

UNIVERSIDAD DE ESPECIALIDADES ESPIRITU SANTO

FACULTAD DE DERECHO, POLÍTICA Y DESARROLLO

TITULO: VACÍOS NORMATIVOS Y DESAFÍOS PROBATORIOS EN LA EXTORSIÓN DIGITAL: NECESIDAD DE UN SUBTIPO PENAL ESPECIALIZADO EN EL ECUADOR

TRABAJO DE TITULACIÓN QUE SE PRESENTA COMO REQUISITO PREVIO A OPTAR EL GRADO DE ABOGADO DE LOS TRIBUNALES Y JUZGADOS DE LA REPÚBLICA

NOMBRE DEL ESTUDIANTE

HELLEN STEFANNY VERA ÁLVAREZ

NOMBRE DEL TUTOR

Mgtr. BRICCIDA MAGALI ROBLES PIEDRAHITA

Samborondón, diciembre, 2025

VACÍOS NORMATIVOS Y DESAFÍOS PROBATORIOS EN LA EXTORSIÓN DIGITAL: NECESIDAD DE UN SUBTIPO PENAL ESPECIALIZADO EN EL ECUADOR

CARTA DE APROBACIÒN DEL TUTOR

En mi calidad de tutor de **HELLEN STEFANNY VERA ÁLVAREZ**, estudiante de la Facultad de Derecho, Política y Desarrollo de la Universidad de Especialidades Espíritu Santo,

CERTIFICO

Que, una vez analizado el trabajo de titulación titulado "VACÍOS NORMATIVOS Y DESAFÍOS PROBATORIOS EN LA EXTORSIÓN DIGITAL: NECESIDAD DE UN SUBTIPO PENAL ESPECIALIZADO EN EL ECUADOR", presentado como requisito previo a obtener el grado de Abogado, el mismo cumple con los requisitos y méritos académicos, razón por la cual lo APRUEBO en su totalidad.

MGS. BRICCIDA MAGALI ROBLES PIEDRAHITA

TUTORA

VACÍOS NORMATIVOS Y DESAFÍOS PROBATORIOS EN LA EXTORSIÓN DIGITAL: NECESIDAD DE UN SUBTIPO PENAL ESPECIALIZADO EN EL ECUADOR

INFORMACIÓN DEL AUTOR

Nombre completo: Hellen Stefanny Vera Álvarez

Título académico más alto: Bachiller

Institución donde estudia: Universidad Espíritu Santo – Ecuador

Especialidad / área: Ciencias Sociales

Dependencia en la que trabaja: No aplica

Institución de procedencia: Academia Naval Almirante Illingworth

Grupo de investigación / Filiación institucional: Universidad Espíritu Santo – Ecuador

Correo institucional: hellen.vera@uees.edu.ec

Dirección de correspondencia: Facultad de Derecho, Edificio P, Universidad Espíritu Santo, Km. 2.5 Vía Puntilla, Samborondón

DEDICATORIA

A mi madre, por su amor incondicional, su fortaleza y por enseñarme que la perseverancia siempre abre caminos.

Y, de manera muy especial, a mi hijo Antonio Guzmán Vera, cuya existencia da sentido a cada uno de mis esfuerzos. Este logro es para él, con la esperanza de que un día comprenda que todo lo que hago es para brindarle un futuro lleno de oportunidades y orgullo.

VACÍOS NORMATIVOS Y DESAFÍOS PROBATORIOS EN LA EXTORSIÓN DIGITAL: NECESIDAD DE UN SUBTIPO PENAL ESPECIALIZADO EN EL ECUADOR

Índice de Contenido

Resumen 7

Abstract 8

1. Introducción 9

2. Marco teórico 11

2.1. Conceptos doctrinales sobre extorsión 11

2.2. Doctrina penal sobre estructura de delito 13

2.2.1. Tipicidad 13

2.2.2. Antijuridicidad 13

2.2.3. Culpable 14

2.3. Delitos informáticos: teoría y evolución 14

2.4. Elementos de la prueba digital: integridad, cadena de custodia y autenticidad 16

2.5. Estándares internacionales 18

2.5.1. Budapest 18

2.5.2. ISO 19

2.5.3. Recomendaciones Periciales 21

2.6. Posturas doctrinales sobre subtítulos penales 22

2.7. Volatilidad de la evidencia digital y su afectación en la impunidad objetiva . 23

2.8. Ejemplos prácticos sobre esquemas de Cyber extorsión 24

2.9. Imposibilidad de imputar responsabilidad penal con estándares tradicionales de prueba 25

2.10. Breve análisis de países que han tipificado subtipos de ciberextorsión. 27

3. Marco Metodológico 28

3.1. Tipo de investigación 28

3.2. Enfoque 28

3.3. Método 29

3.5. Fuentes 29

3.6. Delimitación 30

4. Resultados y Discusión 31

4.1. Evolución doctrinal y normativa de los delitos informáticos en el derecho ecuatoriano 31

4.2. Dificultades probatorias y procesales en la persecución penal de la ciberextorsión 33

4.3. Valoración de la necesidad de un tipo penal autónomo para la ciberextorsión en Ecuador 35

4.4. Implicaciones del vacío normativo en la seguridad jurídica, el debido proceso y la eficacia de la persecución penal 37

5. Conclusiones 39

6. Recomendaciones 40

7. Bibliografía 41

VACÍOS NORMATIVOS Y DESAFÍOS PROBATORIOS EN LA EXTORSIÓN DIGITAL: NECESIDAD DE UN SUBTIPO PENAL ESPECIALIZADO EN EL ECUADOR

Resumen

La investigación identificó los vacíos normativos y probatorios de la extorsión informática en Ecuador y propuso la creación de un tipo penal autónomo de ciberextorsión. Se utilizó un enfoque metodológico cualitativo, jurídico-documental, analítico-comparado, con análisis de contenido y hermenéutico, siendo sus fuentes el COIP, estándares internacionales (Budapest, NIST, ENISA), doctrina, jurisprudencia y derecho comparado. Los resultados mostraron la insuficiencia del art. 185 del COIP para tipificar la ciberextorsión en sus dimensiones técnica y criminológica, la dispersión entre los arts. 230-233, la falta de protocolos nacionales de evidencia digital y las dificultades para la autoría y cadena de custodia en un ambiente de anonimización y volatilidad de datos. Se determinó que la tipificación de un delito autónomo de ciberextorsión, en línea con estándares técnicos internacionales y acompañado de estándares probatorios comunes, es una condición necesaria para fortalecer la seguridad jurídica, la efectividad de la persecución penal y la protección de las víctimas.

Palabras clave: vacíos normativos, extorsión digital, COIP, prueba electrónica, criminalidad informática.

VACÍOS NORMATIVOS Y DESAFÍOS PROBATORIOS EN LA EXTORSIÓN DIGITAL: NECESIDAD DE UN SUBTIPO PENAL ESPECIALIZADO EN EL ECUADOR

Abstract

The research identified the regulatory and evidentiary gaps in cyber extortion in Ecuador and proposed the creation of an autonomous criminal offense of cyber extortion. A qualitative, legal-documentary, analytical-comparative methodological approach was used, employing content and hermeneutic analysis. Sources included the Comprehensive Organic Criminal Code (COIP), international standards (Budapest, NIST, ENISA), legal scholarship, jurisprudence, and comparative law. The results showed the inadequacy of Article 185 of the COIP to define cyber extortion in its technical and criminological dimensions, the fragmentation between Articles 230-233, the lack of national protocols for digital evidence, and the difficulties in establishing authorship and chain of custody in an environment of data anonymization and volatility. It was determined that defining an autonomous crime of cyber extortion, in line with international technical standards and accompanied by common evidentiary standards, is a necessary condition for strengthening legal certainty, the effectiveness of criminal prosecution, and the protection of victims.

Keywords: Regulatory gaps, digital extortion, COIP, electronic evidence, cybercrime.

VACÍOS NORMATIVOS Y DESAFÍOS PROBATORIOS EN LA EXTORSIÓN DIGITAL: NECESIDAD DE UN SUBTIPO PENAL ESPECIALIZADO EN EL ECUADOR

1. Introducción

En Ecuador, la extorsión se posicionó como el delito más denunciado en 2023, con 21 811 casos denunciados ante la Fiscalía, lo que demuestra la magnitud y continuidad del problema[1]. Hoy el fenómeno se ha movido a los canales digitales, como la mensajería, las redes sociales y los mecanismos de coerción a distancia difíciles de rastrear. Para 2024, noticias de prensa con fuentes oficiales informaron de 19 473 denuncias hasta noviembre, pero verificaciones independientes calcularon un promedio mensual de 1 975 casos, lo que demuestra que sigue siendo alta la criminalidad que afecta principalmente a zonas urbanas y comerciales[2].

Desde el ámbito legal, el Código Orgánico Integral Penal (COIP) en su artículo 185 ya sanciona la extorsión, pero no como un delito específico cometido por medios cibernéticos; en la práctica, estos casos se subsumen en la tipificación general o se acercan a otros delitos cibernéticos. Por otro lado, el andamiaje probatorio sí reconoce la especificidad digital: el artículo 456 exige cadena de custodia también para evidencia digital, y el artículo 457 enumera criterios de valoración que incluyen legalidad, autenticidad y sujeción a la cadena, lo que demuestra la necesidad de engranar política criminal y técnica probatoria con un posible subtipo especializado[3].

---

[1] OBSERVATORIO ECUATORIANO DE CRIMEN ORGANIZADO (OECO), Tipologías y resultados de la Encuesta Nacional de Victimización de Casos de Extorsión Empresarial, Quito, 2024, disponible en: https://oeco.padf.org/wp-content/uploads/2024/05/OECO_Radiografia-de-la-extorsion-en-Ecuador-1.pdf.

