diseño del instrumento empleado, es decir, la entrevista semiestructurada aplicada a expertos, en conjunto con la revisión literaria y el estudio del caso "Operación KAERB 2024".

3.8.2 Aplicación del instrumento de investigación

Se aplicaron las entrevistas a expertos en el tema, para recopilar información, cuyos datos se integran a los aspectos obtenidos en el análisis documental-normativo y la indagación del caso previamente mencionado, lo que refuerza su sentido pragmático.

3.8.3 Tabulación de datos

Una vez obtenida la información, se codifica en base a lo obtenido en la aplicación de la entrevista, la información literaria-normativa y el estudio de caso "Operación KAERB

2024” acoplado en una tabla de análisis, lo que facilita el proceso de interpretación y argumentación.

8.3.4 Procesamiento de los datos e información

La información se recopila individualmente, para luego clasificarla según su pertinencia, proceso que facilita el análisis de datos para responder a la pregunta de investigación, se incluye una definición de cada categoría de análisis (Valdés, 2008). Dentro de esta etapa, se examinan los objetivos de estudio para clasificarlos en temas específicos.

8.3.5 Interpretación o análisis de resultados

Los datos serán convertidos en afirmaciones conceptuales, que superan una descripción empírica; la teoría nace de una realidad investigada, que se vincula con un análisis descriptivo de fuentes primarias y secundarias, las cuales dotan de información interpretativa para los resultados (Mejía, 2011). El proceso de triangulación de datos incluye información de expertos, como sucesos descritos en el caso “Operación KAERB 2024”; se considera también el estudio del marco dogmático-jurídico.

8.3.6 ***Discusión de resultados***

Los datos recopilados se discuten, con respecto a caracteres teóricos de información y estudios asociados a las categorías de análisis, que permiten extraer conclusiones para confirmar la conjetura planteada, sin alejarse de los objetivos de la tesis (Contreras et al., 2022).

CAPÍTULO IV. RESULTADOS Y DISCUSIÓN

4.1. Resultados

Este capítulo contiene los hallazgos relevantes del estudio, obtenidos de la triangulación de datos, que combina el análisis doctrinal-normativo, el estudio de caso "Operación KAERB 2024" y la sapiencia técnica recolectada por medio de entrevistas efectuadas a expertos del sistema judicial, de seguridad e investigación de Ecuador. La muestra poblacional se encuentra descrita por:

El conocimiento propio que se consolida con el paso de los años y la práctica en ingenieros informáticos y que coexiste con organizaciones internacionales como la INTERPOL y la ONU. Se observa, que el experto Tlgo. Carlos García, Jefe de la Unidad Nacional de Ciberdelitos de la Policía Nacional, son autores que han dotado de un enfoque completo que certifica un sustento teórico en la información. El sustento científico y la experiencia en la perfilación criminal de Jaime Alfonso Guevara Pintado, criminólogo avalado por el Consejo de la Judicatura, permite una comprensión de la silueta en la conducta del ciberdelincuente.

Por su parte, I.A.G.V., Presidente de la Corte Provincial de Justicia de Tungurahua, y el Agente Fiscal de la Unidad de Patrimonio Ciudadano de la Fiscalía Provincial de Tungurahua con sede en Ambato, Gustavo Fernando Casco Lozada, ofertan una visión crítica de los desafíos relevantes a los que se enfrenta la judicialización del phishing y la necesidad de contar con instrumentos técnicos adecuados. Finalmente, la abogada e ingeniera en sistemas Clara Marisela V. L., especializada en ciberseguridad y protección de datos, describe aspectos técnicos del ciberdelito y retos institucionales.

4.1.1 La cibercriminología y los elementos constitutivos del perfil criminológico.

4.1.1.1 Opiniones de agentes del sistema de justicia, seguridad e investigación especializados en delitos y antisociales cibernéticos.

4.1.1.1.1 Resúmenes de las entrevistas.

Entrevistado 1

En Ecuador, la ciberdelincuencia ha desplazado las infracciones físicas hacia el ciberespacio. Según el criterio del Tcnl. Carlos García, el ciberdelincuente, no necesita una formación universitaria previa ni conocimientos especializados. Es decir, solo requiere acceso libre a herramientas digitales y la capacidad de emplear búsquedas dentro de redes sociales. El atacante aprovecha dos factores críticos: la exposición de datos personales no autorizada y el desconocimiento digital que impacta entre el 90% y el 95% de la población.

En la actualidad, los jóvenes poseen un riesgo incrementado de ser víctimas; su exceso de confianza les conduce a aceptar perfiles falsos o incluso compartir información personal dentro de plataformas digitales; de igual forma, se evidencia que los niños

experimentan una exposición considerable en los juegos digitales. Es así, como la ciberdependencia ha facilitado la recepción de información personal de carácter sensible por medio de mecanismos tecnológicos, lo que favorece a los ciberdelincuentes para gestar ataques de ingeniería social.

Entrevistado 2

De acuerdo con el criterio de Jaime Guevara, el perfil criminal se define como una herramienta de investigación, cuya función es reconocer a ciberdelincuentes desconocidos, emplea un estudio de rasgos conductuales, que se evidencian en la escena del crimen, este análisis posee un enfoque vinculado al modus operandi y la firma del infractor, examina métodos de ataque, hábitos de contacto, pruebas materiales y comportamiento.

El uso del perfilamiento criminal disminuye el número de personas sospechosas, brinda datos sociodemográficos, educativos y de edad, así se determina si la persona infractora es organizada o no; todo esto se sustenta en el estudio de expedientes. Las personas afectadas identifican que su vulneración nace en la sensibilidad frente a medios tecnológicos, la falta de conocimientos en ciberseguridad y la carencia de capacidades especiales, lo cual las convierte en agentes susceptibles a manipulación ejercida mediante llamadas o mensajes que simulan provenir de fuentes legítimas.

Entrevistado 3

El Agente Fiscal Gustavo Casco indica que el perfil criminológico del ciberdelincuente presenta características específicas como la adopción de un dominio técnico de software y otros mecanismos digitales, utilizados con fines maliciosos. Los delincuentes cibernéticos son personas que tienen conocimiento informático clave para maniobrar servicios web, correos electrónicos o mensajes de texto, lo que les permite insertar virus y robar datos personales.

Un agresor quien se ha especializado en el delito estudiado, puede adquirir una gran habilidad en el acceso a información de tipo económico, que se asocian con cuentas del banco, tarjetas de créditos. Sin embargo, es necesario considerar que las víctimas han presentado un desconocimiento en el área de seguridad informática, que impacta en adultos mayores quienes, son identificados como los más vulnerables a causa de su descornamiento en el área digital, así podrían anticiparse a riesgos, como una inadecuada transacción electónica.

Entrevistado 4

I.A.G.V., menciona que el perfil criminal del ciberdelincuente especializado en el phishing presenta rasgos comportamentales psicopáticos como trastornos antisociales de la personalidad y falta de empatía, lo que permite usar un lenguaje manipulador para engañar a sus víctimas. Los atacantes tienen conocimiento técnico avanzado en temas informáticos, gestión de redes, sistemas electrónicos y procesos de hackeo. Sus acciones se enfocan en la aplicación de fraudes informáticos o bancarios con el mínimo esfuerzo.

Las cibervíctimas son vulnerables por su bajo nivel de conocimiento en ciberseguridad, y comportamientos de riesgo que recaen en el uso de redes Wi-Fi públicas, mantenimiento de software antiguos y la utilización de dispositivos desprotegidos. Las consecuencias más frecuentes son el robo de identidad, estafas en redes, pérdida de acceso a cuentas bancarias, que suelen derivarse en otros delitos como ciberacoso o sexting.

Entrevistado 5

Con sustento en esto, Clara Marisela V. L., indica que los ciberdelincuentes, se caracterizan por que aplican un estudio profundo, demostrando que los patrones comportamentales se presentan organizados, aplicando métodos de ingeniería social determinadas, que se vinculan con comportamientos digitales y el papel de las víctimas. Se han mostrado determinantes criminológicos, que describen a la inequidad digital, entre un atacante y un operador que es la víctima, la cual mantiene una percepción escasa del riesgo criminal que podría mantener, así como una baja consideración de costos de funcionamiento.

Las personas afectadas muestran que su vulneración se asocia a una carencia de cultura de ciberseguridad, con nulas habilidades dentro de la web y una sobredependencia a medios comunicativos. Por su parte, el agresor emplea factores psicológicos como el sentimiento de urgencia y el miedo para manipular a los individuos e incitar a tomar acciones impulsivas.

4.1.1.1.2 Análisis de entrevistas a expertos.

El análisis de las entrevistas identifica una problemática alarmante, que asocia el fenómeno de la ciberdelincuencia en el país con factores técnicos, psicológicos y educativos. El Tcnl. Carlos García evidencia que el perfil criminal del ciberdelincuente no requiere una especialización profunda, solo necesita de la exploración en el ciberespacio. Esta visión es matizada por el Agente Fiscal Gustavo Casco e I.A.G.V., quienes identifican al ciberdelincuente como un individuo con conocimiento técnico en software, gestión de redes y sistemas informáticos. A su vez, el criminólogo Jaime Guevara adapta una dimensión metodológica, que expone las habilidades digitales y el modus operandi del infractor, como indicadores que permiten clasificar a los sospechosos a través del estudio de expedientes y pruebas.

Los aspectos psicológicos y estratégicos que permiten la comisión de un atacante son mencionados por I.A.G.V. que destaca los rasgos psicopáticos y el trastorno antisocial de la personalidad, así como la utilización de un lenguaje persuasivo para manipular a las víctimas. Aporte que se profundiza por el pensamiento de la experta Clara Marisela V. L., quien induce el concepto de asimetría tecnológica, al mencionar el aprovechamiento de factores psicológicos como el miedo y la urgencia para generar respuestas impulsivas. Finalmente, la alta rentabilidad y los costos operativos bajos conllevan una mínima percepción de riesgo criminal, lo que transforma los ataques aleatorios en ataques impulsados por la ingeniería social, criterio compartido por el Tcnl. Carlos García y Clara Marisela V.L.

La vulnerabilidad de las cibervictimas expone una segmentación clara, comparten un denominador común: falta de competencias digitales. Según el Tcnl. Carlos García, los niños y adolescentes, tienden a ser más vulnerables por su alta confianza y dependencia en plataformas digitales. El Agente Fiscal Gustavo Casco menciona otro grupo vulnerable: los adultos mayores, expuestos a riesgos financieros por una insuficiente asesoría en transacciones electrónicas. El criminólogo Jaime Guevara y Clara Marisela V.L. coinciden en que la fragilidad de las cibervíctimas se deriva de su analfabetismo digital, que, según el Tcnl. Carlos García, afecta entre el 90 y el 95 %, además reconoce como problemática la falta de cultura digital. Mientras I.A.G.V., argumenta que las conductas de riesgo, como el uso de redes Wi-Fi públicas y softwares antiguos, fomentan la vulnerabilidad.

4.1.1.2 Análisis doctrinal.

La cibercriminología, según el criterio de Cámara (2020), es considerada una rama de la ciencia empírica interdisciplinaria, integra la tríada criminal al entorno digital. Es considerada una disciplina que va más allá de una simple valoración de comportamientos antisociales básicos; estudia la causa de los delitos que se originan dentro del ciberespacio y mantiene un equilibrio técnico-emocional en la interfaz hombre-máquina. Alvaracín (2023), por medio de su criterio, expone que, en la actualidad, el individuo ha pasado de un control físico limitado a un panóptico digital, cuyo poder se manifiesta por medio de un monitoreo continuo de datos. La criminología moderna se enfoca en sistemas digitales gestionados por mecanismos de dominio sobre el comportamiento humano.

El origen de la ciberdelincuencia se relaciona con el desarrollo tecnológico. Punín (2021) enfatiza que el comportamiento antisocial se expandió al encontrar nuevas oportunidades en el mundo digital carente de fronteras físicas. Dicho autor, expone que un ciberataque, dependerá de su técnica, de si se aplica o no una réplica y de su contenido. Sin embargo, con el avance tecnológico, se han ampliado sus mecanismos en la tecnocriminología. Es así como en base al criterio del Colegio Profesional de la Criminología de la Comunidad de Madrid (2025), deberá exigirse al funcionario que evalúa el área del crimen digital, que mantenga su ética algorítmica que le permita manejar peligros para las víctimas de forma autónoma por medio de la inteligencia artificial.

Un perfilamiento en criminología, es un mecanismo técnico importante que permite determinar una motivación y rasgos biográficos del ciberdelincuente. Márquez (2022) describe estos métodos desde el enfoque inductivo y deductivo. Según López (2022), suelen ser nativos digitales, que a menudo pertenecen a la clase media o alta, y aprovechan el cifrado de identidad. Jativa et al. (2025) determinan tres dimensiones de la estructura conductual: la superioridad técnica, el anonimato estratégico y la deshumanización de la víctima; los ataques son influenciados por el poder, el lucro o la venganza.

El modus operandi del delincuente en el ciberespacio se encarga de armonizar las herramientas de tecnología e ingeniería social. Castillo (2021) clasifica a los ciberdelincuentes en base al nivel de experiencia, que va desde el empirismo hasta llegar a un experto en informática. La INTERPOL y el documento técnico “El Phishing” exponen

métodos sofisticados que exploran la confianza humana para adquirir datos sensibles. Mientras que Montiel (2020) y López (2020) alertan que la ciberdelincuencia ya no es un hecho aislado, ahora se encuentra en un estado de vulnerabilidad permanente, que causa daños a los sujetos pasivos e incluso da lugar a otras formas de delito.

4.1.2 Sofisticación del phishing y limitaciones jurídico-institucionales para su detección.

4.1.2.1 Opiniones de agentes del sistema de justicia, seguridad e investigación especializados en delitos y antisociales cibernéticos.

4.1.2.1.1 Resúmenes de las entrevistas.

Entrevistado 1

Según el Tcnl. Carlos García, la evolución del phishing en el país evidencia una creciente sofisticación de ciberdelitos, impulsados por la aplicación de inteligencia artificial. El uso de herramientas tecnológicas permite la adopción de mensajes personalizados o smishing, que mantiene una similitud gramatical expedita y perfecciona el robo de identidad. También se han identificado métodos más avanzados como la utilización de códigos QR de carácter malicioso y la clonación de voz donde la IA captura patrones de audio de los afectados. Ante los avances de la digitalización, el sistema institucional no logra evolucionar a la par del phishing. La ausencia de una definición legal precisa en el Código Orgánico Integral Penal crea un vacío donde los investigadores y los juristas están obligados a adecuar comportamientos cibernéticos en delitos tradicionales.

Entrevistado 2

Jaime Guevara argumenta que, en el último año, se ha registrado un aumento aproximado del 60 % de ciberdelitos, impulsado por la creciente sofisticación de los delincuentes y el uso de nuevas tecnologías, como la inteligencia artificial. El triunfo de un ataque dependerá de la oportunidad que presenta el atacante, donde se aprovechará de su anonimato en entorno digital, su conocimiento previo y el que con el tiempo va adquiriendo, así podrá anexarse a sus víctimas. No obstante, la respuesta institucional se ha visto ineficaz, como consecuencia de una limitación legal: aunque no existen artículos que los vinculen a delitos cibernéticos, las normas actuales requieren de una actualización rápida que la evite. En el mundo actual estas medidas se podrán clasificar en base a delitos como la estafa, cayendo en lagunas que los ciberdelincuentes usan para su beneficio.

Entrevistado 3

El Agente Fiscal Gustavo Casco asevera que, en el país, se ha identificado un crecimiento y sofisticación de delitos digitales, fenómeno analizado en las investigaciones penales. Los ataques se han consumado mediante interacciones con correos electrónicos fraudulentos que logran el robo de credenciales para acceder a plataformas tecnológicas. Con relación al marco institucional, se han encontrado limitaciones en el área operativa con un

alcance crítico; es así que la centralización de la Unidad Nacional de Ciberdelitos de la Policía Nacional del Ecuador en Quito refleja un retraso investigativo en las demás provincias del país. Aunque existe normativa, su aplicación aún plantea problemas; el público desconoce en gran escala los instrumentos jurídicos como la ley de protección de datos personales.

Entrevistado 4

El Estado ecuatoriano ha sido testigo de un incremento en la sofisticación de ataques asociados al phishing. Los datos de la Fiscalía denotan un aumento significativo previsto hasta el año 2025. Los infractores abusan de su anonimato digital, la aplicación de instrumentos digitales como la inteligencia artificial y su capacidad para cometer delitos desde países extranjeros, esto complica la concepción de jurisdicción y competencia penal. En relación con las instituciones, se observa que existe una limitación grave en operaciones, como la falta de laboratorios forenses y la escasez de especialistas en esta área, como es el caso de Tungurahua, que cuenta con un perito, ante lo cual las víctimas recurren a especialistas privados. Lo expuesto complica la investigación y la determinación de culpables en base al artículo 453 del Código Orgánico Integral Penal; este criterio fue emanado por I.A.G.V.

Entrevistado 5

Según la experta Clara Marisela V. L. existe un incremento significativo de este tipo de delitos en el Ecuador, que, con el paso del tiempo y el desarrollo informático, se ha extendido de forma masiva, aprovecha el uso de gráficos profesionales, dominios falsos con características visuales similares y la integración de malware. La entrevistada encuentra limitantes en la detección oportuna, que se traducen en la falta de coordinación interinstitucional, en el funcionamiento aislado de entidades y en la demora de procesos judiciales. Asimismo, enfatiza problemas que se alinean con la falta de recursos tecnológicos para llevar a cabo investigaciones digitales y la dificultad jurídica de procesar los delitos efectuados a nivel nacional e internacional, por ende, es relevante la aplicación de una colaboración mutua entre instituciones, Estado y ciudadanos.

4.1.2.1.2. Análisis de entrevistas a expertos.

Por medio del análisis de las entrevistas, se observa que, en Ecuador, el phishing ha pasado de ser una práctica antigua o rudimentaria a transformarse en un fenómeno técnico complejo. El Tcnl. Carlos García manifiesta que el uso de la IA ha impulsado el desarrollo del smishing y la clonación de voz, cuya forma de engaño es casi imperceptible. Este criterio se reafirma, con la opinión del criminólogo Jaime Guevara, quien cuantifica su impacto al observar un aumento del 60 % en los delitos cibernéticos en contraste con los años pasados, que se alimentan por el anonimato y la especialización técnica.

La especialista Clara Marisela V.L. indica que esta evolución no solo surge en la parte técnica, sino que también maneja un componente estratégico; en donde se usan

dominios falsos que son visualmente semejantes a los legítimos, espacios de interfaz que añaden a plataformas malwares agresivos que afectan a la víctima. Ante esta situación, el Agente Fiscal Gustavo Casco confirma que los delitos vinculados al robo de credenciales con el uso de correos electrónicos fraudulentos son ahora un fenómeno recurrente en las investigaciones penales del país.

En el ámbito jurídico, se determinan retos críticos entre la innovación criminal y la respuesta institucional. El Tcnl. Carlos García advierte que el avance tecnológico ha evolucionado desmedidamente, motivo por el cual la ley no consigue subsanar estos vacíos jurídicos, y obliga a los juristas a adaptar delitos tradicionales al mundo digital. Con un criterio similar, Jaime Guevara e I.A.G.V. mencionan la necesidad de definir al phishing como un delito, bajo criterios del Código Orgánico Integral Penal, para evitar que estos actos ilícitos queden en la impunidad. Se debe considerar que la I.A.G.V. plantea que existe una posibilidad de que un ciberdelincuente acciones desde un lugar lejano al país en donde se aplica la fechoría, impactando en el ejercicio penal e impactando en la responsabilidad jurídica.

Finalmente, el autor indica que ante la existencia de restricciones en las competencias de instituciones y funcionarios dentro de las operaciones en el Ecuador. Motivo por el cual, el agente Fiscal Casco, confirma que la centralización de unidades que son del área, solamente se encuentras existentes en la ciudad de Quito, causando un gran retraso en los casos que se presentan en otros sectores del país, logrando poner en manifiesto que una cultura digital en los habitantes es una necesidad que les proporcionará conocimiento y mecanismos preventivos o defensorios. Esta falta de recursos es especialmente grave en provincias como Tungurahua, donde, según I.A.G.V., apenas existe un perito quien es el encargado de analizar casos en el área pública, situación que obliga a las víctimas a recurrir a especialistas privados, lo que dificulta su acceso a la justicia. Por último, la experta Clara Marisela V. L. concluye que el sistema funciona ineficientemente por una carencia en la coordinación entre instituciones y ante la actuación aislada de diferentes actores, también se determina fallas en infraestructura como laboratorios periciales y la defensa nula de la justicia, ante la ciberdelincuencia

4.1.2.2 Análisis doctrinal.

El phishing se ha posicionado como una infracción que va más allá del delito técnico; se direcciona a la manipulación psicológica del sujeto pasivo. Según Alvaracín (2023), los agresores implementan técnicas de seducción en las plataformas digitales que inducen a la divulgación de información personal. Estos delitos han evolucionado desde foros hasta su perfeccionamiento actual, que obtuvo un gran impulso tras la pandemia por COVID-19 y la inteligencia artificial (Cano, 2021; Aguilar y Balseca, 2024). Autores como Pazmiño et al. (2024) y la Dirección de Ciberdelitos (2024) sugieren que el phishing ha trasmutado de mecanismos artesanales a métodos más amplios que utilizan la ingeniería social y sistemas automatizados, con el objetivo de maximizar su efectividad, a costa del error del ser humano, responsable del 95 % de las vulnerabilidades en la seguridad informática.