[2] BRANDON, Andrés; MARFETAN, Valeria y MACHADO, Marco, "Evidencias Deepfake en sistema penal ecuatoriano: reconocimiento, autenticidad y aceptación probatoria en juicios", en Verdad y Derecho. Revista Arbitrada de Ciencias Jurídicas y Sociales, vol. 4, 2025, pp. 325–343, doi: https://doi.org/10.62574/r083dh53

[3] Código Orgánico Integral Penal (COIP), arts. 185, 456 y 457.

En el contexto planteado, se evidencia que el derecho penal ecuatoriano todavía se queda corto en dar respuesta a las nuevas formas delictivas que surgen de las tecnologías digitales. Si bien el COIP desde 2014 ya contiene algunas figuras relacionadas con delitos informáticos, aún adolece de una tipificación específica para la extorsión por medios electrónicos[4]. Esta falta de información no permite reconocer con exactitud los rasgos de la ciberextorsión como el uso tecnológico para manipular psicológica y financieramente a las víctimas. El Observatorio Ecuatoriano de Crimen Organizado advierte que el aumento de estos casos se relaciona con el uso de plataformas digitales y servicios de mensajería, creando un vacío entre la realidad tecnológica y el marco legal existente[5].

Asimismo, el problema también se vuelve probatorio, ya que las amenazas cibernéticas, el robo de identidad y la manipulación de datos dificultan la preservación y autenticidad de la evidencia digital. Si bien la legislación ecuatoriana necesita ser reformada para incluir sanciones proporcionales y criterios técnicos para evaluar la prueba digital[6], otros países de la región ya han actualizado parcialmente sus marcos legales, pero sin generar subtipos penales[7]. Por lo cual, el Ecuador debe alinear su legislación a estándares internacionales como el Convenio de Budapest y fortalecer la capacidad investigativa con peritos especializados y capacitación judicial[7].

La investigación es relevante porque trata sobre la falta de un tipo penal para la extorsión informática en Ecuador, lo que impide una persecución y protección efectiva para las

[4] ORDOÑEZ, Luis, "El Marco Legal de los Delitos Cibernéticos en Ecuador", en Reincisol, vol. 5, núm. 3, 2024, pp. 1447–1469, doi: https://doi.org/10.59282/reincisol.V3(5)1447-1469

[5] OECO, Tipologías…, p. 40

[6] SARMIENTO, Juan y MALDONADO, Laura, "Delitos informáticos y ciberataques: análisis jurídico en el derecho penal del Ecuador", en MQRInvestigar, vol. 8, núm. 3, 2024, pp. 1753–1781, doi: https://doi.org/10.56048/MQR20225.8.3.2024.1753-1781

[7] Consejo de Europa, Convenio de Budapest sobre Ciberdelincuencia, Budapest, 2001.

víctimas. Su estudio proporciona bases jurídicas y técnicas para modernizar el COIP y mejorar la política criminal contra los delitos informáticos. Además, analiza los problemas probatorios que surgen de la evidencia digital, sugiriendo lineamientos de preservación y evaluación que fortalezcan la eficacia del proceso y la seguridad jurídica.

El objetivo general de la investigación es identificar los vacíos legales y problemas probatorios de la extorsión informática en el Ecuador y plantear la necesidad de un subtipo penal específico que mejore la respuesta legal ante la ciberdelincuencia. Para lograr este objetivo, se proponen los siguientes objetivos específicos: (I) Analizar la evolución doctrinal y normativa de los delitos informáticos en el derecho ecuatoriano; (II) Determinar las principales dificultades probatorias y procesales en la persecución penal de la ciberextorsión; (III) Valorar la necesidad de crear un tipo penal autónomo que tipifique la extorsión cometida por medios cibernéticos.

El estudio se organiza en seis partes: la introducción, que plantea y delimita el problema; el marco teórico, que trata sobre los fundamentos doctrinales y normativos; el marco metodológico, que explica el método bibliográfico y analítico; los resultados y discusión, en los que se exponen y comparan los resultados; y las conclusiones y recomendaciones, que resumen las propuestas finales. Finalmente, la bibliografía.

2. Marco teórico

2.1. Conceptos doctrinales sobre extorsión

La extorsión ha sido conceptualizada doctrinariamente como el comportamiento en el que el victimario, usando fuerza, intimidación o amenazas, obliga a la víctima a hacer, tolerar u omitir algo para obtener un beneficio pecuniario ilícito[8]. En el derecho penal, este tipo

[8] SARMIENTO/MALDONADO, “Delitos informáticos y ciberataques…”, p. 1755

de extorsión se distingue por el uso de la fuerza sobre la víctima, anulando su voluntad y atentando contra su autonomía y seguridad patrimonial. Las teorías actuales señalan que la clave de la extorsión es el uso de un medio capaz de infundir temor justificado en la víctima y que la obligue a hacer algo en contra de su voluntad[9].

Desde un punto de vista dogmático, la extorsión se encuadra entre los delitos contra la propiedad, pero su estructura típica va más allá de la protección del patrimonio, ya que protege también la libertad[10]. El derecho penal distingue la extorsión del robo con violencia en que en éste el apoderamiento es directo e inmediato, en tanto que en aquélla la víctima coopera forzada en la disposición patrimonial. Esta diferencia hace hincapié en que no se requiere necesariamente un contacto físico, sino una transferencia realizada bajo presión, lo que amplía la conducta típica[11].

En los estudios actuales, los autores señalan que la extorsión se ha adaptado a las nuevas tecnologías, creando así nuevos contextos en los que el victimario puede lograr el mismo resultado intimidatorio sin estar presente físicamente, mediante amenazas virtuales, manipulación de información o suplantación de identidad[12]. Estas nuevas formas mantienen los elementos del delito amenaza, sumisión y obtención de beneficio, pero ahora en el mundo virtual, por lo que se han llegado a proponer tipificaciones más específicas que logren dar cuenta de la complejidad del mundo tecnológico actual.

---

[9] NAVARRO, Luis, El ciberacoso y la impunidad: razones para el correcto desarrollo de una nueva normativa penal peruana en base al análisis de investigaciones archivadas. Escuela Académica Profesional de Derecho, Universidad Continental, Huancayo, Perú, 2024.

[10] SINALUISA SAGÑAY, Fabián, Deepfakes, dificultades probatorias y su incidencia en la vulneración al derecho de intimidad, tesis de pregrado, Universidad Nacional de Chimborazo, Riobamba, 2024.

[11] CADILLO, B. A., ¨La evidencia digital en el cibercrimen – Perú 2022¨, tesis de licenciatura, Universidad Privada del Norte, Lima, 2022, disponible en: https://hdl.handle.net/11537/32802

[12] SINALUISA SAGÑAY, Deepfakes…, p. 234

2.2. Doctrina penal sobre estructura de delito

El derecho penal actual define el delito como una estructura jurídica compleja, sistematizada por el causalismo clásico del siglo XIX, reformulado por el finalismo del siglo XX y perfeccionada por las teorías funcionalistas actuales. En este contexto, el delito se estudia en tres categorías: tipicidad, antijuridicidad y culpabilidad, el modelo actualmente prevaleciente en Europa y Latinoamérica[13].

2.2.1. Tipicidad

La tipicidad es la adecuación de la conducta a la descripción del tipo penal. Para Welzel y el finalismo, la tipicidad requiere no sólo una acción humana voluntaria, sino también la presencia de elementos objetivos (nexo causal, resultado típico y circunstancias externas del tipo). La visión actual añade la teoría de la imputación objetiva (creada por Claus Roxin), según la cual un resultado sólo puede imputarse al autor cuando éste crea un riesgo jurídicamente disaprobado que se realiza en el resultado lesivo. La tipicidad subjetiva, en cambio, comprende el dolo y la culpa (el conocimiento y la voluntad o la infracción del deber de cuidado)[14].

2.2.2. Antijuridicidad

[13] LÓPEZ SORIA, Y.; SÁNCHEZ OVIEDO, D. X.; CAJAS PÉREZ, J. L. y ORTIZ CRIOLLO, O. C., "La culpabilidad prescindible como elemento en la estructura del delito", en Revista Universidad y Sociedad, vol. 14, núm. 6, 2022, pp. 278–289.

[14] GRANJA ZURITA, D. F.; ABAD TANDAZO, M. H.; PAREDES LÓPEZ, J. A. y REY SIQUILANDA, C. F., "La ausencia del error en el Código Orgánico Integral Penal en la conducta delictiva del procesado en Ecuador", en *Universidad y Sociedad*, vol. 14, suplemento 4, 2022, pp. 59–69.

Una conducta ordinaria no es delito a menos que sea antijurídica. La antijuridicidad significa que la conducta es contraria al derecho, viola un bien jurídico protegido. Para Zaffaroni y Muñoz Conde, lo antijurídico no se agota en la contradicción formal con la ley penal, sino que requiere una lesión o puesta en peligro material del bien jurídico.

Pero hay causas de justificación que eliminan la antijuridicidad, aunque la conducta sea típica, como la legítima defensa, el estado de necesidad justificante, el cumplimiento de un deber o el ejercicio legítimo de un derecho. Cuando alguna de estas causas está presente, el hecho pierde su carácter antijurídico y no es susceptible de reproche penal[15].