En Ecuador, la detección y prevención de este tipo de delitos afronta retos legales y operacionales. Solano et al. (2023); Juca y Medina (2023) señalan que la falta de coordinación entre organismos como la Fiscalía General del Estado y ARCOTEL, con una carencia de recursos tecnológicos, propicia actos de impunidad. A pesar de la adhesión de Ecuador a la Convención de Budapest en 2024, el Código Orgánico Integral Penal presenta importantes brechas normativas. León et al. (2024) y Flores et al. (2024) indican que el sistema de justicia toma el phishing como un delito tradicional, ejercicio impreciso, que no representa la naturaleza técnica del ilícito, lo que impacta al principio de legalidad.

Es por este motivo que se propone la toma de medidas que prevengan este tipo de actos delictivos con un enfoque estratégico y proactivo. Al analizar la percepción de la criminología de derechos humanos y la liberación, autores como Castro (2009) y Alvaracín (2023) consideran que la respuesta que se obtiene ante estos contextos no es punitiva, sino que solo se enfocan en la reducción de vulneraciones sociales que protegen la autonomía del ciudadano, frente al control algorítmico.

Morales (2025), junto con Campos et al. (2025), recalcan la necesidad de adaptar barreras técnicas y un asesoramiento digital que se contrapongan a factores como el analfabetismo que, en el país, afecta al 8,2% de la población. Autores como Camacho et al. (2024) recomiendan la aplicación de metodologías en enseñanza como la gamificación, que da las herramientas necesarias para que la ciudadanía vulnerable gestione el riesgo en el medio digital.

4.1.3 Interpretar la figura del phishing en el Código Orgánico Integral Penal, la ratificación del Ecuador al Convenio de Budapest y la casuística de la "Operación KAERB 2024".

4.1.3.1 Opiniones de agentes del sistema de justicia, seguridad e investigación especializados en delitos y antisociales cibernéticos.

4.1.3.1.1 Resúmenes de las entrevistas.

Entrevistado 1

En base a la realidad jurídica del país, la terminología phishing no se encuentra definida de forma clara; las sanciones de este tipo de actuaciones en el Código Orgánico Integral Penal se rigen por articulados convencionales, dentro de estos, se describe el artículo 190. El Tcnl. Carlos García indica que el Ecuador ha modificado su marco institucional, en base a la Convención de Budapest y a la Convención de Hanoi de las Naciones Unidas, que se enfocan en implementar figuras jurídicas técnicas, como los agentes digitales infiltrados. No obstante, la táctica con mayor eficiencia que contrarresta estos efectos se fundamenta en la prevención y la formación integral dentro del sistema educativo; debido a que es un área, en donde la ley no exime de responsabilidad a quienes cometen delitos como el acceso no autorizado a los sistemas electrónicos o el almacenamiento de datos sensibles.

Entrevistado 2

El criminólogo Jaime Guevara detalla que la vulnerabilidad al phishing en Ecuador empeora con el bajo nivel de conocimiento en el uso digital de plataformas e instrumentos tecnológicos y la carencia de familiaridad con la web. Razón por la cual las estrategias de prevención incluyen la capacitación de usuarios con campañas de sensibilización, que gesten herramientas de protección, así como la formación obligatoria desde los centros educativos para formar una cadena de protección. El mundo académico requiere la promoción de leyes y sanciones específicas que integren las técnicas de ciberdelincuencia en el sistema jurídico ecuatoriano.

Entrevistado 3

Para el Agente Fiscal Gustavo Casco, el phishing es descrito como una categoría jurídica de delitos tradicionales. Esta complejidad requiere de una formación especializada que actualmente no existe, situación que complica el desarrollo de investigaciones y la adopción de técnicas de detección. Como un mecanismo de prevención, se recalca la necesidad de concientizar a los ciudadanos sobre ciberseguridad, con el objetivo de disminuir la confianza en sitios web. Destaca la importancia de confirmar la autenticidad de correos electrónicos, actuar con precaución y no divulgar la información confidencial en dispositivos móviles. Un elemento significativo de la ciberdelincuencia es la analafabetización digital.

Entrevistado 4

La legislación actual de Ecuador no posee una figura jurídica exacta sobre ciberdelitos, por ende, carece de proporcionalidad en las sanciones tradicionales frente al daño que causa el cibercrimen. I.A.G.V., identifica el artículo 190, que penaliza ineficazmente al phishing como un delito complejo que afecta a la propiedad y otros bienes jurídicos. Asimismo, es importante que se actualice la legislación nacional respecto a los lineamientos de la Convención de las Naciones Unidas contra la Ciberdelincuencia y otras normas internacionales. Estos métodos promocionan una cultura que promueva la denuncia, sensibilice la opinión pública en seguridad informática para que la ciudadanía verifique la autenticidad de direcciones de correo electrónico, de esta manera se precisan las estrategias de prevención.

Entrevistado 5

Clara Marisela V. L. expone que la respuesta institucional no se limita a establecer sanciones en el Código Orgánico Integral Penal, sino que aplica un manejo integral de riesgos. El reforzamiento de la norma es un mecanismo eficaz en la sanción de infractores de delitos, pero sobre todo para las instituciones que, por negligencia u omisión, no establecen controles internos sólidos. Es así que considera pertinente la promoción de una cultura educativa ante este tipo de incidentes, que reduzcan el temor a la reputación y que se ajusten a políticas públicas, que se centren en la criminología moderna y la inteligencia

preventiva. Esto indica, que se debería adoptar monitoreos técnicos, que se alinean a una autentificación que todos los factores que existen, vigilando constantemente una reducción de dichos ataques.

4.1.3.1.2. Análisis de entrevistas a expertos.

El profundizar normas jurídicas en el Ecuador, permitió comprender que existe una tensión clave entre las normas vigentes y la naturaleza evolutiva del ciberdelincuente. Ante esto el Tcnl. Carlos García e I.A.G.V. afirma que la inexistencia de una descripción técnica sobre el phishing al considerarlo como un delito, hace que se clasifique en base una tipificación tradicional, que se alinea a pautas del artículo 190 del Código Orgánico Integral Penal. En base al criterio de I.A.G.V. dicha norma es insuficiente y desproporcionada; el phishing causa una vulneración profunda dentro de los derechos de la propiedad, que coincide con la percepción del Tcnl. Carlos García en la necesidad de aplicar una armonización de la legislación nacional con los instrumentos internacionales, como el Convenio de Budapest y la Convención de las Naciones Unidas contra la Ciberdelincuencia, estrategias que facilitan la introducción de instrumentos técnicos y promueven la implementación de figuras como los agentes infiltrados digitales, para fortalecer los procesos penales.

La viabilidad de las investigaciones se compromete por la ineficacia en la materia de competencias técnicas. Es por esto que el Agente Fiscal Gustavo Casco expresa que la complejidad de estos delitos necesita de especialistas que adquieran una instrucción clara en la materia. La idea que se comparte por medio del criminólogo Jaime Guevara sustenta que el mundo académico requiere de una evolución en la redacción de normas, cuya finalidad es abordar temas con alta complejidad de delitos digitales en comparación con medidas punitivas tradicionales. La especialista Clara Marisela V. L. propone un cambio de pensamiento que motive a los habitantes a gestionar el riesgo, con normas que sancionen no solo al infractor, sino también a las instituciones que, por negligencia en sus controles internos, facilitan la comisión del phishing.

Los expertos reafirman que la respuesta del Estado deja de ser reactiva y se convierte en proactiva. El Tcnl. Carlos García y el criminólogo Jaime Guevara destacan que la estrategia más poderosa ante este tipo de delito es la formación completa en sistemas educativos que favorezcan competencias digitales para reducir la fragilidad cognitiva de la población. Es necesario que se tomen decisiones que concienticen a la opinión social; que abarcan temarios que se vinculan a una práctica digital eficaz, así como a una comprobación del nombre del dominio, el accionar de mecanismos previos en enlaces que mantienen una apariencia sospechosa.

Clara Marisela V. L., persona con conocimiento en el área, indica que se mantiene una urgencia de la obtención de un control técnico de carácter obligatorio, que aplique una autentificación en múltiples factores, donde se promueva una implementación de una cultura automática, que sobrepase el daño. De todo esto, se describe la necesidad de que se aplique una defensa contra este tipo de ciberdelito en el país, ejerciendo un enfoque continuo que

abarca una modificación legal, competencias técnicas en ciberseguridad y una campaña de sociabilización.

4.1.2.3 Análisis doctrinal.

El ámbito jurídico del phishing en Ecuador refleja una debilidad estructural marcada dentro del Código Orgánico Integral Penal, como consecuencia de la omisión de una definición jurídica que contenga a este delito. Es por esto que para Ponce (2024), la existencia de estas brechas obliga a los diferentes agentes del sistema de justicia a recurrir a interpretaciones análogas, que son escasas, ante nuevos avances del mundo digital. En el día a día, el phishing se subdivide en otros delitos, depende de la forma de operación y medio en el cual se comete la acción. Vela (2023), Flores et al. (2024); Suárez y Ernesto (2024) subsumen este ciberdelito a los artículos 186, 290, 230, 234 y 234.1, que deslegitima al sistema jurídico-penal.

La ratificación del Ecuador al Convenio Budapest mediante el Decreto Ejecutivo N.º 332 supone un avance dentro de la modernización del sistema penal del país (Presidencia de la República, 2024). Autores como Coronel y Argüello (2025) mencionan que la adhesión armonizará las normas existentes en el país, promueve la cooperación internacional y recolecta pruebas rápidas. Iñiguez et al. (2025) consideran que la eficacia de este avance normativo va a depender de una modificación en el Código Orgánico Integral Penal y de la especialización del sistema judicial para hacer frente a tácticas delictivas cada vez más automatizadas y transnacionales.