2.2.3. Culpable

La culpabilidad es el juicio de reproche que se hace al autor por haber cometido un hecho típico y antijurídico cuando podía haber obrado conforme a derecho. Para Roxin y Jakobs, la culpabilidad se compone de tres elementos: imputabilidad, conciencia de la antijuridicidad y exigibilidad de una conducta diferente.

La imputabilidad requiere capacidad para comprender la ilicitud del acto; la conciencia de la antijuridicidad es el conocimiento real o supuesto de la prohibición; y la exigibilidad consiste en determinar si, en las circunstancias específicas, era exigible al autor ajustarse al derecho[16].

2.3. Delitos informáticos: teoría y evolución

[15] BASTIDAS GONZÁLEZ, K. A., "El delito en el derecho penal: construcción jurídica y retos contemporáneos", en Sapiens Evolución Científica, vol. 2, núm. 1, 2024, e-21004.
[16] IZQUIERDO MORILLAS, M., "Desentrañando el delito: un viaje por las principales teorías dogmáticas y los retos actuales", en Revista Estudios Jurídicos. Segunda Época, núm. 24, 2024, e8909.

La criminología informática surge como una respuesta a la evolución tecnológica que cambió la manera de cometer y encubrir delitos. En un principio, estos delitos se concebían como aquellos en los que los sistemas informáticos solo eran medios para cometer fraudes o accesos indebidos, pero con la digitalización la doctrina abrió el concepto a toda conducta que atente contra la integridad, confidencialidad o disponibilidad de los datos y sistemas[17].

Esta evolución hizo posible distinguir entre delitos cometidos por medios informáticos y delitos contra sistemas, reconociendo riesgos que van más allá de la pérdida patrimonial[18]. Con el cibercrimen, las legislaciones nacionales fueron incluyendo normas específicas, espoleadas también por textos internacionales como el Convenio de Budapest, que puso de manifiesto la necesidad de unas normas comunes ante unos delitos transnacionales[18].

El surgimiento de formas como el phishing, el ransomware o la ciberextorsión dejó claro que los tipos penales tradicionales no eran suficientes para enfrentarse a delitos cuya prueba es volátil, intangible y manipulable. Por eso, la nueva ley ha venido a definir mejores términos como sistema informático, acceso ilegítimo o dato informático, necesarios para una mejor interpretación de la ley[19].

En tiempos recientes, el desarrollo tecnológico inteligencia artificial, deepfakes, comunicaciones encriptadas, etc. vino a complicar aún más el panorama delictivo,

[17] LÓPEZ SORIA, Y.; SÁNCHEZ OVIEDO, D. X.; CAJAS PÉREZ, J. L. y ORTIZ CRIOLLO, O. C., "La culpabilidad prescindible como elemento en la estructura del delito", en Revista Universidad y Sociedad, vol. 14, núm. 6, 2022, pp. 278–289.
[18] ROMERO ESTÉVEZ, I. M., "Aplicabilidad de la teoría de la imputación objetiva en los delitos culposos del COIP", en Revista Lex, vol. 7, núm. 27, 2024, pp. 1546–1562.
[19] BECERRA, J. y GOICOCHEA, W., "Razones jurídicas para incorporar la autopuesta en peligro de la víctima como causa de disminución de punibilidad en los delitos culposos", 2020.

dificultando la atribución de responsabilidad y la preservación de la evidencia digital. La teoría actual ya no considera a los delitos informáticos como meras adaptaciones tecnológicas de delitos tradicionales, sino como delitos autónomos que necesitan tipificaciones específicas y métodos probatorios especializados[20]. Este avance reafirma la necesidad de que el derecho penal se actualice continuamente a los avances tecnológicos para tutelar de manera efectiva bienes jurídicos cada vez más vinculados al mundo digital[21].

2.4. Elementos de la prueba digital: integridad, cadena de custodia y autenticidad

La evidencia digital tiene la peculiaridad de que necesita ciertos parámetros técnico-jurídicos para ser válida en el proceso penal, a diferencia de la evidencia física, la evidencia digital es vulnerable, replicable y susceptible de alterarse sin dejar rastro, por lo que su manejo debe ajustarse a estándares de conservación que permitan certificar su integridad[21].

En ese contexto, los factores que no pueden faltar para que se considere en su valor son la integridad, la cadena de custodia y la autenticidad, que trabajan en conjunto para garantizar que el material presentado no haya sido manipulado y que realmente corresponda al hecho en cuestión[22].

[20] GRANJA ZURITA et al., "La ausencia del error…", p. 60.
[21] SARMIENTO, Juan y MALDONADO, Laura, "Delitos informáticos y ciberataques: análisis jurídico en el derecho penal del Ecuador", en MQRInvestigar, vol. 8, núm. 3, 2024, pp. 1753–1781, doi: https://doi.org/10.56048/MQR20225.8.3.2024.1753-1781
[22] SARMIENTO/MALDONADO, "Delitos informáticos y ciberataques…", p. 1753

La integridad es la garantía de que la evidencia digital no ha sido alterada desde el momento de la adquisición hasta su presentación ante la autoridad competente. En la práctica forense, esto se autentica con métodos como hash values, clonación forense o imagen bit a bit, las cuales prueban que lo preservado es idéntico al original. Si la integridad no se puede verificar, el material pierde valor como evidencia, ya que no se puede garantizar que represente con precisión la información recopilada durante la investigación[23].

La cadena de custodia garantiza el registro cronológico de todos los pasos involucrados en la recolección, transferencia, almacenamiento y análisis de la evidencia digital. Toda persona que manipule el material debe ser identificada con fecha, hora, lugar y procedimiento utilizado[21]. En Ecuador, este requisito está consagrado en el código penal, que exige una cadena de custodia para las pruebas electrónicas por su facilidad de manipulación. La falla o ausencia de cadena de custodia puede causar su exclusión o pérdida de credibilidad[24].

Así también, la autenticidad es la capacidad de probar que la evidencia digital realmente se originó en la fuente que se afirma y fue creada por el dispositivo, usuario o sistema especificado. Este es esencial para relacionar el contenido con un sujeto procesal, un acto comunicacional o un artefacto tecnológico. La autenticidad se confirma con técnicas de análisis, metadatos, registros de actividad y peritajes forenses para establecer la

[23] IZQUIERDO MORILLAS, "Desentrañando el delito…", p. 70.
[24] BASTIDAS GONZÁLEZ, "El delito en el derecho penal…", p. 51.

procedencia y autoría digital. Cuando la autenticidad no puede probarse, la evidencia no es confiable y no alcanza el estándar requerido para el proceso penal[25].

2.5. Estándares internacionales

Los estándares internacionales sobre ciberdelincuencia son el punto de referencia para la armonización legislativa entre los Estados, especialmente para delitos transfronterizos que exigen cooperación judicial y técnica. Varias instituciones (Consejo de Europa, Naciones Unidas, OEA, etc.) han elaborado directrices para mejorar la investigación, conservación de pruebas digitales y persecución penal de delitos informáticos.

2.5.1. Budapest

El Convenio de Budapest, es el principal instrumento internacional jurídicamente vinculante en materia de ciberdelincuencia y sirve de marco para la lucha mundial contra la ciberdelincuencia. Este tratado crea definiciones comunes de acceso no autorizado, intercepción ilegal, manipulación de datos, fraude informático y delitos de contenido en línea[26].

Además, establece estándares procesales para adquirir evidencia digital rápidamente, como la preservación acelerada de datos, el acceso transfronterizo regulado y la colaboración entre unidades especializadas. Su importancia es que da un lenguaje legal común a los Estados, permite la cooperación internacional y establece las bases para

[25] GRANJA ZURITA et al., "La ausencia del error…", p. 64.
[26] SARMIENTO, Juan y MALDONADO, Laura, "Delitos informáticos y ciberataques: análisis jurídico en el derecho penal del Ecuador", en MQRInvestigar, vol. 8, núm. 3, 2024, pp. 1753–1781, doi: https://doi.org/10.56048/MQR20225.8.3.2024.1753-1781

combatir nuevas formas como la ciberextorsión, los ataques contra infraestructuras críticas y la ciberdelincuencia organizada[27].

2.5.2. ISO

Los estándares ISO son una de las bases técnicas más importantes para la gestión de la información y el tratamiento de la evidencia digital[28]. Desde la informática forense, estas normas representan medidas de objetividad, reproducibilidad y verificabilidad, para que los procedimientos realizados por los expertos y los investigadores se ajusten a estándares internacionales. Su uso en la investigación criminal no es sólo práctico, sino que cumple con el requisito de fiabilidad científica para la admisión de prueba pericial en tribunales modernos.

La doctrina penal y pericial ya reconoce que la evidencia digital solo tiene valor legal si los métodos para recolectarla y analizarla siguen estándares que aseguren su integridad, autenticidad y trazabilidad. Aquí es donde las normas ISO 27000 vienen en juego, proporcionando un marco metodológico para organizar la respuesta de la investigación bajo control técnico, garantía forense y documentación, lo necesario para vencer cualquier duda sobre contaminación, manipulación o alteración de datos[29].

A continuación, los subapartados desde una mirada técnico-doctrinal:

---

[27] Consejo de Europa, *Convenio de Budapest sobre Ciberdelincuencia*, 23 de noviembre de 2001 (Serie de Tratados del Consejo de Europa, No. 185).

[28] Organización Internacional de Normalización (ISO/IEC), ISO/IEC 27037: Directrices para la identificación, recolección y preservación de evidencia digital, Ginebra, 2012.

[29] Organización Internacional de Normalización (ISO/IEC), *ISO/IEC 27037: Directrices para la identificación, recolección y preservación de evidencia digital*, Ginebra, 2012.