4.1.2.4 Análisis normativo.

El enfoque legal del phishing en Ecuador no se limita a un punto de vista superficial, necesita de un análisis técnico sobre el comportamiento de los atacantes, con el fin de adecuarlo dentro de los preceptos del Código Orgánico Integral Penal. Para dar cumplimiento a lo expuesto, es importante diferenciar entre una fase preparatoria, donde el autor diseña un delito, y la fase de ejecución, que engloba procesos de materialización de daños a bienes jurídicos protegidos. Este panorama propone una interpretación de verbos reactores que permiten establecer una correlación entre el ejercicio técnico y el derecho penal vigente:

Tabla 3. *Interpretación del phishing en relación al articulado del COIP.*

ARTÍCULO	VERBO RECTOR	SÍNTESIS DEL ARTÍCULO	APLICACIÓN AL PHISHING
Art. 186.- Estafa	Inducir, defraudar, entregar, efectuar y emitir.	Una persona que, con el fin de obtener ganancias económicas, engaña a otros al fabricar información falsa.	El ciberdelincuente utiliza sitios web fraudulentos para manipular el consentimiento del usuario y engañarlo para que revele sus

			credenciales de inicio de sesión.
Art. 190.- Apropiación fraudulenta por medios electrónicos	Utilizar, facilitar, procurar, alterar, manipular, modificar, inutilizar, descubrir o descifrar y violentar.	Un delincuente que utiliza fraudulentamente un sistema para facilitar la transferencia no autorizada de bienes, al alterar o manipular redes.	Una vez obtenidas las claves, el ciberdelincuente utiliza programas o dispositivos para transferir los activos de la víctima sin su permiso.
Art. 230.- Interceptación ilegal de datos	Interceptar, escuchar, desviar, grabar, observar, diseñar, desarrollar, ejecutar, producir, programar, enviar, poseer, vender, distribuir, copiar, clonar y comercializar.	Un delincuente que crea, produce o envía ilegalmente páginas web, enlaces o ventanas emergentes engañosas.	Esta es la fase preparatoria: la amplia distribución de enlaces y el uso de herramientas digitales para clonar información y capturar flujos de datos.
Art. 234.- Acceso no consentido a un sistema informático, telemático o de telecomunicaciones	Acceder, mantener, modificar, desviar, redireccionar y ofrecer.	Un delincuente que, sin autorización, accede o permanece en un sistema informático contra la voluntad del propietario.	El ciberdelincuente redirige al usuario a sitios web falsos para obtener las claves y, una vez obtenidas, explota el acceso al sistema informático de la víctima.
Art. 234.1.- Falsificación informática	Provocar, introducir, modificar, eliminar, suprimir, interferir y usar.	Cualquier persona que, con intención de engañar, produzca datos o documentos falsificados o distribuya contenido digital falso.	La creación de correos electrónicos fraudulentos y la clonación de interfaces bancarias con intención de engañar constituyen este delito.

Nota: Elaborado por Salguero, S. (2026). Esta matriz se basa en el análisis normativo del Código Orgánico Integral Penal (2014) y en la adecuación del phishing dentro de las clasificaciones jurídicas tradicionales.

4.1.3.3 Análisis casuístico.

A partir del análisis de la Operación KAERB, se constató que el phishing no constituye un delito autónomo según la legislación ecuatoriana, sino que lo es el verbo rector "acceder", tal y como se define en el artículo 234 del Código Orgánico Integral Penal:

- La operación expone el acceso sin autorización previa de las personas afectadas, como meta final. El phishing es el medio por el cual se comete este delito.
- Este delito no solo afecta a bienes robados, debido a que incluye fases de invasión a sistemas electrónicos, que modifican la conducta delictiva, pasa de la vulneración patrimonial a la transgresión a la seguridad informática.

La Operación KAERB es una evidencia comprobada de la aplicación del Convenio de Budapest, pese a la reciente ratificación por parte de Ecuador.

- El servidor central "iServer", en Argentina, permitió ser el pilar de un núcleo que incluyó a seis países. Motivo por el cual es imprescindible la aplicación de los lineamientos del Convenio de Budapest sobre la asistencia jurídica mutua acelerada para frenar la transnacionalidad del ciberdelito.
- Sin la intervención de organismos como Europol y Ameripol, en el sistema judicial del país, solo sería factible el procesamiento penal por robo de dispositivos móviles, gracias a la cooperación internacional actualmente se logra judicializar los delitos digitales como mecanismos de desbloqueo y el acceso a carteras virtuales "Binance", sin embargo, los ciberdelitos aún requieren subsumirse a la norma tradicional.

La operación KAERB en Santo Domingo de los Tsáchilas proporcionó datos cuantificables y cualitativos sobre la complejidad de la ciberdelincuencia en Ecuador:

Tabla 4. *Sistematización de las pruebas digitales y físicas incautadas durante la Operación KAERB.*

PRUEBAS	CATEGORÍA	RELEVANCIA JURÍDICA
Equipos	921 dispositivos incautados	Prueba de la magnitud del delito.
Soporte de almacenamiento	11 discos duros y 30 memorias USB	Demuestra la existencia del software "iServer" y los registros de acceso.
Activos virtuales	Criptomonedas	Representa pérdidas económicas e incluso blanqueo de capitales.
Armas	Armas de fuego y municiones	Nexo entre la ciberdelincuencia y el crimen común organizado.

Nota: Elaborado por Salguero, S. (2026) respecto al Boletín de Prensa N.º 1048-DC-2024 de la Fiscalía General de la Nación, datos oficiales de la Policía Nacional del Ecuador y artículos de medios de comunicación certificados. La diversidad de las pruebas demuestra una convergencia de actividades delictivas que van más allá del ámbito meramente informático.

Los hallazgos del estudio de caso determinaron que la delincuencia digital en el país ha reformado los actos delictivos:

- Determina una estructura jerárquica, que era manipulada desde Argentina por medio de un “iServer”, mecanismo que fue operado por delincuentes en el país, quienes fueron detenidos.
- Demuestra que el phishing no parte de un error dentro del sistema, existe un ataque psicológico en usuarios, donde el agresor engaña a la víctima con el objetivo de adquirir credenciales bajo las promesas de recuperar sus dispositivos robados.

4.2 Discusión de resultados

Los hallazgos del presente estudio exponen que la ciberdelincuencia ha evolucionado; actualmente se consolida como un fenómeno delictivo sofisticado en el país, se representa como una asociación tecnoemocional, donde el atacante no necesita actuar de forma física (Cámara, 2021). Expertos como García sostienen que los ciberdelincuentes no necesitan una formación avanzada, solo requieren un acceso empírico a instrumentos digitales. Por su parte, Castillo (2021), Casco e I.A.G.V. argumentan que el perfil criminológico del ciberdelincuente especializado en phishing tiene como carácter fundamental el dominio técnico de sistemas tecnológicos que le garantiza un anonimato estratégico. Esta dualidad sugiere que el perfilamiento criminal del infractor en el ciberespacio oscila entre la simplicidad operativa y la alta especialización digital.

Con relación a la psiquis de los atacantes, se evidencia una tendencia crítica entre la práctica y la teoría. El entrevistado, I.A.G.V. expone rasgos psicopatológicos, como la falta de empatía y el trastorno antisocial de la personalidad, que se relaciona con la despersonalización de la víctima, en concordancia con Jativa et al. (2025). El ciberdelincuente carece de una conexión emocional con el sujeto pasivo amplificada por el cifrado de identidad (López, 2022), también reconoce el uso de técnicas de ingeniería social y factores psicológicos como el miedo y la urgencia que sirven como un mecanismo de manipulación (Clara Marisela V. L.). El modus operandi es un proceso de persuasión que explota la vulnerabilidad humana, al transformar un ataque aleatorio en una estrategia dirigida de alta rentabilidad y bajo riesgo para el atacante.

La cibervictimización expone una crisis de analfabetismo digital en Ecuador; García menciona que existe un porcentaje del 90% al 95%, patrón crítico que indica una mayor probabilidad de riesgo, tal como lo expone Montiel (2020). Es así como los resultados reflejan una segmentación marcada de víctimas, con mayor alcance a niños y adolescentes, resultado de la confianza excesiva y la dependencia de la tecnología actual (García). A esto, se suma el desconocimiento de la población adulta mayor sobre la veracidad de interfaces digitales (Casco). La asimetría tecnológica reafirma lo expuesto por Alvaracin (2023), quien destaca que el control social ha sido desplazado a un panóptico digital; la consecuencia es un incremento en comportamientos antisociales automáticos.

Un hallazgo relevante es la validación de la construcción de perfiles criminales como mecanismo de inferencia rigurosa. Márquez (2022) define este proceso mediante enfoques inductivos y deductivos, mientras Guevara expone que, en el entorno digital, se ejerce una escena de crimen que diferencia los modos de operación y firma de los agresores; el primero desarrolla y adapta la comisión de delitos, el segundo destaca las necesidades psicológicas del agresor y los rasgos de personalidad que ayudan a la persuasión de la víctima. Esta distinción es respaldada por la perspectiva de I.A.G.V. que clasifica a los ciberdelincuentes en organizados o desorganizados, gracias al análisis del trastorno de personalidad antisocial. Las huellas digitales no solo son un rastro técnico, sino que se consideran como una prueba conductual, que influyen positivamente en la reducción del número de sospechosos, tras reconstruir sus hábitos de contacto y sus patrones de comportamiento (Guevara).

En la actualidad existe una brecha crítica entre la evolución del phishing y la capacidad de respuesta del Estado ecuatoriano. Aunque García y Guevara coinciden en que la inteligencia artificial y la clonación de voz han transformado el phishing en un fenómeno extremadamente preciso y personalizado, la doctrina respalda este criterio y expone que la sofisticación refleja un cambio de paradigma que opera bajo engaños masivos, con el empleo de algoritmos maliciosos y deepfakes (Pazmiño et al., 2024). Este desarrollo, según Guevara, potencia la ciberdelincuencia en un 60 %, Cano (2021) aporta un criterio similar, donde se menciona que la ingeniería moderna explota sistemáticamente el error del ser humano, responsable del 95 % de las afectaciones en seguridad informática.

Desde el punto de vista jurídico, se revela un vacío normativo, que impacta al principio de legalidad. Casco e I.A.G.V. describen que la falta de una definición explícita del phishing en el Código Orgánico Integral Penal es el problema principal, motivo por el cual, los funcionarios del sistema de justicia, tratan estas infracciones como delitos generales. Este punto de vista es corroborado por León et al. (2024), que advierten sobre la impunidad que otorga la interpretación análoga de lesividades cibernéticas en figuras delictivas clásicas. Pese a que en el país, se ha establecido un apego por el Convención de Budapest, en el ejercicio, se evidencia que es nulo, evidenciando con un anonimato complicado y una naturaleza trasnacional del ciberdelito.

En este estudio, se han expuesto deficiencias en el funcionamiento y ejecución de procesos estatales, por otra parte, se evidencia, que existen bajas unidades especializadas en el país, encontrándose solamente en la ciudad de Quito, argumento que se reafirma con el criterio de (Casco) que expone la existencia de una limitación que se ajusta a la inexistencia de insumos tecnológicos. Este fallo de coordinación, sumado a las acciones aisladas de organismos como ARCOTEL y la Fiscalía General del Estado, citadas por Clara Marisela V. L., debilitan estructuralmente el sistema. En consecuencia, se comparte la opinión de Castro (2009) y Camacho (2024): la solución no se limita al castigo, requiere un enfoque proactivo, basado en la alfabetización digital y la especialización en informática forense, con el fin de reducir la vulnerabilidad de los ciudadanos en el ecosistema digital.

El delito estudiado en la investigación, demuestra un claro vacío entre los avances técnicos en ciberdelincuencia, y una vulneración por parte de la legislativa actual. Contexto, que ha sido refutado por (Ponce, 2024) y el experto I.A.G.V., autores que indican una existencia entre la falta de proporcionalidad. El phishing no solo impacta en el patrimonio, si no que además impacta en bienes jurídicos, en base a esto, se evidencia un discurso jurídico penal no legítimo, como consecuencia de una falta de precisión técnica.