2.5.2.1. ISO/IEC 27001 – Seguridad de la información como base institucional

La ISO/IEC 27001 especifica los requisitos para establecer un Sistema de Gestión de Seguridad de la Información (SGSI), erigiéndose como el marco de referencia que asegura que las instituciones de investigación penal Fiscalía, Policía, laboratorios forenses tengan controles sobre la información que manejan. Su importancia legal se debe a que define políticas, procedimientos y controles para preservar la evidencia digital en su totalidad y evitar cualquier laguna en la cadena de custodia o en la confidencialidad de la información sensible[30].

2.5.2.2. ISO/IEC 27037 - Estándar para la identificación y preservación de evidencia digital

La ISO/IEC 27037 es reconocida por la doctrina como la norma marco de preservación forense. Establecer criterios técnicos para el reconocimiento, recolección, adquisición y preservación de evidencia digital, tales como mínima intervención, preservación de metadatos y documentación de la cadena de custodia. Su importancia legal se basa en que puede probar la integridad de la evidencia contra acusaciones de manipulación o alteración, garantizando que la evidencia digital presentada en la corte sea una copia exacta del original[31].

[30] Organización Internacional de Normalización (ISO/IEC), ISO/IEC 27001: Sistemas de Gestión de Seguridad de la Información (SGSI), Ginebra, 2013.
[31] Organización Internacional de Normalización (ISO/IEC), ISO/IEC 27037: Directrices para la identificación, recolección y preservación de evidencia digital, Ginebra, 2012.

2.5.2.3.ISO/IEC 27041:2015 - Aseguramiento de la validez metodológica en el análisis forense

La ISO/IEC 27041 trata la necesidad teórica de medir la adecuación y reproducibilidad de los métodos forenses en una investigación digital. Define criterios para evaluar si las técnicas utilizadas son fiables, validadas y están en línea con las mejores prácticas internacionales. Desde el punto de vista penal, esta norma refuerza la legitimidad de los informes periciales, en el sentido de poder evidenciar que el análisis se llevó a cabo bajo criterios verificables, disminuyendo el margen de subjetividad técnica[32].

2.5.2.4. ISO/IEC 27042:2015 - Directrices para la interpretación técnico-jurídica de la evidencia digital

La ISO/IEC 27042 aborda la interpretación y el análisis de la evidencia, el corazón de la doctrina de la informática forense. Guía sobre cómo reconstruir incidentes, interpretar registros, analizar artefactos digitales y presentar hallazgos de una manera que sea comprensible para el sistema legal. Su importancia es que introduce el principio de transparencia metodológica, esencial para que la evidencia digital sea considerada objetiva y susceptible de contradicción en juicio[33].

2.5.3. Recomendaciones Periciales

Las recomendaciones periciales informáticas van dirigidas a garantizar que la evidencia digital sea adquirida, preservada y analizada bajo estándares técnicos que garanticen su

[32] Organización Internacional de Normalización (ISO/IEC), ISO/IEC 27041: Guía para asegurar la idoneidad y adecuación de los métodos de investigación de incidentes, Ginebra, 2015.
[33] Organización Internacional de Normalización (ISO/IEC), ISO/IEC 27042: Directrices para el análisis e interpretación de evidencia digital, Ginebra, 2015.

admisibilidad en la corte. Entre las guías más conocidas se encuentra la Guía de Buenas Prácticas en Informática Forense de la ENISA (Agencia Europea de Ciberseguridad), que define los pasos para recolectar, etiquetar, preservar y analizar soportes digitales[34].

Además, agencias como el NIST en Estados Unidos han creado estándares técnicos (por ejemplo, la serie NIST SP 800) que especifican procedimientos para el análisis forense de discos, dispositivos móviles y nubes[35]. Estas recomendaciones refuerzan la labor del perito, ofreciendo procedimientos reconocidos a nivel internacional y asegurando que toda intervención cumpla con los principios de trazabilidad, integridad y replicabilidad, esenciales para la evidencia en un juicio.

2.6. Posturas doctrinales sobre subtítulos penales

La dogmática penal ha abordado distintas posturas sobre la utilidad y necesidad de los subtipos penales, entendidos como descripciones específicas dentro de un tipo penal que posibilitan una reacción más afinada ante conductas con características específicas. En general, los subtipos vienen a satisfacer la necesidad de especialización que hoy día necesita el derecho penal, con sus tipos delictivos cada vez más ricos y complejos, hasta el punto de que muchas veces no se llega a abarcar con la descripción básica del tipo todas las formas posibles de comisión[36].

---

[34] **ENISA**, *Digital Forensics — Guidelines for Evidence Acquisition*, European Union Agency for Cybersecurity, Heraklion, 2019.

[35] National Institute of Standards and Technology (NIST), *NIST Special Publication 800-101: Guidelines on Mobile Device Forensics*, Maryland, 2014.

[36] ROMÁN-NARANJO, J. A. y CHIMBORAZO-CASTILLO, L. A., "La falsedad material e ideológica de títulos ejecutivos: análisis comparado entre Ecuador y Chile", en Portal de la Ciencia, vol. 6, suplemento 1, 2025, pp. 22–36, doi: https://doi.org/10.51247/pdlc.v6iS1.604

Para la teoría tradicional, los subtipos representan una técnica legislativa para garantizar el principio de proporcionalidad, evitando una respuesta penal homogénea ante delitos de diferente gravedad o criminológicamente diferenciados[37]. Autores afirman que los subtipos penales también son precisos en la norma, ya que definen con mayor exactitud la conducta prohibida, disminuyendo la discrecionalidad judicial y reforzando las garantías del principio de legalidad[38].

En este sentido, los subtipos pueden constituir modalidades agravadas o atenuadas del tipo base o descripciones sustitutivas que añaden elementos descriptivos significativos (por ejemplo, el medio utilizado, el contexto tecnológico, la calidad del sujeto activo o la afectación a bienes jurídicos especialmente protegidos). Las corrientes funcionalistas, en cambio, señalan que la tipificación en subtipos hace posible la imputación objetiva, ya que permite identificar con mayor precisión los riesgos no permitidos para cada tipo delictivo[39].

2.7. Volatilidad de la evidencia digital y su afectación en la impunidad objetiva

La evidencia digital es altamente volátil; puede cambiar, manipularse, eliminarse o perderse en un abrir y cerrar de ojos, como resultado de acciones humanas, automatizaciones del sistema o procesos de red. Esta volatilidad hace que la preservación de rastros digitales requiera de herramientas forenses especializadas y protocolos rigurosos de cadena de custodia, tal como recomiendan estándares internacionales del

[37] CEVALLOS VALLEJO, Juan Nicolás, "Compatibilidad de los delitos de infracción de deber con el Código Orgánico Integral Penal", en USFQ Law Working Papers, 2023/05.
[38] GRANJA ZURITA et al., "La ausencia del error…", p. 62.
[39] SANTANDER, Y., "El elemento subjetivo en la responsabilidad del superior por crímenes de derecho penal internacional", en *Boletín Mexicano de Derecho Comparado*, vol. 57, núm. 171, 2024, pp. 239–273.

NIST y ENISA. Cuando estos procedimientos no se llevan a cabo adecuadamente, la información puede contaminarse o volverse irreproducible, lo que disminuye su valor como evidencia en un caso penal[40].

Esta volatilidad impacta en la impunidad objetiva, ya que sin evidencia técnica confiable es imposible probar la autoría, el rastro del ataque o incluso la existencia de la amenaza cibernética. En delitos como la ciber extorsión, en los que los victimarios utilizan VPN, teléfonos desechables, correos temporales o cifrado de extremo a extremo, cada minuto que pasa dificulta más la recolección de pistas. La falta de conservación o de personal preparado puede imposibilitar una acusación firme y dejar impune el delito, por grave que sea[41].

2.8. Ejemplos prácticos sobre esquemas de Cyber extorsión

En la ciberextorsión se pueden reconocer diferentes formas de acción. Otra es el phishing extorsivo, en el que el atacante se hace pasar por un banco o plataforma legítima para hacerse de las credenciales de acceso y, ya dentro de la cuenta, condiciona a no hacer transferencias, no bloquear dispositivos o no revelar información sensible al pago de dinero. Es un plan que usa ingeniería social y suplantación de identidad para crear un temor justificado en la víctima que vulnere su libertad de disposición patrimonial[42].

---

[40] SARMIENTO/MALDONADO, “Delitos informáticos y ciberataques…”, p. 1757

[41] IZQUIERDO MORILLAS, M., “Desentrañando el delito: un viaje por las principales teorías dogmáticas y los retos actuales”, en Revista Estudios Jurídicos. Segunda Época, núm. 24, 2024, e8909, doi: https://doi.org/10.17561/rej.n24.8909

[42] GRANJA ZURITA, D. F.; ABAD TANDAZO, M. H.; PAREDES LÓPEZ, J. A. y REY SIQUILANDA, C. F., “La ausencia del error en el Código Orgánico Integral Penal en la conducta delictiva del procesado en Ecuador”, en Universidad y Sociedad, vol. 14, suplemento 4, 2022, pp. 59–69, disponible en: https://rus.ucf.edu.cu/index.php/rus/article/view/3112

Otra forma importante es la sextorsión, que implica la obtención no autorizada de imágenes o videos de naturaleza íntima, ya sea a través de engaños, intrusiones en sistemas o manipulación emocional, y luego se amenaza con su difusión masiva si no se cumplen las demandas económicas o de comportamiento del victimario. A esto se añade el ransomware propagado a través de aplicaciones de mensajería instantánea, donde la descarga de software malicioso codifica la información del dispositivo y el restablecimiento del acceso depende del pago de un rescate, generalmente en criptoactivos. Estos mapas ilustran cómo la extorsión tradicional se transforma en digital utilizando malware, anonimato tecnológico y técnicas avanzadas de coerción[43].