En el país, se han tomado medidas que se sustentan en el Convenio de Budapest, el cual indica ser una norma decisiva en la trasmutación de todo el sistema institucional. Todos los hallazgos de la operación KAERB 2024 confirman una necesidad en este instrumento, donde se demuestra que este ciberdelito, funciona según un sistema, como un servicio, en donde los actores de la localidad, dependerán de como el país lo maneja, considerando además medidas internacionales. El criterio de García y Casco: expone al cumplimiento legal como una medida que no dependerá solo de una sanción de tipo penal, si no que deberán tomarse decisiones estatales, que se ajusten a una cooperación internacional, aplicando además estrategias y técnicas específicas, considerando aspectos a los cuales los agentes digitales se enfrentan día a día, relacionados a una volatidad de pruebas.

También se deberá considerar que existe una vulneración integral que no solo se asocia a lo tecnológico y digital, sino que también incluye una parte humanitaria y educativa. En contraste entre el enfoque punible y la gestión de riesgo, sustentado por la experta Clara Marisela V. L. que indica que la legislación, deberá modificarse para que puedan tomarse medidas de negligencia institucional cuando no se lleven a cabo controles internos. La afinidad de opiniones, entre Guevara y Casco fomenta que, aunque se ha actualizado la norma del Código Orgánico Integral Penal, las medidas generales, dan mayor prioridad a sanciones más que a una respuesta preventiva. Esto hace que el éxito de las operaciones com KAERB sea obtenido por medio de un asesoramiento en ciberseguridad que elimine o reduzca la frecuencia de ciberataques.

Por último, la implementación sistemática de la Operación KAERB demuestra que la ciberdelincuencia en Ecuador ha evolucionado hacia un sistema piramidal en el que la delincuencia converge con tecnologías de la información altamente complejas. Esta observación detalla la urgente necesidad de una reforma integral de la normativa, para reconocer al phishing como un delito distinto o se definan sus términos técnicos con mayor rigor. En conclusión, la lucha contra este ciberdelito en el país se basa en tres pilares afirmados por Clara Marisela V. L: la armonización legislativa internacional, la especialización técnica de los expertos y una sólida alfabetización digital de la población

CAPÍTULO V. CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

A partir del análisis de la cibercriminología y de los elementos del perfilado criminal, se infiere que los ciberdelincuentes especializados en phishing en Ecuador no actúan de forma impulsiva, sino que siguen un enfoque planificado que combina curiosidad empírica y conocimientos técnicos. Los resultados demuestran que los autores de estos ataques utilizan la ingeniería social como su principal arma, al explotar los mecanismos psicológicos de urgencia, con ello, se ha logrado identificar un patrón recurrente: la despersonalización de la víctima y la ausencia total de empatía, facilitadas por el anonimato digital. Esta caracterización teórica es crucial, permite al sistema institucional distinguir a los delincuentes oportunistas de las redes organizadas y optimizar el uso de recursos periciales del país.

Según la información recopilada, se detectó una brecha crítica entre la creciente sofisticación del phishing amplificada por la inteligencia artificial y la falta de respuesta institucional de Ecuador. La centralización de entes especializados como la: "Unidad Nacional de Ciberdelitos de la Policía Nacional del Ecuador" y "Unidad Nacional Especializada en Investigación de Ciberdelitos de la Fiscalía General del Estado de Ecuador", en conjunto con la ausencia de laboratorios forenses descentralizados constituyen una falla estructural que garantiza el éxito de los ciberdelincuentes, esta limitación institucional, se ve agravada por la falta de competencias digitales de la población. Por lo tanto, un enfoque preventivo resulta indispensable y constituye la única estrategia viable, es decir, sin una cultura de seguridad digital y una fuerza operativa distribuida por todo el territorio, el Estado es incapaz de competir con la rapidez de ejecución y la automatización de los ataques de phishing.

En última instancia, la indagación de la "Operación KAERB 2024" y de la normativa vigente demuestra que la falta de una definición precisa del phishing en el Código Orgánico Integral Penal constituye una laguna institucional, que se subsana mediante la elaboración de perfiles criminales, herramienta estratégica que ayuda a comprender los comportamientos atípicos del ciberdelincuente, por consiguiente, la fenomenología del phishing se adecua a verbos rectores de delitos tradicionales. Sin una metodología de elaboración de perfilados criminales, cualquier normativa o ratificación internacional sería una mera formalidad sin aplicación práctica. La Operación KAERB 2024 ha demostrado que la simple incautación de material no garantiza la justicia; la clave está en el análisis del comportamiento delictivo, que permite identificar al autor del delito, la distribución de roles y jerarquías. Al integrar la dimensión humana con los datos digitales, se logra desmantelar la ciberdelincuencia local y transnacional.

5.2.Recomendaciones

Es imprescindible que el Ministerio del Interior y la Fiscalía General del Estado implementen una reestructuración operativa que rompa con la centralización de unidades

especializadas, la descentralización de entes compuestos por personal con experticia en análisis conductual delictual, es la única forma de corregir la falla estructural que garantiza la impunidad y ventaja táctica de los ciberdelincuentes.

Se sugiere que el Ministerio de Educación, en coordinación con los organismos reguladores de la ciberseguridad, convierta la alfabetización digital en un pilar de seguridad nacional y prevención primaria del phishing. El Estado elabora programas de formación obligatorios que vayan más allá del simple uso de herramientas tecnológicas, y se centren en la identificación de mecanismos de ingeniería social y técnicas usadas por los ciberdelincuentes.

Es necesario que el Estado ecuatoriano no observe las adhesiones a convenios internacionales como un mero marco legal y comience a utilizarlas como una plataforma para el intercambio de información transnacional sobre comportamientos delictivos cibernéticos, esto fomenta la creación de una base de datos de firmas criminales, en relación al análisis de comportamientos detectados durante operaciones como la KAERB 2024.

BIBLIOGRÁFIA

Aguilar, P., & Balseca, J. (2024). Tendencias, Desafíos y Vulnerabilidades de los Ataques Cibernéticos en Ambientes de Desarrollo. Revisión Sistemática. *Estudios y Perspectivas_Revista científica y académica*. Obtenido de https://doi.org/10.61384/r.c.a..v4i4.689

Aldaz, Á. (2023). Metodología para redactar un proyecto de investigación en la ciencia del derecho. *FIPCAEC_Revista Científica: Ciencias económicas y empresariales* . doi:https://doi.org/10.23857/fipcaec.v8i2

Arciniegas, M., Vargas, G., Triana, C., & Bello, G. (2022). Caracterización del hurto callejero: Modalidades y Técnicas. Modelo formativo para la Policía Nacional de Colombia. *Dialnet*. Obtenido de https://dialnet.unirioja.es/descarga/articulo/8910700.pdf

Asamblea Nacional. (2014). Código Orgánico Integral Penal. *Ediciones Leales*. Obtenido de https://biblioteca.defensoria.gob.ec/bitstream/37000/3817/15/COIP.%20%20C%c3%b3digo%20Org%c3%a1nico%20Integral%20Penal.%20S%c3%a9ptimo%20Suplemento.%20Actualizado.pdf

Benavides, E., Fuertes, W., Sanchez, S., & Nuñez, D. (2020). Caracterización de los ataques de phishing y técnicas para mitigarlos. Ataques: una revisión sistemática de la literatura. *Revista Ciencia y Tecnología, 13*(1). doi:https://doi.org/10.18779/cyt.v13i1.357

Camacho, A., Erazo, M., Salazar, C., & Pardo, B. (2024). Ingeniería Social: Revisión Sistemática de Phishing y. *Revista Ibérica de Sistemas e Tecnologias de Informação*. Obtenido de https://www.proquest.com/openview/1fd16ad18f6a54aad742c130b2fcf230/1?pq-origsite=gscholar&cbl=1006393

Camacho, G. (2023). Criminología forense: concepto y aplicaciones en el sistema de justicia penal. *Dialnet*. Obtenido de https://dialnet.unirioja.es/servlet/articulo?codigo=8336322

Cámara, S. (2020). Estudios criminológicos contemporáneos (IX): La Cibercriminología y el perfil del ciberdelincuente. *Dialnet*. Obtenido de https://dialnet.unirioja.es/servlet/articulo?codigo=7524987

Campos, M., Moreno, R., & Jiménez, B. (2025). Detección de fraudes y estafas basadas en ingeniería social en Ecuador. *REVISTA INVECOM "Estudios transdisciplinarios en comunicación y sociedad", 4*(3). Obtenido de https://revistainvecom.org/index.php/invecom/article/view/3551/700

Cano, C. (2021). Evolución e impacto del Phishing y como combatirlo. *Universitat Oberta de Catalunya (UOC)*. Obtenido de https://hdl.handle.net/10609/133755

Castillo, Ó. (2021). Phishing: Día de pesca. *Universidad Externado de Colombia*. Obtenido de https://bdigital.uexternado.edu.co/server/api/core/bitstreams/e8eac144-41c1-4efe-a7a8-85d8f4f93097/content

Ceballos, F. (2021). De la criminología clásica a la criminología moderna: La investigación criminal multifactorial en la era digital - De la Criminología Clásica. *Formación y Desarrollo Policial*. Obtenido de https://www.aacademica.org/fceballose/22/1.pdf

Celis, D. (2024). La investigación dogmática en el derecho: un análisis reconstructivo sobre el quehacer académico de los juristas. *Revista de la Facultad de Derecho y Ciencias Políticas*. Obtenido de https://revistas.upb.edu.co/index.php/derecho/article/view/8331/7372

Colegio Profesional de la Criminología de la Comunidad de Madrid. (2025). Papeles de Criminologí. *Revista del Colegio Profesional de la Criminología de la Comunidad de Madrid*(7). Obtenido de https://colegiocriminologosmadrid.es/wp-content/uploads/PdC_7_Julio2025.pdf

Conforme , J., & Vela, N. (2023). El phishing como ciberdelito y su conducta típica diferenciada de otros delitos informáticos en el Ecuador. *Universidad Espiritu Santo*. Obtenido de http://201.159.223.2/bitstream/123456789/3893/1/CONFORME%20OJEDA%20-%20VELA%20ANDRADE.pdf

Consejo de Europa. (2001). Convenio sobre la Ciberseguridad . *OAS*. Obtenido de https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

Coronel, J., & Argüello, E. (2025). Análisis forense digital: La eficacia de la legislación ecuatoriana ante el cibercrimen. *Polo del Conocimiento* . doi:10.23857/pc.v10i11.10748

Díaz, G., Molina , A., Serrador , L., & Cárdenas, J. (2023). Aproximación al ciberdelincuente desde la perspectiva del control social. *Revista Criminalidad* . Obtenido de https://doi.org/10.47741/17943108.508

Díaz, S. (2020). Desarrollo de sistema de análisis automático de phishing. *Repositorio Institucional UAM_Universidad Autónoma de Madrid*. Obtenido de https://repositorio.uam.es/server/api/core/bitstreams/7061c94f-0596-4c2b-abe8-c9265386ede2/content