2.9. Imposibilidad de imputar responsabilidad penal con estándares tradicionales de prueba.

La atribución de responsabilidad penal en delitos informáticos se topa con obstáculos cuando se aplican criterios probatorios clásicos, pensados para delitos materiales y no para acciones cibernéticas. En la extorsión informática, la evidencia forense se compone de metadatos, direcciones IP, logs de servidores, análisis de tráfico y otras evidencias altamente técnicas que no se ajustan a los modelos probatorios tradicionales basados en testigos oculares, documentos en papel o evidencia física. Esto crea lagunas, ya que la autoría digital necesita atribución técnica y correlación de datos de varias fuentes, lo que el sistema legal tradicional no siempre reconoce[44].

---

[43] SARMIENTO, Juan y MALDONADO, Laura, "Delitos informáticos y ciberataques: análisis jurídico en el derecho penal del Ecuador", en MQRInvestigar, vol. 8, núm. 3, 2024, pp. 1753–1781, doi: https://doi.org/10.56048/MQR20225.8.3.2024.1753-1781.

[44] IZQUIERDO MORILLAS, M., "Desentrañando el delito: un viaje por las principales teorías dogmáticas y los retos actuales", en Revista Estudios Jurídicos. Segunda Época, núm. 24, 2024, e8909, doi: https://doi.org/10.17561/rej.n24.8909

Además, los atacantes a menudo utilizan redes encriptadas, servicios de anonimización y aplicaciones de mensajería con autodestrucción para hacer imposible rastrear la actividad hasta el perpetrador. Cuando la evidencia se basa únicamente en capturas de pantalla, mensajes efímeros o direcciones IP variables, es difícil alcanzar el nivel de certeza requerido por el derecho penal. Como resultado, muchos casos se cierran por "falta de pruebas", no porque el delito no haya ocurrido, sino porque la forma tradicional de reunir pruebas no encaja con la naturaleza técnica, dispersa y transfronteriza de las pruebas digitales[45].

La dificultad de atribuir responsabilidad penal cuando no se cumplen estándares probatorios suficientes puede observarse en distintos precedentes constitucionales. En la sentencia 1406-17-EP/22[46], la Corte Constitucional confirmó el archivo de una investigación previa por extorsión al constatar que no existían elementos que permitieran sostener la imputación, lo que demuestra que, sin una base probatoria sólida, el proceso penal no puede avanzar. De manera complementaria, en el dictamen 3-25-EE/25[47], la Corte insistió en que las decisiones deben apoyarse únicamente en hechos verificables y técnicamente sustentados, descartando valoraciones basadas en información incompleta o no constatada. Aunque ninguna de estas sentencias analiza directamente la prueba digital, ambas sirven como ejemplo de cómo el sistema exige rigor y suficiencia

[45] BASTIDAS GONZÁLEZ, "El delito en el derecho penal…", p. 29

[46] **Corte Constitucional del Ecuador.** *Sentencia 1406-17-EP/22: Acción extraordinaria de protección respecto del archivo de denuncia penal por extorsión.* Quito, 2022. https://buscador.corteconstitucional.gob.ec/buscador-externo/principal/fichaSentencia?numero=1406-17-EP%2F22

[47] Corte Constitucional del Ecuador. Dictamen 3-25-EE/25: Control de constitucionalidad del estado de excepción declarado mediante Decreto Ejecutivo 599. Quito, 2025. https://buscador.corteconstitucional.gob.ec/buscador-externo/principal/fichaSentencia?numero=3-25-EE%2F25

probatoria, exigencia que se vuelve aún más compleja en delitos de extorsión informática, donde la evidencia técnica es determinante para acreditar autoría.

2.10. Breve análisis de países que han tipificado subtipos de ciberextorsión.

Algunos países han tipificado figuras muy cercanas a la ciberextorsión en su código penal. En España, la extorsión está tipificada en el art. 243 del Código Penal, pero hay subtipos tecnológicos importantes: el art. 197.5 (difusión no autorizada de datos o imágenes capturadas ilegalmente, común en sextorsión) y el art. 264 (daño informático, como bloquear o hacer inaccesibles datos, lo que permite perseguir casos de ransomware en los que se exige un rescate para recuperar el acceso)[48].

En tanto, Chile, con la Ley 21.459 de 2022, adecuó su Código Penal al Convenio de Budapest y tipificó delitos relacionados con la extorsión informática. El art. 2 castiga la interferencia o interrupción de sistemas informáticos (típico de los ataques en que se exige dinero a cambio de restaurar el sistema) y el art. 4 sanciona el acceso y difusión ilegítima de datos, útil en amenazas de divulgación de información robada. Ambos ejemplos demuestran cómo estos países han tipificado subtipos penales informáticos para complementar la extorsión clásica y así sancionar la coacción informática.

Como evidencia la experiencia de España y Chile, la tipificación de subtipos penales tecnológicos permite la subsunción adecuada de delitos como la sextorsión, el ransomware o la coacción digital, sin forzar la figura de la extorsión. Implementar un modelo como este en Ecuador ayudaría a definir mejor los aspectos técnicos de la

[48] BALLESTERO, Fernando, "Cómo mejorar la ciberseguridad en España: pasos ante una gran oportunidad", en Boletín Económico de ICE, núm. 3148, 2022, pp. 35–49.

ciberextorsión, disminuir la ambigüedad del art. 185 del COIP y proporcionar a fiscales y peritos un marco legal unificado para mejorar la investigación, preservación de evidencia y cooperación internacional.

3. Marco Metodológico

3.1. Tipo de investigación

La metodología es cualitativa, jurídico-documental, se basa en el análisis crítico de normas, doctrina, jurisprudencia y estándares internacionales referentes a la extorsión informática y su regulación penal en el Ecuador. Este tipo de estudio hace posible conocer la estructura normativa existente, encontrar lagunas jurídicas y determinar si el artículo 185 del COIP es suficiente ante las nuevas formas delictivas que emergen en el ciberespacio. Además, permite comparar el marco ecuatoriano con legislaciones extranjeras y estándares de organismos especializados, lo que proporciona una visión completa del fenómeno y su impacto en la prueba.

3.2. Enfoque

El enfoque es cualitativo-interpretativo, buscando comprender el fenómeno jurídico desde adentro, en su significado. Esta metodología es apropiada para analizar nociones como tipicidad, subtipos penales, evidencia digital, imputación objetiva, estándares de prueba y cómo la ley actual se aplica (o no) a los delitos cibernéticos. A través de él se analiza lo que realmente significan, en términos semánticos y operativos, las normas, la doctrina y la jurisprudencia, para establecer si hay correspondencia entre la realidad criminológica y la reacción penal que se tiene a disposición.

3.3.Método

El método utilizado es analítico-comparado, ya que se desglosa el art. 185 del COIP, la doctrina y los elementos de la extorsión informática, para compararlos con legislaciones extranjeras, normas internacionales como el Convenio de Budapest y directrices técnicas de evidencia digital. Esta metodología permite encontrar similitudes, lagunas y fortalezas entre modelos normativos y determinar la necesidad de tipificar un subtipo penal específico en el Ecuador. La comparación sistemática permite identificar buenas prácticas y criterios susceptibles de ser utilizados para mejorar la seguridad jurídica y la persecución penal.

3.4. Técnicas

Las técnicas utilizadas para esta investigación son el análisis documental y la hermenéutica jurídica, a través del estudio de la normativa penal, la doctrina y la jurisprudencia relacionada con la extorsión informática. Se aplicó el método de análisis de contenido, el cual permitió reconocer patrones, lagunas legales y conflictos interpretativos en el artículo 185 del COIP y su relación con las formas tecnológicas del delito. Para el componente comparado se utilizó el método de contraste normativo, para determinar cómo otras legislaciones abordan la ciberextorsión y qué aspectos podrían tomarse como referencia para la creación de un posible subtipo penal ecuatoriano.

3.5. Fuentes

La revisión normativa se basó en el art. 185 del COIP, que sanciona la extorsión, por ser la norma que se subsume directamente al objeto de estudio. Pero como en el ordenamiento jurídico ecuatoriano no existe un tipo penal de extorsión informática, se recurrió a normas

supletorias del mismo cuerpo legal, como el art. 230 (interceptación ilegal de datos), 231 (transferencia electrónica no autorizada), 232 (ataques a sistemas informáticos) y 186 (estafa). La comparación de dichas normas pudo evidenciar la dispersión normativa y el vacío legal que implica la falta de tipificación específica para la ciberextorsión. Este marco se nutrió de aportes doctrinales como los de Silva Sánchez[49], y de estándares internacionales como el Protocolo sobre Ciberdelito de la OEA[50] y el Convenio de Budapest.

Desde el punto de vista técnico, se adoptaron estándares del NIST[51], organismo estadounidense de referencia en evidencia digital y ciberseguridad, y de ENISA[52], agencia europea de referencia en buenas prácticas y gestión de incidentes cibernéticos. Además, se revisaron artículos científicos recientes de bases indexadas como SciELO, Redalyc, Dialnet, DOAJ, Web of Science, los cuales brindaron perspectivas comparadas, criterios periciales y debates actuales sobre política criminal en la extorsión informática.