Dirección de ciberdelitos_Ministerio del Interior. (2024). Boletín de Análisis de la Ciberdelincuencia: "La nueva era de la ciberdelincuencia, el lado oscuro de la Inteligencia Artificial". *Ministerio del Interior*. Obtenido de https://www.ministeriodelinterior.gob.ec/wp-content/uploads/downloads/2025/07/Boletin-La-nueva-era-de-la-ciberdelincuencia-el-lado-oscuro-de-la-Inteligencia-Artificial.pdf

El Diario. (2024). *Operativo internacional logra desarticular una red criminal*. Obtenido de https://www.eldiario.ec/sin-categoria/operativo-internacional-logra-desarticular-una-red-criminal-19092024/

El Phishing. (s.f.). *Grupo Smartekh*. Obtenido de https://blog.smartekh.com/hubfs/Grupo_Smartekh_PDF/El%20Phishing.pdf

Fiscalía General del Estado. (2021). Ciberdelitos: Perfil criminologíco . *Revista Científica de Ciencias Jurídicas, Criminología y Seguridad*. Obtenido de https://www.fiscalia.gob.ec/pdf/politica-criminal/Ciberdelitos-Perfil-Criminologico.pdf

Fiscalía General del Estado. (2024). *Boletín de Prensa FGE Nº 1048-DC-2024*. Obtenido de Operación KAERB: red criminal internacional dedicada a delitos cibernéticos es desarticulada con la participación de fiscalías y policías de 6 países: https://www.fiscalia.gob.ec/accesibilidad/operacion-kaerb-red-criminal-

internacional-dedicada-a-delitos-ciberneticos-es-desarticulada-con-la-participacion-de-fiscalias-y-policias-de-6-paises/

Flores, L., Carrión, K., & Rivera, J. (2024). Fundamentos jurídicos para la inclusión del delito de phishing en el código penal ecuatoriano. *Revista Dilemas Contemporáneos: Educación, Política y Valores*. Obtenido de https://dilemascontemporaneoseducacionpoliticayvalores.com/index.php/dilemas/article/view/4515/4347

García, J. (2024). La criminología y cibercriminología, en la investigación criminal. *Constructos Criminologícos: Revista Internacional de Investigación en criminología* . Obtenido de https://constructoscriminologicos.uanl.mx/index.php/cc/article/view/98/69

Gutiérrez, E., Urueña, R., & Rojas, J. (2025). Análisis de los Delitos Cibernéticos en el Ámbito de los Videojuegos, Metaverso y Estrategias para Mejorar la Gestión de Incidentes Cibernéticos en la Policía Nacional. *Ciencia Latina Revista Científica Multidisciplinar*. doi:https://doi.org/10.37811/cl_rcm.v9i3.18675

Iñiguez, J., Méndez, C., Mafla, J., & Puetate, J. (2025). Análi-sis de ratificación del Convenio de Budapest y su impacto en delitos informáticos en Ecuador. *Revista UGC*. Obtenido de https://universidadugc.edu.mx/ojs/index.php/rugc/article/view/188/181

Jativa, S., Hernández, H., Rojas, N., Villalta, J., & Palacios, S. (2025). Criminología del Siglo XXI: delincuencia, perfiles criminales y nuevos desafíos globales. *Editorial Tecnocientífica Americana_ETECAM*. Obtenido de https://etecam.com/index.php/etecam/article/view/91/112

Juca, F., & Medina, R. (2023). Ciberdelitos en Ecuador y su impacto social; panorama actual y. *Revista científica Portal de la Ciencia*. Obtenido de https://doi.org/10.51247/pdlc.v4i3.394

La Hora. (2024). *En Santo Domingo se detuvieron a dos personas por ciberdelitos*. Obtenido de https://www.lahora.com.ec/santodomingo/En-Santo-Domingo-se-detuvieron-a-dos-personas-por-ciberdelitos-20240919-0064.html

León, L., Olmedo, A., & Durán, A. (2024). Los delitos informáticos en el COIP y su actualización frente a nuevas formas de ciberdelitos. *Revista Ciencias Holguín*. Obtenido de http://www.ciencias.holguin.cu/revista/article/view/443/360

López, J. (2022). Sobre el alcance de los fines de la pena en el fenómeno criminal de la ciberdelincuencia. *Revista Chilena de Derecho y Tecnología*. Obtenido de https://rchdt.uchile.cl/index.php/RCHDT/article/view/60913/70904

Márquez, D. (2022). El uso del perfil criminológico en la investigación penal. *Revista UBA*. Obtenido de https://revistasuba.com/index.php/UBAIUS/article/view/309/682

Ministerio de Telecomunicaciones y Sociedad de la Información. (2022). Estrategia Nacional de Ciberseguridad del Ecuador . *ASOBANCA* . Obtenido de https://asobanca.org.ec/wp-content/uploads/2022/08/ESTRATEGIA-NACIONAL-DE-CIBERSEGURIDAD-DEL-ECUADOR-2022481.pdf

Morales, O. (2025). Ciberfraude: Principales Métodos de Ataque y Estrategias para su Prevención. *Ciencia Latina Revista Multidisciplinar, 9*(3). Obtenido de https://ciencialatina.org/index.php/cienciala/article/view/18122/26007

Organización Internacional de Policía Criminal. (s.f.). *Fraudes basados en la ingeniería social*. Obtenido de INTERPOL : https://www.interpol.int/es/Delitos/Delincuencia-financiera/Fraudes-basados-en-la-ingenieria-social

Pazmiño, J., Saavedra, M., & Yulan, L. (2024). Análisis de la efectividad de phishingautomático. *Revista Élite, 6*(2). Obtenido de https://www.revistaelite.itsqmet.edu.ec/index.php/elite/article/view/88/207

Policía Nacional del Ecuador . (2024). *Policía desarticula red internacional de ciberdelincuentes en Ecuador*. Obtenido de Comunicamos Noticias : https://noticias.policia.gob.ec/policia-desarticula-red-internacional-de-ciberdelincuentes-en-ecuador/

Ponce, M. (2024). Delitos informáticos: Caso Ecuador. *Revista San Gregorio*. Obtenido de https://revista.sangregorio.edu.ec/index.php/REVISTASANGREGORIO/article/view/2667/1665

Presidencia de la República del Ecuador . (2024). Decreto Ejecutivo N°332. *Strapi Lexis*. Obtenido de https://strapi.lexis.com.ec/uploads/DE_332_20240612145331_1_6683002cc1.pdf

Primicias . (2024). *Desarticulan red internacional de delitos informáticos con conexiones en Ecuador*. Obtenido de Sucesos : https://www.primicias.ec/sucesos/detenidos-ciberdelitos-criptomonenas-ecuador-operativo-kaerb-79187/

Punín, P. (2021). Breve aproximación a la ciberdelincuencia desde una perspectiva criminológica. *Revista Ruptura de la Asociación Escuela de Derecho PUCE.* Obtenido de http://www.revistaruptura.com/index.php/ruptura/article/view/85/40

Sánchez, S. (2021). Perfiles del ciberdelito: un campo de estudio inexplorado. *Central American Journals Online_Revista de Derecho*(30). Obtenido de https://camjol.info/index.php/DERECHO/article/view/12223/14276

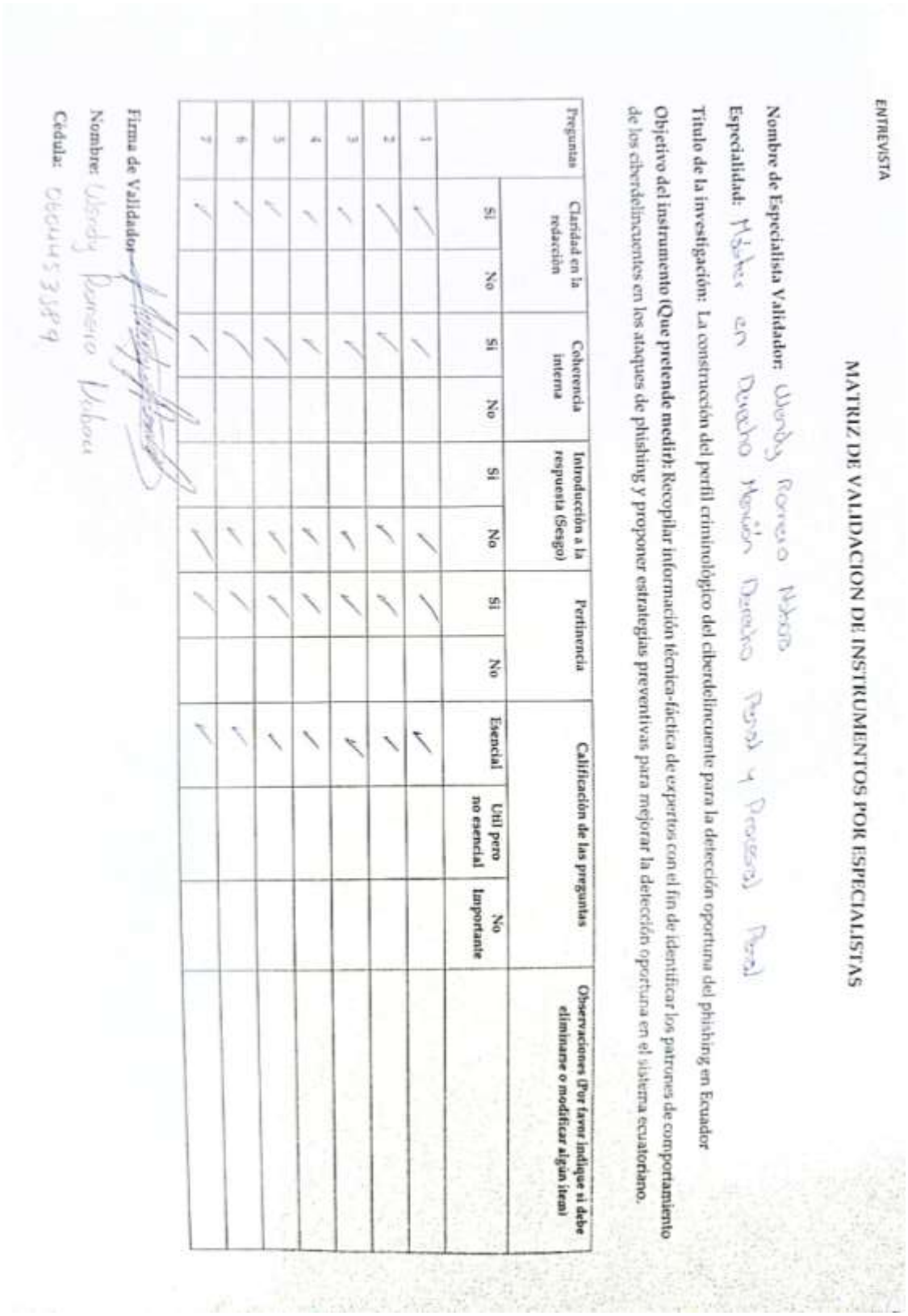
Solano, G., Quintero, N., Cedeño, L., & Eras, S. (2023). Análisis de datos y tendencias emergentes en delitos informáticos en redes sociales en Ecuador. *Polo del Conocimiento, 8*(5). doi:10.23857/pc.v8i5