3.6. Delimitación

La investigación se circunscribe al derecho penal ecuatoriano, en específico al art. 185 del COIP y demás normas conexas que intentan llenar el vacío de un subtipo de extorsión informática, como los arts. 230, 231, 232 y 186, cuya aplicación dispersa deja entrever vacíos tipológicos en la legislación interna. A nivel internacional, el análisis se limita a

[49] SILVA SÁNCHEZ, Jesús-María, La expansión del Derecho penal: aspectos de la política criminal en las sociedades postindustriales, Civitas, Madrid, 2006.
[50] ORGANIZACIÓN DE LOS ESTADOS AMERICANOS (OEA), Propuesta de Protocolo Hemisférico contra el Ciberdelito, Secretaría de Seguridad Multidimensional, 2016.
[51] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST), NIST Special Publication 800-86: Guide to Integrating Forensic Techniques into Incident Response, 2006.
[52] ENISA — EUROPEAN UNION AGENCY FOR CYBERSECURITY, Digital Forensics Guidelines: Identification, Collection, Acquisition and Preservation of Digital Evidence, 2021.

los estándares aplicables a la persecución de delitos cibernéticos, como el Convenio de Budapest y el Protocolo Hemisférico contra el Ciberdelito de la OEA, por ser marcos que informan la tipificación, cooperación y preservación de evidencia digital.

Metodológicamente, el estudio se limita a herramientas y guías técnicas de referencia como las del NIST o ENISA, las cuales definen procesos para preservar la autenticidad e integridad de la evidencia digital. Temporalmente, la investigación comprende los años 2019-2025, en los cuales se observa un aumento de comportamientos extorsivos cibernéticos y mayor producción científica sobre el tema.

4. Resultados y Discusión

4.1. Evolución doctrinal y normativa de los delitos informáticos en el derecho ecuatoriano

La evolución legislativa de los delitos informáticos en Ecuador ha sido gradual pero dispersa, más reactiva al avance tecnológico que a una política criminal planificada. Doctrinalmente, los primeros estudios aparecieron a principios de la década de 2000, cuando autores como Bastidas Gonzales[53] ya señalaban que el Código Penal de 1971 no contaba con mecanismos para sancionar delitos como el acceso ilegítimo, la interceptación de datos o el fraude informático, por lo que estos se subsumían a la fuerza en figuras tradicionales como daño, hurto o violación de correspondencia. Esta fase, conocida por la doctrina como de analogía expansiva, demostró la insuficiencia del derecho penal para abordar las nuevas formas de criminalidad informática.

[53] BASTIDAS GONZÁLEZ, K. A., "El delito en el derecho penal: construcción jurídica y retos contemporáneos", en Sapiens Evolución Científica, vol. 2, núm. 1, 2024, e-21004, disponible en: https://sapiensjournal.org/index.php/sec/article/view/28

Con la aprobación del COIP en 2014, por primera vez Ecuador cuenta con un cuerpo legal exclusivo para delitos informáticos. Artículos como el 230 (interceptación ilegítima), 231 (transferencias no autorizadas), 232 (alteración o destrucción de datos) y 233 (fraude informático) marcaron un gran avance al reconocer la autonomía de estas conductas[54]. Pero la doctrina ha advertido que esta primera clasificación fue incompleta y no logró ajustarse a un modelo completo de cibercriminalidad. La dispersión de las normas y la ausencia de un eje conceptual imposibilitaron su aplicación uniforme, especialmente en delitos complejos como la ciberextorsión, el phishing o los ataques transnacionales[55].

En estos años, el debate doctrinario se ha alimentado de estándares internacionales como el Convenio de Budapest sobre Ciberdelincuencia[56], que el Ministerio de Telecomunicaciones, la fiscalía general del Estado y la Policía Nacional han tomado como referencia para sus políticas de ciberseguridad. Si bien Ecuador no es parte del Convenio, sus principios tipificación tecnológica, preservación expedita de datos, cooperación internacional y reglas específicas de evidencia digital han sido referidos en informes técnicos y capacitaciones institucionales. Esto ha abierto interés de inevstigaciones doctrinales como la de Quezada y Genda[57] que afirman que la legislación ecuatoriana necesita actualizar sus tipos penales para ajustarlos al derecho comparado en delitos que involucren ingeniería social, anonimización y plataformas digitales encriptadas.

---

[54] Asamblea Nacional del Ecuador. Código Orgánico Integral Penal (COIP). Registro Oficial Suplemento 180, Quito, 2014.

[55] HERRERA, Santiago y MASAPANTA, Cristian, El papel de la prueba digital en los procedimientos penales en Ecuador, Universidad Andina Simón Bolívar, Quito, 2025, disponible en: https://repositorio.uasb.edu.ec/bitstream/10644/10524/1/T4605-MDPE-Herrera-El%20papel.pdf

[56] Consejo de Europa, Convenio de Budapest sobre Ciberdelincuencia, Budapest, 2001.

[57] QUEZADA, Andrea y GENDA, Carlos, "Delito de Ciberextorsión: un análisis jurídico y comparativo en países de Latinoamérica, Perú, Colombia y Ecuador", en Digital Publisher CEIT, vol. 10, núm. 1, 2025, pp. 546–556, doi: https://doi.org/10.33386/593dp.2025.1.2893.

La reciente evolución legislativa, con la Ley Orgánica de Protección de Datos Personales[58], viene a confirmar la necesidad de un abordaje integral que combine protección de datos, ciberseguridad y derecho penal. Pero esta ley no llena los vacíos del COIP en cuanto a ciberextorsión, porque se enfoca en proteger derechos de información y no en perseguir criminales. La doctrina actual reconoce que la ausencia de un tipo penal específico de extorsión informática crea inseguridad jurídica y resta eficacia al sistema penal, ya que obliga a forzar la interpretación del art. 185 COIP. Por lo tanto, la evolución legislativa ecuatoriana, aunque importante, aún es insuficiente para abordar la realidad actual del cibercrimen.

4.2. Dificultades probatorias y procesales en la persecución penal de la ciberextorsión

La persecución penal de la ciberextorsión en Ecuador se topa con obstáculos probatorios inherentes a la ciberextorsión. Uno de los grandes problemas es dar con el autor, pues los extorsionadores usan VPN, redes encriptadas, números virtuales o cuentas anónimas. Informes del Centro de Respuesta a Incidentes Informáticos (CSIRT-Ecuador)[59] y de la Policía Nacional indican que en la mayoría de casos denunciados entre 2021 y 2024 se aplican mecanismos de anonimización que imposibilitan identificar el origen verdadero de la comunicación, perjudicando la imputación penal.

[58] Asamblea Nacional del Ecuador. Ley Orgánica de Protección de Datos Personales. Registro Oficial Suplemento 459, Quito, 2021.
[59] CSIRT-Ecuador. Boletín Anual de Incidentes Cibernéticos 2021–2024. Ministerio de Telecomunicaciones y de la Sociedad de la Información, Quito, 2024.

Un segundo reto es la conservación de evidencia digital. La Fiscalía General del Estado reconoce en sus Lineamientos para el Manejo de Evidencia Digital[60] que no existen protocolos estandarizados para la recolección, preservación y análisis de datos digitales. Esto crea lagunas en la cadena de custodia de archivos, metadatos y capturas de pantalla, evidencia crucial para probar la amenaza o la extorsión. La falta de estándares unificados hace que la validez procesal quede supeditada al criterio del fiscal o el perito de turno.

También existen restricciones en la cadena de custodia digital. Si bien el COIP y el Código Orgánico de Procesos señalan normas generales de integridad para la evidencia, los delitos informáticos exigen procedimientos específicos: hash de verificación, duplicación forense, registro de logs. Las guías del NIST (National Institute of Standards and Technology) y del Convenio de Budapest las recomiendan, pero en Ecuador no se aplican de manera uniforme, sobre todo en las fiscalías provinciales donde no cuentan con personal capacitado en informática forense.

En el plano procesal, otra barrera es la colaboración con proveedores de servicios digitales cuyos servidores se localizan en el extranjero. Para acceder a información de cuentas, direcciones IP o historiales de mensajes se necesita ayuda legal internacional, la cual puede tardar meses. La misma Fiscalía ha reconocido que esta dilación perjudica la eficacia de la investigación, ya que muchas huellas se borran automáticamente debido a las políticas de privacidad de plataformas como Meta, Google o Telegram.

Además, la ciberextorsión enfrenta dificultades en la prueba ante tribunales, ya que jueces y fiscales no siempre coinciden en la autenticidad de archivos digitales. Investigaciones

[60] Fiscalía General del Estado. Lineamientos para el Manejo de Evidencia Digital. Quito, 2022.

académicas de López et al[61] advierten que, sin un protocolo nacional unificado, la valoración probatoria queda en manos de interpretaciones subjetivas que comprometen la seguridad jurídica y abren la puerta a nulidades en la fase de juicio.

4.3. Valoración de la necesidad de un tipo penal autónomo para la ciberextorsión en Ecuador

Los estudios doctrinales y normativos muestran que el art. 185 del COIP no tipifica las características técnicas y operativas de la ciberextorsión. Este descubrimiento es importante porque, si bien en la práctica la Fiscalía tipifica estos comportamientos como extorsión tradicional, la doctrina nacional y los estudios institucionales[62] coinciden en que la forma digital agrega elementos distintivos como anonimización, uso de plataformas encriptadas, amenazas automatizadas que el legislador no anticipó en 2014. Esta distancia entre ley y crimen nos muestra que existe un vacío legal que afecta la subsunción típica.

La comparación con tendencias internacionales confirma esta conclusión. En códigos penales como el de Colombia, Chile o España se han introducido agravantes o subtipos que expresamente tipifican como delito el uso de tecnologías para cometer delitos, lo que permite definir mejor los elementos objetivos del injusto. En Ecuador, en cambio, los

[61] LÓPEZ SORIA, Y.; SÁNCHEZ OVIEDO, D. X.; CAJAS PÉREZ, J. L. y ORTIZ CRIOLLO, O. C., "La culpabilidad prescindible como elemento en la estructura del delito", en Revista Universidad y Sociedad, vol. 14, núm. 6, 2022, pp. 278–289, disponible en: http://scielo.sld.cu/pdf/rus/v14n6/2218-3620-rus-14-06-278.pdf

[62] HERRERA, Santiago y MASAPANTA, Cristian, El papel de la prueba digital en los procedimientos penales en Ecuador, Universidad Andina Simón Bolívar, Quito, 2025, disponible en: https://repositorio.uasb.edu.ec/bitstream/10644/10524/1/T4605-MDPE-Herrera-El%20papel.pdf

informes del MINTEL[63] y del CSIRT-Ecuador[64] registran un aumento constante de extorsiones cibernéticas desde 2021, sobre todo por redes sociales, sin que haya una reacción normativa en el mismo sentido. Esta diferencia que se evidencia en el análisis nos muestra que la ausencia de un subtipo propio no solo es una carencia legislativa, sino que incide en la prevención, persecución y sanción de este fenómeno.

Desde una perspectiva procesal, los operadores jurídicos tienen problemas para imputar la conducta de manera consistente por la falta de un marco legal explícito. La Fiscalía ya ha alertado de que casos similares se califican de forma diferente en función de la provincia o el fiscal de turno, lo que crea un riesgo para la seguridad jurídica. Y esto importa porque demuestra que la vaguedad común no es un problema teórico, sino algo que afecta el debido proceso y la igualdad ante la ley. En un momento de debate, esto puede defender que un subtipo autónomo disminuiría la variabilidad interpretativa y aumentaría la uniformidad procesal.

La evaluación conjunta del fenómeno muestra que la ciberextorsión es un delito híbrido extorsión, fraude informático, tratamiento ilegal de datos, uso de herramientas de anonimato que no puede ser encajado en un único precepto general. Los delitos informáticos del COIP (arts. 230-233) tampoco lo hacen, porque tipifican daños técnicos a sistemas o datos. La dispersión normativa que se verificó en el análisis evidencia que el tratamiento penal hoy en día se mueve por analogía y acumulación de tipos, en desmedro de la eficacia de la persecución penal. Este descubrimiento refuerza la discusión doctrinal

[63] Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL). Reporte de Ciberdelincuencia en Ecuador 2021–2023. Quito, 2023.
[64] **CSIRT-Ecuador.** *Boletín Anual de Incidentes Cibernéticos 2021–2024.* Quito, 2024.

de avanzar hacia una tipificación autónoma, acorde al Convenio de Budapest y la tendencia legislativa comparada de crear una ley específica de ciberdelincuencia.

4.4. Implicaciones del vacío normativo en la seguridad jurídica, el debido proceso y la eficacia de la persecución penal

El análisis normativo evidenció que la ausencia de un tipo penal autónomo de ciberextorsión crea un vacío que atenta contra la seguridad jurídica, ya que obliga a los operadores jurídicos a realizar una interpretación extensiva del art. 185 del COIP. Esta dispersión se manifiesta en posiciones encontradas entre fiscales, algo ya avisado en el Informe de Directrices para la actuación fiscal en delitos informáticos de la Fiscalía General del Estado, al reconocer que la redacción actual no cubre las formas de comisión digital[65]. Esta verificación refuerza la alerta doctrinal de Cevallos Vallejo[66] que indica que el principio de legalidad se vulnera cuando el tipo penal no se ajusta a la realidad tecnológica del delito.

La revisión judicial constató que el vacío legal impacta también el debido proceso, específicamente en la imputación. Según informes institucionales revisados, la falta de una descripción típica unívoca genera disparidad en la calificación jurídica entre provincias para casos similares. Lo anterior se alinea con lo indicado por Román y Chimborazo que advierten sobre la pérdida de previsibilidad penal cuando el legislador

[65] Fiscalía General del Estado. Informe Anual de Gestión 2022. Quito, 2022.
[66] CEVALLOS VALLEJO, Juan Nicolás, "Compatibilidad de los delitos de infracción de deber con el Código Orgánico Integral Penal", en USFQ Law Working Papers, 2023/05, disponible en: https://ssrn.com/abstract=4461614 (consultado 15/11/2025).

no internaliza las particularidades del mundo digital[67]. En el debate, estos datos revelan que el asunto no es técnico, sino que se adentra en garantías constitucionales fundamentales.

Otro hallazgo importante es el efecto sobre la eficacia de la persecución penal. Datos del CSIRT-Ecuador muestran que entre 2021 y 2024 la ciberextorsión fue uno de los incidentes más notificados, pero menos judicializados por problemas de identificación y falta de criterios probatorios unificados (CSIRT-Ecuador, 2023; 2024). La Policía Nacional también ha informado que la mayoría de los casos utilizan VPN y plataformas encriptadas para permanecer en el anonimato, lo que dificulta las investigaciones[68]. Estos resultados confirman que el vacío legal no solo influye en la tipificación, sino que compromete la capacidad del sistema penal para dar respuesta a un delito en auge.

Además, la dispersión normativa entre el art. 185 del COIP y los delitos informáticos de los arts. 230-233 dificulta construir una teoría del caso articulada. Las guías forenses NIST SP 800-101r1, de referencia en capacitaciones de cuerpos policiales, indican que delitos que involucran ingeniería social, anonimato y manipulación de datos necesitan marcos tipológicos para definir caminos probatorios repetibles[69]. El vacío encontrado en el análisis evidencia que Ecuador carece de esa coherencia sistemática y que por eso se dan exclusiones de prueba o decisiones contradictorias entre jueces.

[67] ROMÁN-NARANJO, J. A. y CHIMBORAZO-CASTILLO, L. A., "La falsedad material e ideológica de títulos ejecutivos: análisis comparado entre Ecuador y Chile", en Portal de la Ciencia, vol. 6, suplemento 1, 2025, pp. 22–36, doi: https://doi.org/10.51247/pdlc.v6iS1.604.
[68] Policía Nacional del Ecuador. Informe Técnico sobre Denuncias de Extorsión Digital 2021–2024. Dirección Nacional de Investigación de Delitos Tecnológicos, Quito, 2024.
[69] National Institute of Standards and Technology (NIST), NIST Special Publication 800-101: Guidelines on Mobile Device Forensics, Maryland, 2014.

La conversación deja ver que la ausencia de un subtipo autónomo también restringe la colaboración internacional, tan necesaria en delitos cometidos a través de plataformas cuyas infraestructuras se encuentran en el extranjero. El Convenio de Budapest crea normas de conservación de datos y cooperación internacional que exigen definiciones comunes[70]. Al compararlos con los estándares ecuatorianos, se puede notar que la falta de tipificación deja al país en desventaja para exigir una asistencia eficaz y de protección a las víctimas y la acción penal estatal.

5. Conclusiones

La revisión doctrinal y normativa permitió determinar que la legislación ecuatoriana en materia de delitos informáticos ha ido evolucionando, pero sin una política criminal integral que tutele la complejidad del ciberespacio. Si bien el COIP tipificó ciertas figuras a partir del año 2014, estas son incompletas y no logran dar respuesta a la realidad actual del cibercrimen. La doctrina patria coincide en que esta evolución incompleta crea lagunas interpretativas que impactan la aplicación del derecho penal ante figuras como la ciberextorsión.

El estudio mostró que la persecución penal de la ciberextorsión se enfrenta a grandes desafíos probatorios y procesales, entre las principales barreras se incluyen la imposibilidad de reconocer autores por el uso de herramientas de anonimización, la ausencia de protocolos estandarizados para la conservación y autenticación de evidencia digital y la dificultad de cooperación internacional para conseguir registros de

[70] Consejo de Europa, Convenio de Budapest sobre Ciberdelincuencia, Budapest, 2001.

plataformas localizadas en el extranjero. Estos obstáculos disminuyen la eficacia de la investigación, contaminan la evidencia y abren la puerta a violaciones del debido proceso.

El estudio permitió concluir que la creación de un tipo penal autónomo de ciberextorsión es necesaria y jurídicamente justificada. La figura actual de extorsión prevista en el COIP no recoge las particularidades técnicas, operativas y transnacionales del delito cuando se ejecuta mediante tecnologías digitales. Esta insuficiencia normativa afecta la seguridad jurídica, aumenta la discrecionalidad interpretativa y limita la eficacia de la persecución penal, un subtipo específico permitiría delimitar con precisión los elementos objetivos y subjetivos del injusto, fortalecer la coherencia del sistema penal y mejorar la respuesta estatal frente a esta modalidad delictiva en expansión.

6. Recomendaciones

- Incorporar un tipo penal autónomo de ciberextorsión que defina sus elementos digitales y se coordine con los delitos informáticos del COIP, disminuyendo la discrecionalidad interpretativa.
- Establecer un protocolo nacional de evidencia digital que estandarice los procedimientos de preservación, autenticación y cadena de custodia, en línea con estándares internacionales como el Convenio de Budapest y el NIST.
- Fortalecer la capacitación especializada en ciberdelincuencia, rastreo digital y evaluación de pruebas para asegurar
- Aplicar criterios consistentes para la admisión y valoración de evidencia digital, con énfasis en la integridad técnica y el uso de herramientas forenses verificables.

- Promover canales más rápidos de cooperación internacional para acceder a datos almacenados en servidores extranjeros, fortaleciendo la capacidad de respuesta en casos de ciberextorsión.

7. Bibliografía

BRANDON, Andrés; MARFETAN, Valeria y MACHADO, Marco, "Evidencias Deepfake en sistema penal ecuatoriano: reconocimiento, autenticidad y aceptación probatoria en juicios", en *Verdad y Derecho. Revista Arbitrada de Ciencias Jurídicas y Sociales*, vol. 4, 2025, pp. 325–343, doi: https://doi.org/10.62574/r083dh53.

ORDOÑEZ, Luis, "El Marco Legal de los Delitos Cibernéticos en Ecuador", en *Reincisol*, vol. 5, núm. 3, 2024, pp. 1447–1469, doi: https://doi.org/10.59282/reincisol.V3(5)1447-1469.

QUEZADA, Andrea y GENDA, Carlos, "Delito de Ciberextorsión: un análisis jurídico y comparativo en países de Latinoamérica, Perú, Colombia y Ecuador", en *Digital Publisher CEIT*, vol. 10, núm. 1, 2025, pp. 546–556, doi: https://doi.org/10.33386/593dp.2025.1.2893.

SARMIENTO, Juan y MALDONADO, Laura, "Delitos informáticos y ciberataques: análisis jurídico en el derecho penal del Ecuador", en *MQRInvestigar*, vol. 8, núm. 3, 2024, pp. 1753–1781, doi: https://doi.org/10.56048/MQR20225.8.3.2024.1753-1781.

OBSERVATORIO ECUATORIANO DE CRIMEN ORGANIZADO (OECO), *Tipologías y resultados de la Encuesta Nacional de Victimización de Casos de Extorsión Empresarial*, Quito, 2024, disponible en:

https://oeco.padf.org/wp-content/uploads/2024/05/OECO_Radiografia-de-la-extorsion-en-Ecuador-1.pdf

HERRERA, Santiago y MASAPANTA, Cristian, *El papel de la prueba digital en los procedimientos penales en Ecuador*, Universidad Andina Simón Bolívar, Quito, 2025, disponible en: https://repositorio.uasb.edu.ec/bitstream/10644/10524/1/T4605-MDPE-Herrera-El%20papel.pdf

Consejo de Europa, *Convenio de Budapest sobre Ciberdelincuencia*, Budapest, 2001.

Código Orgánico Integral Penal, 10 de febrero de 2014 (Registro Oficial Suplemento 180, 10 de febrero de 2014).

LÓPEZ SORIA, Y.; SÁNCHEZ OVIEDO, D. X.; CAJAS PÉREZ, J. L. y ORTIZ CRIOLLO, O. C., "La culpabilidad prescindible como elemento en la estructura del delito", en *Revista Universidad y Sociedad*, vol. 14, núm. 6, 2022, pp. 278–289, disponible en: http://scielo.sld.cu/pdf/rus/v14n6/2218-3620-rus-14-06-278.pdf

GRANJA ZURITA, D. F.; ABAD TANDAZO, M. H.; PAREDES LÓPEZ, J. A. y REY SIQUILANDA, C. F., "La ausencia del error en el Código Orgánico Integral Penal en la conducta delictiva del procesado en Ecuador", en *Universidad y Sociedad*, vol. 14, suplemento 4, 2022, pp. 59–69, disponible en: https://rus.ucf.edu.cu/index.php/rus/article/view/3112

BASTIDAS GONZÁLEZ, K. A., "El delito en el derecho penal: construcción jurídica y retos contemporáneos", en *Sapiens Evolución Científica*, vol. 2, núm. 1, 2024, e-21004, disponible en: https://sapiensjournal.org/index.php/sec/article/view/28

IZQUIERDO MORILLAS, M., "Desentrañando el delito: un viaje por las principales teorías dogmáticas y los retos actuales", en *Revista Estudios Jurídicos. Segunda Época*, núm. 24, 2024, e8909, doi: https://doi.org/10.17561/rej.n24.8909

ROMERO ESTÉVEZ, I. M., "Aplicabilidad de la teoría de la imputación objetiva en los delitos culposos del COIP", en *Revista Lex*, vol. 7, núm. 27, 2024, pp. 1546–1562, doi: https://doi.org/10.33996/revistalex.v7i27.261

BECERRA, J. y GOICOCHEA, W., "Razones jurídicas para incorporar la autopuesta en peligro de la víctima como causa de disminución de punibilidad en los delitos culposos", 2020, disponible en: https://lc.cx/M2Pv67

ORGANIZACIÓN INTERNACIONAL DE NORMALIZACIÓN (ISO/IEC), *ISO/IEC 27037: Directrices para la identificación, recolección y preservación de evidencia digital*, Ginebra, 2012.

ORGANIZACIÓN INTERNACIONAL DE NORMALIZACIÓN (ISO/IEC), *ISO/IEC 27041: Guidance on assuring suitability and adequacy of incident investigative methods*, Ginebra, 2015.

ENISA — EUROPEAN UNION AGENCY FOR CYBERSECURITY, *Digital Forensics — Guidelines for Evidence Acquisition*, Heraklion, 2019.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST), *NIST Special Publication 800-101: Guidelines on Mobile Device Forensics*, Maryland, 2014.

ROMÁN-NARANJO, J. A. y CHIMBORAZO-CASTILLO, L. A., "La falsedad material e ideológica de títulos ejecutivos: análisis comparado entre Ecuador y Chile", en

Portal de la Ciencia, vol. 6, suplemento 1, 2025, pp. 22–36, doi: https://doi.org/10.51247/pdlc.v6iS1.604.

CEVALLOS VALLEJO, Juan Nicolás, "Compatibilidad de los delitos de infracción de deber con el Código Orgánico Integral Penal", en *USFQ Law Working Papers*, 2023/05, disponible en: https://ssrn.com/abstract=4461614 (consultado 15/11/2025).

SANTANDER, Y., "El elemento subjetivo en la responsabilidad del superior por crímenes de derecho penal internacional", en *Boletín Mexicano de Derecho Comparado*, vol. 57, núm. 171, 2024, pp. 239–273.

SILVA SÁNCHEZ, Jesús-María, *La expansión del Derecho penal: aspectos de la política criminal en las sociedades postindustriales*, Civitas, Madrid, 2006.

ORGANIZACIÓN DE LOS ESTADOS AMERICANOS (OEA), *Propuesta de Protocolo Hemisférico contra el Ciberdelito*, Secretaría de Seguridad Multidimensional, Washington D. C., 2016, disponible en: https://www.oas.org/es/sms/cyber/ (consultado 15/11/2025).

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST), *NIST Special Publication 800-86: Guide to Integrating Forensic Techniques into Incident Response*, U.S. Department of Commerce, Maryland, 2006, doi: https://doi.org/10.6028/NIST.SP.800-86.

ENISA — EUROPEAN UNION AGENCY FOR CYBERSECURITY, *Digital Forensics Guidelines: Identification, Collection, Acquisition and Preservation of Digital Evidence*, Heraklion, 2021, disponible en: https://www.enisa.europa.eu/publications/digital-forensics (consultado 15/11/2025).

BALLESTERO, Fernando, "Cómo mejorar la ciberseguridad en España: pasos ante una gran oportunidad", en *Boletín Económico de ICE*, núm. 3148, 2022, pp. 35–49.

Organización Internacional de Normalización (ISO/IEC), *ISO/IEC 27037: Directrices para la identificación, recolección y preservación de evidencia digital*, Ginebra, 2012.

ORGANIZACIÓN INTERNACIONAL DE NORMALIZACIÓN (ISO/IEC), *ISO/IEC 27041: Guía para asegurar la idoneidad y adecuación de los métodos de investigación de incidentes*, Ginebra, 2015.

ORGANIZACIÓN INTERNACIONAL DE NORMALIZACIÓN (ISO/IEC), ISO/IEC 27042: Directrices para el análisis e interpretación de evidencia digital, Ginebra, 2015.

ORGANIZACIÓN INTERNACIONAL DE NORMALIZACIÓN (ISO/IEC), ISO/IEC 27001: Sistemas de Gestión de Seguridad de la Información (SGSI), Ginebra, 2013.

CORTE CONSTITUCIONAL DEL ECUADOR. *Sentencia 1406-17-EP/22: Acción extraordinaria de protección respecto del archivo de denuncia penal por extorsión.* Quito, 2022. https://buscador.corteconstitucional.gob.ec/buscador-externo/principal/fichaSentencia?numero=1406-17-EP%2F22

CORTE CONSTITUCIONAL DEL ECUADOR. Dictamen 3-25-EE/25: Control de constitucionalidad del estado de excepción declarado mediante Decreto Ejecutivo 599. Quito, 2025.

ASAMBLEA NACIONAL DEL ECUADOR. *Ley Orgánica de Protección de Datos Personales.* Registro Oficial Suplemento 459, Quito, 2021.

Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL). Reporte de Ciberdelincuencia en Ecuador 2021–2023. Quito, 2023.

CSIRT-ECUADOR. *Boletín Anual de Incidentes Cibernéticos 2021–2024.* Quito, 2024.

CSIRT-ECUADOR. *Boletín Anual de Incidentes Cibernéticos 2021–2024.* Ministerio de Telecomunicaciones y de la Sociedad de la Información, Quito, 2024.

POLICÍA NACIONAL DEL ECUADOR. *Informe Técnico sobre Denuncias de Extorsión Digital 2021–2024.* Dirección Nacional de Investigación de Delitos Tecnológicos, Quito, 2024.

FISCALÍA GENERAL DEL ESTADO. *Lineamientos para el Manejo de Evidencia Digital.* Quito, 2022.