Suárez , D., & Ernesto , R. (2024). El phishing como delito informático en el ámbito de las legislaciones de Ecuador, Argentina y España, 2023. *Repositorio Universidad Estatal Península de Santa Elena*. Obtenido de https://repositorio.upse.edu.ec/server/api/core/bitstreams/8c5c5bc2-1eca-4ea2-92fd-16987b14062c/content

Torres, A., Contreras, B., & Garrós , I. (2021). Análisis criminológico, técnico y legal del phishing. *Revista Aranzadi Doctrinal*(9). Obtenido de https://dsp.interior.gencat.cat/bitstream/handle/20.500.14007/5470/An%c3%a1lisis%20criminol%c3%b3gico%2c%20t%c3%a9cnico%20y%20legal%20del%20phishing.PDF?sequence=1&isAllowed=y

ANEXOS

Anexo 1. *Matrices de validación del instrumento "Guía de entrevistas" para la aplicación a expertos. Elaborado por Salguero, S (2026).*



ENTREVISTA

MATRIZ DE VALIDACION DE INSTRUMENTOS POR ESPECIALISTAS

Nombre de Especialista Validador: Wendy Romero Ribeiro

Especialidad: Máster en Derecho Penal y Procesal Penal

Título de la investigación: La construcción del perfil criminológico del ciberdelincuente para la detección oportuna del phishing en Ecuador

Objetivo del instrumento (Que pretende medir): Recopilar información técnica-fáctica de expertos con el fin de identificar los patrones de comportamiento de los ciberdelincuentes en los ataques de phishing y proponer estrategias preventivas para mejorar la detección oportuna en el sistema ecuatoriano.

Preguntas	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 ítem)
	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: Wendy Romero Ribeiro

Cédula: 0604453989

ENTREVISTA

MATRIZ DE VALIDACION DE INSTRUMENTOS POR ESPECIALISTAS

Nombre de Especialista Validador: Mag. Nelson Freire

Especialidad: Máster en Derecho Penal y Criminología

Titulo de la investigación: La construcción del perfil criminológico del ciberdelincuente para la detección oportuna del phishing en Ecuador

Objetivo del instrumento (Que pretende medir): Recopilar información técnica-fáctica de expertos con el fin de identificar los patrones de comportamiento de los ciberdelincuentes en los ataques de phishing y proponer estrategias preventivas para mejorar la detección oportuna en el sistema ecuatoriano.

Preguntas	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)
	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: Mag. Nelson Freire

Cèdula: 0602463491

ENTREVISTA

MATRIZ DE VALIDACION DE INSTRUMENTOS POR ESPECIALISTAS

Nombre de Especialista Validador: Adrián Alvarado Jarrín

Especialidad: Derecho Penal y Criminología

Titulo de la investigación: La construcción del perfil criminológico del ciberdelincuente para la detección oportuna del phishing en Ecuador

Objetivo del instrumento (Que pretende medir): Recopilar información técnica-fáctica de expertos con el fin de identificar los patrones de comportamiento de los ciberdelincuentes en los ataques de phishing y proponer estrategias preventivas para mejorar la detección oportuna en el sistema ecuatoriano.

Preguntas	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 ítem)
	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: Adrián Alvarado Jarrín

Cèdula: 0604031375

Anexo 2. *Guía de entrevistas y consentimiento informado. Elaborado por Salguero, S (2026).*

UNIVERSIDAD NACIONAL DE CHIMBORAZO
FACULTAD DE CIENCIAS POLÍTICAS Y ADMINISTRATIVAS
CARRERA DE DERECHO

GUÍA DE ENTREVISTA

Objetivo: Recopilar información técnica-fáctica de expertos con el fin de identificar los patrones de comportamiento de los ciberdelincuentes en los ataques de phishing y proponer estrategias preventivas para mejorar la detección oportuna en el sistema ecuatoriano.
Introducción: Esta entrevista tiene como objetivo recopilar información para la elaboración de la tesis previa a la obtención del título de Abogada de los Tribunales del Ecuador con la temática "La construcción del perfil criminológico del ciberdelincuente para la detección oportuna del phishing en Ecuador".
Datos sociodemográficos

- **Nombre completo**:
- **Formación académica**:
- **Años de experiencia profesional**:
- **Área de especialización**:
- **Institución u organización donde labora actualmente**:
- **Cargo o función que desempeña**:

Preguntas:

1. ¿Cuáles considera que son los patrones de comportamiento recurrentes y los factores criminógenos esenciales que caracterizan a los ciberdelincuentes especializados en phishing?
2. ¿Qué oportunidades aprovechan los ciberdelincuentes para ejecutar con éxito sus ataques de phishing en Ecuador?
3. ¿Cómo aportaría el análisis del perfil criminológico del ciberdelincuente en el entendimiento del delito de phishing en el Ecuador?
4. Según su experiencia, ¿cuáles considera que son los efectos más comunes del phishing en las cibervíctimas de Ecuador y qué factores las han convertido en sujetos vulnerables a este tipo de ciberdelito?
5. ¿Ha notado un incremento en la sofisticación de los ataques de phishing en Ecuador?
6. ¿Considera que existen limitaciones operativas-legales obstaculizan la capacidad de responder eficazmente al phishing y como se traducen en una ventaja para los ciberdelincuentes?
7. Desde su experiencia y conocimiento, ¿cuáles serían las estrategias para prevenir el delito de phishing?

CONSENTIMIENTO INFORMADO
UNIVERSIDAD NACIONAL DE CHIMBORAZO – CARRERA DE DERECHO

Proyecto de investigación: La construcción del perfil criminológico del ciberdelincuente para la detección oportuna del phishing en Ecuador.
Investigadora: Sandy Solange Salguero Muñoz
CONSENTIMIENTO INFORMADO PARA PARTICIPANTES
Le invito a participar en esta entrevista semiestructurada como experto/a en el marco de un proyecto de investigación universitaria.
El objetivo es recopilar sus conocimientos técnicos y empíricos sobre los rasgos y métodos operativos de los ciberdelincuentes, ataques de phishing, el marco institucional y jurídico, así como la viabilidad de establecer el perfil criminológico como herramienta elemental para la detección oportuna del phishing.

Al participar, usted acepta las siguientes condiciones:

- La entrevista, se grabará exclusivamente con fines de transcripción y análisis.
- Se tomará una fotografía al inicio o al final de la entrevista con el fin de documentar el uso de la herramienta.

Se colocará la fotografía con su rostro al descubierto.	
Se colocará la fotografía con su rostro tapado.	

- Toda la información, se tratará con la máxima confidencialidad, su identificación:

Se citará con su nombre completo y el cargo institucional.	
Se citará únicamente el cargo institucional.	
Se citará sus iniciales y el cargo institucional.	
Se citará únicamente sus iniciales	

- Los datos recopilados, se utilizarán exclusivamente para la investigación y el desarrollo de la tesis.

Su participación es voluntaria, tiene derecho a negarse a responder determinadas preguntas o a interrumpir la entrevista en cualquier momento, sin tener que dar ninguna explicación.

Nombre del entrevistado:
Firma:
Fecha:

Anexo 3. *Fotografías con los expertos entrevistados. Elaborado por Salguero, S (2026).*

Entrevistado 1: Tcnl. Carlos García (Jefe de la Unidad Nacional de Ciberdelitos de la Policía Nacional del Ecuador).

- Fotografía

Entrevistado 2: Jaime Alfonso Guevara Pintado_ Perito Acreditado por el Consejo de la Judicatura (criminólogo).

- Fotografía

Entrevistado 3: Gustavo Fernando Casco Lozada_ Agente Fiscal.

- Fotografía

Entrevistado 4: I.A.G.V_ Presidente de la Corte Provincial de Justicia de Tungurahua.

- Fotografía

Entrevistado 5: Clara Marisela V.L_ Abogada e ingeniería en sistemas con maestría en ciberseguridad.

- Fotografía

Anexo 4. ***C****onsentimiento informado firmado por los expertos. Elaborado por Salguero, S (2026).*

Entrevistado 1: Tcnl. Carlos García (Jefe de la Unidad Nacional de Ciberdelitos de la Policía Nacional del Ecuador).

- Consentimiento informado

CONSENTIMIENTO INFORMADO

UNIVERSIDAD NACIONAL DE CHIMBORAZO – CARRERA DE DERECHO

Proyecto de investigación: La construcción del perfil criminológico del ciberdelincuente para la detección oportuna del phishing en Ecuador.

Investigadora: Sandy Solange Salguero Muñoz

CONSENTIMIENTO INFORMADO PARA PARTICIPANTES

Le invito a participar en esta entrevista semiestructurada como experto/a en el marco de un proyecto de investigación universitaria.

El objetivo es recopilar sus conocimientos técnicos y empíricos sobre los rasgos y métodos operativos de los ciberdelincuentes, ataques de phishing, el marco institucional y jurídico, así como la viabilidad de establecer el perfil criminológico como herramienta elemental para la detección oportuna del phishing.

Al participar, usted acepta las siguientes condiciones:

- La entrevista se grabará exclusivamente con fines de transcripción y análisis.
- Se tomará una fotografía al inicio o al final de la entrevista con el fin de documentar el uso de la herramienta. *(Seleccione con una X)*

Se colocará la fotografía con su rostro al descubierto.	x
Se colocará la fotografía con su rostro tapado.	

- Toda la información se tratará con la máxima confidencialidad *(Seleccione con una X)*:

Se citará con su nombre completo y el cargo institucional.	x
Se citará únicamente el cargo institucional.	
Se citará usando sus iniciales y el cargo institucional.	

Se citará únicamente sus iniciales	

- Los datos recopilados se utilizarán exclusivamente para la investigación y el desarrollo de la tesis.

Su participación es voluntaria, tiene derecho a negarse a responder determinadas preguntas o a interrumpir la entrevista en cualquier momento, sin tener que dar ninguna explicación.

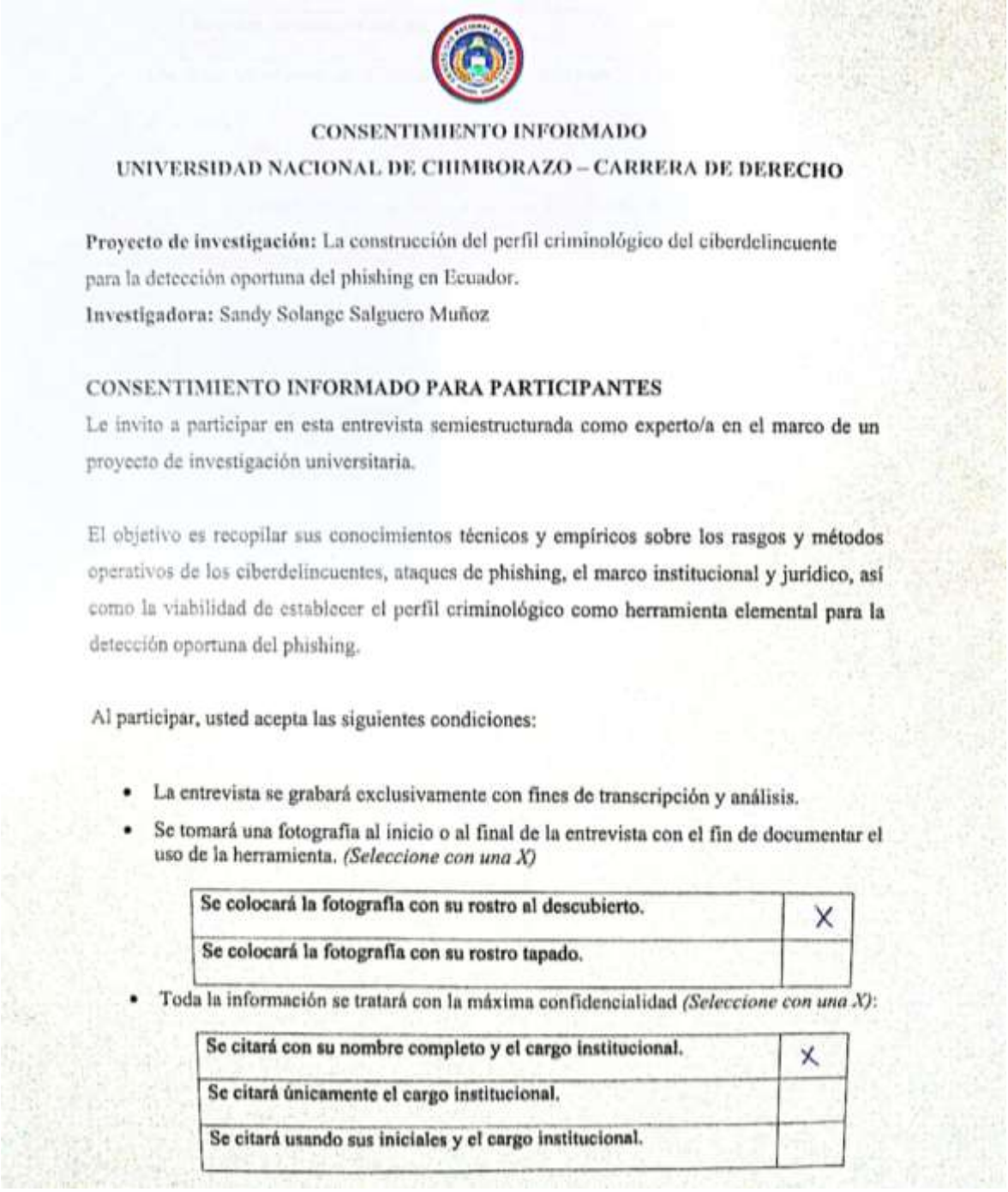
Nombre del entrevistado: TCNL. HÉCTOR GONZALO GARCÍA CATAÑA

Firma: 

Fecha: 29/12/2025

Entrevistado 2: Jaime Alfonso Guevara Pintado_ Perito Acreditado por el Consejo de la Judicatura (criminólogo).

- Consentimiento informado



CONSENTIMIENTO INFORMADO

UNIVERSIDAD NACIONAL DE CHIMBORAZO – CARRERA DE DERECHO

Proyecto de investigación: La construcción del perfil criminológico del ciberdelincuente para la detección oportuna del phishing en Ecuador.

Investigadora: Sandy Solange Salguero Muñoz

CONSENTIMIENTO INFORMADO PARA PARTICIPANTES

Le invito a participar en esta entrevista semiestructurada como experto/a en el marco de un proyecto de investigación universitaria.

El objetivo es recopilar sus conocimientos técnicos y empíricos sobre los rasgos y métodos operativos de los ciberdelincuentes, ataques de phishing, el marco institucional y jurídico, así como la viabilidad de establecer el perfil criminológico como herramienta elemental para la detección oportuna del phishing.

Al participar, usted acepta las siguientes condiciones:

- La entrevista se grabará exclusivamente con fines de transcripción y análisis.
- Se tomará una fotografía al inicio o al final de la entrevista con el fin de documentar el uso de la herramienta. *(Seleccione con una X)*

Se colocará la fotografía con su rostro al descubierto.	X
Se colocará la fotografía con su rostro tapado.	

- Toda la información se tratará con la máxima confidencialidad *(Seleccione con una X)*:

Se citará con su nombre completo y el cargo institucional.	X
Se citará únicamente el cargo institucional.	
Se citará usando sus iniciales y el cargo institucional.	

Se citará únicamente sus iniciales	

- Los datos recopilados se utilizarán exclusivamente para la investigación y el desarrollo de la tesis.

Su participación es voluntaria, tiene derecho a negarse a responder determinadas preguntas o a interrumpir la entrevista en cualquier momento, sin tener que dar ninguna explicación.

Nombre del entrevistado:

Firma:

Fecha: 16-01-2026

Entrevistado 3: Gustavo Fernando Casco Lozada_ Agente Fiscal.

- Consentimiento informado

CONSENTIMIENTO INFORMADO

UNIVERSIDAD NACIONAL DE CHIMBORAZO – CARRERA DE DERECHO

Proyecto de investigación: La construcción del perfil criminológico del ciberdelincuente para la detección oportuna del phishing en Ecuador.
Investigadora: Sandy Solange Salguero Muñoz

CONSENTIMIENTO INFORMADO PARA PARTICIPANTES

Le invito a participar en esta entrevista semiestructurada como experto/a en el marco de un proyecto de investigación universitaria.

El objetivo es recopilar sus conocimientos técnicos y empíricos sobre los rasgos y métodos operativos de los ciberdelincuentes, ataques de phishing, el marco institucional y jurídico, así como la viabilidad de establecer el perfil criminológico como herramienta elemental para la detección oportuna del phishing.

Al participar, usted acepta las siguientes condiciones:

- La entrevista se grabará exclusivamente con fines de transcripción y análisis.
- Se tomará una fotografía al inicio o al final de la entrevista con el fin de documentar el uso de la herramienta. *(Seleccione con una X)*

Se colocará la fotografía con su rostro al descubierto.	X
Se colocará la fotografía con su rostro tapado.	

- Toda la información se tratará con la máxima confidencialidad *(Seleccione con una X)*:

Se citará con su nombre completo y el cargo institucional.	X
Se citará únicamente el cargo institucional.	
Se citará usando sus iniciales y el cargo institucional.	

Se citará únicamente sus iniciales	

- Los datos recopilados se utilizarán exclusivamente para la investigación y el desarrollo de la tesis.

Su participación es voluntaria, tiene derecho a negarse a responder determinadas preguntas o a interrumpir la entrevista en cualquier momento, sin tener que dar ninguna explicación.

Nombre del entrevistado: Dr. Fernando Cabon.

Firma:

Fecha: 14 de Enero / 2026

Entrevistado 4: I.A.G.V_ Presidente de la Corte Provincial de Justicia de Tungurahua.

- Consentimiento informado

CONSENTIMIENTO INFORMADO

UNIVERSIDAD NACIONAL DE CHIMBORAZO – CARRERA DE DERECHO

Proyecto de investigación: La construcción del perfil criminológico del ciberdelincuente para la detección oportuna del phishing en Ecuador.

Investigadora: Sandy Solange Salguero Muñoz

CONSENTIMIENTO INFORMADO PARA PARTICIPANTES

Le invito a participar en esta entrevista semiestructurada como experto/a en el marco de un proyecto de investigación universitaria.

El objetivo es recopilar sus conocimientos técnicos y empíricos sobre los rasgos y métodos operativos de los ciberdelincuentes, ataques de phishing, el marco institucional y jurídico, así como la viabilidad de establecer el perfil criminológico como herramienta elemental para la detección oportuna del phishing.

Al participar, usted acepta las siguientes condiciones:

- La entrevista se grabará exclusivamente con fines de transcripción y análisis.
- Se tomará una fotografía al inicio o al final de la entrevista con el fin de documentar el uso de la herramienta. *(Seleccione con una X)*

Se colocará la fotografía con su **rostro al descubierto.**	✓
Se colocará la fotografía **con su rostro tapado.**	

- Toda la información se tratará con la máxima confidencialidad *(Seleccione con una X)*:

Se citará con su **nombre completo y el cargo institucional.**	
Se citará **únicamente el cargo institucional.**	
Se citará **usando sus iniciales y el cargo institucional.**	✓

Se citará únicamente sus iniciales	

- Los datos recopilados se utilizarán exclusivamente para la investigación y el desarrollo de la tesis.

Su participación es voluntaria, tiene derecho a negarse **a responder determinadas preguntas o a** interrumpir la entrevista en cualquier momento, sin **tener que dar ninguna explicación.**

Nombre del entrevistado: I. A. G. V.

Firma:

Fecha: 14- Enero de 2026.

Entrevistado 5: Clara Marisela V.L_ Abogada e ingeniería en sistemas con maestría en ciberseguridad.

- Consentimiento informado

CONSENTIMIENTO INFORMADO

UNIVERSIDAD NACIONAL DE CHIMBORAZO – CARRERA DE DERECHO

Proyecto de investigación: La construcción del perfil criminológico del ciberdelincuente para la detección oportuna del phishing en Ecuador.

Investigadora: Sandy Solange Salguero Muñoz

CONSENTIMIENTO INFORMADO PARA PARTICIPANTES

Le invito a participar en esta entrevista semiestructurada como experto/a en el marco de un proyecto de investigación universitaria.

El objetivo es recopilar sus conocimientos técnicos y empíricos sobre los rasgos y métodos operativos de los ciberdelincuentes, ataques de phishing, el marco institucional y jurídico, así como la viabilidad de establecer el perfil criminológico como herramienta elemental para la detección oportuna del phishing.

Al participar, usted acepta las siguientes condiciones:

- La entrevista se grabará exclusivamente con fines de transcripción y análisis.
- Se tomará una fotografía al inicio o al final de la entrevista con el fin de documentar el uso de la herramienta. *(Seleccione con una X)*

Se colocará la fotografía con su rostro al descubierto.	
Se colocará la fotografía con su rostro tapado.	

- Toda la información se tratará con la máxima confidencialidad *(Seleccione con una X)*:

Se citará con su nombre completo y el cargo institucional.	
Se citará únicamente el cargo institucional.	
Se citará usando sus iniciales y el cargo institucional.	

Se citará únicamente sus iniciales	

- Los datos recopilados se utilizarán exclusivamente para la investigación y el desarrollo de la tesis.

Su participación es voluntaria, tiene derecho a negarse a responder determinadas preguntas o a interrumpir la entrevista en cualquier momento, sin tener que dar ninguna explicación.

Nombre del entrevistado:

Firma:

CLARA MARISELA VELIZ LOOR

Fecha: