

INSTRUMENTO TÉCNICO DE POLÍTICA CRIMINAL - CIBERDELINCUENCIA

FISCALÍA GENERAL DEL ESTADO

COORDINACIÓN GENERAL DE
GESTIÓN DEL CONOCIMIENTO

DIRECCIÓN DE POLÍTICA CRIMINAL
2026

FGE

FISCALÍA GENERAL DEL ESTADO
Ecuador

Instrumento Técnico de Política Criminal - Ciberdelincuencia	3
1. Introducción.....	3
2. Antecedentes.....	5
3. Derecho penal sustantivo aplicable a la Ciberdelincuencia.....	7
3.1. Clasificación de la ciberdelincuencia según el Convenio de Budapest.....	7
3.1.1. Delitos contra la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos	7
3.1.2. Delitos informáticos de carácter patrimonial y falsificación informática	8
3.1.3. Delitos relativos con el contenido	8
3.1.4. Delitos relativos con infracciones de la propiedad intelectual y de derechos afines.....	8
3.2. Correspondencia en el Código Orgánico Integral Penal.....	9
3.2.1. Delitos contra la confidencialidad, integridad y disponibilidad de datos y sistemas	9
3.2.2. Delitos informáticos de carácter patrimonial y falsificación informática	11
3.2.3. Delitos relativos con el contenido	12
3.2.4. Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines.....	23
4. Contenido Digital.....	25
4.1. Características del contenido digital.....	26
4.2. Manejo de evidencia en referencia al contenido digital	28
5. Cooperación internacional en materia de ciberdelincuencia.	31
6. Conclusiones.....	40
Bibliografía	43

Instrumento Técnico de Política Criminal – Ciberdelincuencia [1]

1. Introducción

La acelerada digitalización de la vida social, económica e institucional ha transformado de manera profunda las formas de interacción entre las personas y el Estado. Las tecnologías de la información y comunicación se han convertido en un espacio indispensable para el ejercicio de derechos, la conformación de la opinión pública, la prestación de servicios y la circulación de bienes y datos. En el ordenamiento jurídico ecuatoriano, esta centralidad de las tecnologías de la información y comunicación encuentra reconocimiento expreso en el artículo 16 de la Constitución de la República, que garantiza a todas las personas, de manera individual o colectiva, el derecho a una comunicación libre, intercultural, incluyente, diversa y participativa, así como el acceso universal a las tecnologías de la información y comunicación.¹ Este mandato constitucional impone al Estado no solo la obligación de promover el acceso, sino también la de proteger a las personas frente a los riesgos y vulneraciones de derechos que se materializan en el entorno digital².

En este contexto, la Fiscalía General del Estado, a través de la Dirección de Política Criminal, elabora la presente política criminal de Ciberdelincuencia como instrumento técnico de orientación para la investigación, formulación de cargos, acusación y demás actuaciones fiscales frente a las infracciones penales cometidas mediante o contra sistemas informáticos, redes y datos. Este instrumento se sustenta en el modelo de Estado constitucional de derechos y justicia y en la función de la política criminal de armonizar la protección eficaz de los bienes jurídicos con el respeto estricto a los derechos y garantías de las personas sometidas al sistema penal.

El Código Orgánico Integral Penal fija como finalidad de la legislación penal la regulación del poder punitivo del Estado, la tipificación de las infracciones y la garantía del debido proceso, orientando la respuesta penal hacia la rehabilitación y la reparación integral de las víctimas³. Asimismo, reconoce que la intervención penal es de última ratio y debe adecuarse a los estándares constitucionales y a los compromisos internacionales asumidos por el Ecuador, incorporando nuevas conductas penalmente relevantes derivadas, entre otros factores, del desarrollo tecnológico y de las obligaciones internacionales en materia de criminalidad moderna. Esta Política Criminal de Ciberdelincuencia se concibe como desarrollo operativo de

¹ Ecuador, *Constitución de la República del Ecuador*, Registro Oficial 44, 20 de octubre de 2008, art. 16.

² Ecuador, *Constitución de la República del Ecuador*, art. 16.

³ Ecuador, *Código Orgánico Integral Penal*, Registro Oficial 180, Suplemento, 10 de febrero del 2014, art. 1.

tales principios, proporcionando criterios para la interpretación de los tipos penales informáticos y la determinación de la imputación objetiva y subjetiva.

En el plano internacional, el Ecuador es Estado Parte del Convenio sobre la Ciberdelincuencia del Consejo de Europa (Convenio de Budapest)⁴, que establece un marco especializado para la criminalización de conductas contra la confidencialidad, integridad y disponibilidad de los sistemas y datos informáticos, los delitos informáticos tradicionales y los mecanismos de cooperación internacional en la obtención de evidencia digital. Este instrumento, junto con sus protocolos adicionales, constituye la referencia técnica principal para la armonización legislativa y procesal en materia de ciberdelitos, y exige a las autoridades nacionales entre ellas la Fiscalía General del Estado, contar con lineamientos claros para la investigación de este tipo de infracciones penales.

Finalmente, la aprobación de la Convención de las Naciones Unidas sobre Ciberdelincuencia de 2024, establece un nuevo estándar global en la lucha contra la criminalidad en el ciberespacio, fortaleciendo la cooperación entre Estados, la asistencia judicial recíproca y los mecanismos de prevención, con especial énfasis en la protección de víctimas y en la salvaguarda de los derechos fundamentales en entornos digitales⁵. Si bien el Ecuador aún no es Estado Parte de dicho instrumento, la presente Política Criminal de Ciberdelincuencia se limita a reconocer la Convención de las Naciones Unidas contra la Ciberdelincuencia como un referente internacional en la materia, sin asumirla todavía como marco normativo de actuación, porque a la fecha de este instrumento aún no está en vigor. En consecuencia, los lineamientos de persecución penal, cooperación internacional y determinación de jurisdicción y competencia en materia de ciberdelincuencia continúan estructurándose, principalmente, a partir del Convenio de Budapest y de los estándares actualmente vigentes, sin perjuicio de que, en el futuro, la Fiscalía General del Estado adecúe estos criterios e incorpore nuevos parámetros en función de las obligaciones que el Estado ecuatoriano llegue a asumir en el marco de dicho instrumento internacional.

Con base en estos pilares, la Constitución de la República del Ecuador, el Código Orgánico Integral Penal, el Convenio de Budapest y la Convención de Naciones Unidas sobre Ciberdelincuencia, la Fiscalía General del Estado establece un marco de política criminal

⁴ Consejo de Europa, Convenio sobre la Ciberdelincuencia, *Suplemento, Registro Oficial Nro. 13*.

⁵ Naciones Unidas, Asamblea General, Convención de las Naciones Unidas contra la Ciberdelincuencia, *Resolución 79/243*, 24 de diciembre de 2024.

especializado que permita enfrentar de manera eficaz, coherente y respetuosa de los derechos humanos, las nuevas formas de criminalidad asociadas al uso de las tecnologías de la información y comunicación, garantizando al mismo tiempo la vigencia real del derecho de acceso y uso seguro de las tecnologías de la información y comunicación reconocido en el artículo 16 de la Constitución de la República del Ecuador⁶.

2. Antecedentes

El Convenio sobre Ciberdelincuencia del Consejo de Europa (Convenio de Budapest)⁷, se erige como el primer instrumento multilateral de referencia en materia de criminalidad informática en el mundo. Su parte de derecho penal sustantivo se organiza en cuatro grandes ejes: 1.- los delitos contra la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos; 2.- los delitos informáticos de carácter patrimonial (fraude informático) y falsificación informática; 3.- las infracciones vinculadas a contenidos ilícitos (pornografía infantil), y, 4.- los delitos relativos con infracciones de la propiedad intelectual y de los derechos afines.⁸ Estos ejes han marcado el estándar mínimo que los Estados deben incorporar en su legislación penal interna para responder a los riesgos propios del ciberespacio.

En el Ecuador, la entrada en vigencia del Código Orgánico Integral Penal⁹, en el año 2014 supuso la sistematización de un catálogo de infracciones penales que, de forma progresiva, ha ido incorporando los lineamientos del Convenio de Budapest en materia sustantiva. Dentro del título referido a los delitos contra la seguridad de los activos de los sistemas de información y comunicación, tipificado en el capítulo tercero, sección tercera del Código Orgánico Integral Penal; así como en otros capítulos relativos a la protección de los derechos a la propiedad, de la integridad sexual y reproductiva, y los derechos a la propiedad intelectual y derechos de autor.

El Código Orgánico Integral Penal, tipifica conductas que ponen en peligro y lesionan la confidencialidad, integridad y disponibilidad de los datos y sistemas, fraudes y falsificaciones cometidas mediante herramientas informáticas, y diversas formas de criminalidad que se sirven de las tecnologías de la información y comunicación como medio, ámbito o instrumento.

⁶ Ecuador, *Constitución de la República del Ecuador*, art. 16, núm. 2.

⁷ Consejo de Europa, *Convenio sobre la Ciberdelincuencia*.

⁸ Consejo de Europa, *Convenio sobre la Ciberdelincuencia*.

⁹ Ecuador, *Código Orgánico Integral Penal*, Capítulo tercero, Sección tercera.

La reforma al Código Orgánico Integral Penal de 2021¹⁰, profundizó este proceso de adecuación normativa al actualizar el capítulo de delitos contra la seguridad de los activos de los sistemas de información y comunicación. En dicha reforma se incorporaron definiciones legales específicas para facilitar la comprensión y aplicación de estas figuras (tales como contenido digital, sistema informático, proveedor de servicios, entre otras), se fortaleció el régimen de responsabilidad penal de las personas jurídicas en este ámbito, se introdujeron reglas de agravación de las penas cuando la comisión del delito perturba de forma grave o duradera a un sistema informático que apoye una actividad destinada a asegurar funciones sociales críticas, y se tipificó el delito de falsificación informática¹¹.

De igual manera, se ajustaron y ampliaron diversos tipos penales de carácter sexual en los que la utilización de tecnologías de la información y comunicación resulta central para su cometimiento.

En el plano institucional, mediante Resolución No. 034-FGE-2022 de 08 de junio del 2022¹², la Fiscalía General del Estado creó la Unidad Nacional Especializada en Investigación de Ciberdelito, con sede en la ciudad de Quito y competencia a nivel nacional, asignándole la investigación de los delitos previstos en el Código Orgánico Integral Penal, entre los cuales se encuentran: revelación ilegal de base de datos, interceptación ilegal de datos, transferencia electrónica de activo patrimonial (aplica primer inciso del artículo 231 ibídem), ataque a la integridad de sistemas informáticos, delitos contra la información pública reservada legalmente y acceso no consentido a un sistema informático, telemático o de telecomunicaciones. La resolución definió, además, las atribuciones de la Unidad, su estructura básica y la coordinación con otras dependencias de la institución.

Con posterioridad, la Resolución No. 003-FGE-2023¹³, de 16 de enero del 2023, reformó la Resolución No. 034-FGE-2022, precisando el alcance de las competencias de la Unidad Nacional Especializada en Investigación de Ciberdelito y estableciendo reglas específicas para la asignación de las noticias del delito y de los expedientes fiscales a dicha Unidad. Se añadieron otros delitos a parte de los incorporados en la resolución No. 034-FGE-2022, dentro

¹⁰ Ecuador, *Ley Orgánica Reformatoria al Código Orgánico Integral Penal para prevenir y combatir la violencia sexual digital y fortalecer la lucha contra delitos informáticos*, Registro Oficial 526, Cuarto Suplemento, 30 de agosto de 2021.

¹¹ Ecuador, *Código Orgánico Integral Penal*, art. 234.1 y 324.2

¹² Ecuador, Fiscalía General del Estado, *Unidad Nacional Especializada en Investigación de Ciberdelito*. Resolución Nro. 34 – FGE- 2022, 8 de junio del 2022.

¹³ Ecuador, Fiscalía General del Estado, *Unidad Nacional Especializada en Investigación de Ciberdelito*. Resolución Nro. 003 – FGE – 2023, 16 de enero del 2023 reforma a la Resolución Nro. 34 – FGE- 2022, 8 de junio del 2022.

de estos se incluyó: a los hechos relacionados a pornografía con utilización de niñas, niños, o adolescentes y comercialización de pornografía con utilización de niñas, niños o adolescentes; cuyos enunciados normativos se encuentran tipificados en los artículos 103 y 104 del Código Orgánico Integral Penal¹⁴. La reforma también establece reglas y procedimiento específico para la asignación de noticias del delito y expedientes a la Unidad.

En el mismo año 2023 el Código Orgánico Integral Penal¹⁵, fue reformado, incorporando un régimen específico de actuaciones especiales relativas a contenido digital, orientando a dotar al sistema de justicia penal de herramientas idóneas para la preservación, obtención, aseguramiento y análisis de evidencia digital. Estas disposiciones buscan armonizar la actuación fiscal y judicial con los estándares internacionales en materia de investigación de ciberdelitos, reforzando la cadena de custodia, las facultades de requerimiento y colaboración a proveedores de servicios, y las garantías para la protección de derechos fundamentales en el tratamiento de datos y comunicaciones digitales.

En conjunto, estos instrumentos normativos evidencian que la respuesta penal ecuatoriana frente a la ciberdelincuencia ha seguido una trayectoria de progresiva convergencia con los estándares establecidos por el Convenio de Budapest y por la práctica internacional, lo que sienta las bases para la formulación de una Política Criminal de Ciberdelincuencia que articule de manera coherente la investigación y juzgamiento de estas infracciones penales en el país.

3. Derecho penal sustantivo aplicable a la Ciberdelincuencia

3.1. Clasificación de la ciberdelincuencia según el Convenio de Budapest

El Convenio sobre Ciberdelincuencia del Consejo de Europa (Budapest, 2001)¹⁶ constituye el principal referente internacional en materia de criminalidad informática. En su parte de derecho penal sustantivo, estructura la respuesta penal en cuatro grandes bloques de infracciones, que funcionan como una matriz mínima de armonización legislativa:

3.1.1. Delitos contra la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos

Comprenden el acceso ilícito a sistemas informáticos, la interceptación ilícita de datos, el ataque a la integridad de los datos (alteración, daño o supresión), el ataque a la integridad de

¹⁴ Ecuador, *Código Orgánico Integral Penal*, art. 103 y 104.

¹⁵ Ecuador, *Ley Orgánica Reformatoria a Varios Cuerpos Legales para el Fortalecimiento de las Capacidades Institucionales y la Seguridad Integral*, Registro Oficial 279, Suplemento, 29 de marzo de 2023.

¹⁶ Consejo de Europa, Convenio sobre la Ciberdelincuencia, *Suplemento, Registro Oficial Nro. 13*.

los sistemas y la utilización indebida de dispositivos, contraseñas o herramientas informáticas diseñadas para la comisión de estas conductas¹⁷.

3.1.2. Delitos informáticos de carácter patrimonial y falsificación informática

La falsificación informática¹⁸, que obliga a los Estados a sancionar la introducción, alteración, borrado o supresión deliberada e ilegítima de datos informáticos con el fin de generar datos no auténticos que sean utilizados o considerados como auténticos para producir efectos jurídicos; y el fraude informático¹⁹, que exige criminalizar los actos deliberados e ilegítimos que causan un perjuicio patrimonial mediante la manipulación de datos (introducción, alteración, borrado o supresión) o cualquier interferencia en el funcionamiento de un sistema informático, cuando se actúa con la intención de obtener un beneficio económico ilegítimo para sí o para un tercero.

3.1.3. Delitos relativos con el contenido

Dentro de este acápite se encuentran, el delito la producción de pornografía infantil con intención de difundirla a través de un sistema informático, así como su oferta, puesta a disposición, difusión, transmisión, adquisición para sí o para otros y posesión cuando el material se almacena en un sistema informático o en un dispositivo de almacenamiento de datos²⁰. A efectos de este instrumento internacional, se entiende por *pornografía infantil* todo material pornográfico que contenga la representación visual de un menor en comportamiento sexualmente explícito, de una persona que parezca menor en ese tipo de comportamiento o de imágenes realistas que representen a un menor en tal conducta²¹. El referido instrumento establece que por menor se entenderá a toda persona menor de 18 años, aunque los Estados pueden fijar un umbral inferior que no sea menor a los 16 años²².

3.1.4. Delitos relativos con infracciones de la propiedad intelectual y de derechos afines

En este apartado se encuentran las infracciones a los derechos de propiedad intelectual y a los derechos afines, siempre que tales infracciones se cometan de manera deliberada, a escala comercial y por medio de un sistema informático²³.

¹⁷ Consejo de Europa, Convenio sobre la Ciberdelincuencia, arts. 2, 3, 4, 5 y 6.

¹⁸ Consejo de Europa, Convenio sobre la Ciberdelincuencia, art.7.

¹⁹ Consejo de Europa, Convenio sobre la Ciberdelincuencia, art.8.

²⁰ Consejo de Europa, Convenio sobre la Ciberdelincuencia, art.9, núm. 1, lits, a, b, c, d, e.

²¹ Consejo de Europa, Convenio sobre la Ciberdelincuencia, art.9, núm. 2, lits, a, b, c.

²² Consejo de Europa, Convenio sobre la Ciberdelincuencia, art.9, núm. 3.

²³ Consejo de Europa, Convenio sobre la Ciberdelincuencia, art.10, núm. 1.

El instrumento internacional mencionado, determina que, en circunstancias bien delimitadas, un Estado pueda reservarse el derecho de no imponer responsabilidad penal por estas conductas cuando disponga de otros recursos efectivos y ello no vulnere las obligaciones internacionales que ha asumido en materia de protección de la propiedad intelectual y de los derechos afines²⁴.

3.2. Correspondencia en el Código Orgánico Integral Penal

Tomando como referencia la clasificación del Convenio de Budapest, instrumento internacional del cual el Ecuador es Estado Parte, el Código Orgánico Integral Penal articula un conjunto de tipos penales que permiten dar respuesta a las principales manifestaciones de ciberdelincuencia, tanto mediante delitos propiamente informáticos como a través de la incriminación de delitos comunes cometidos por medio de tecnologías de la información y comunicación. A continuación, se presenta un contraste sistemático entre las categorías de ciberdelincuencia previstas en el Convenio de Budapest y los delitos tipificados en el Código Orgánico Integral Penal.

3.2.1. Delitos contra la confidencialidad, integridad y disponibilidad de datos y sistemas

En correspondencia con el primer bloque del Convenio de Budapest, el Código Orgánico Integral Penal tipifica un núcleo de infracciones orientadas a proteger la confidencialidad, integridad y disponibilidad del contenido digital, de los sistemas informáticos y de las infraestructuras tecnológicas. No es casual que el capítulo respectivo se denomine “Delitos contra la seguridad de los activos de los sistemas de información y comunicación”, dentro del cual se contemplan, las siguientes conductas típicas:

Revelación ilegal de base de datos: La persona que, en provecho propio o de un tercero, revele información registrada, contenida en ficheros, archivos, bases de datos o medios semejantes, a través o dirigidas a un sistema electrónico, informático, telemático o de telecomunicaciones; materializando voluntaria e intencionalmente la violación del secreto, la intimidad y la privacidad de las personas, será sancionada con pena privativa de libertad de uno a tres años. Si esta conducta se comete por una o un servidor público, empleadas o empleados bancarios internos o de instituciones de la economía popular y solidaria que realicen intermediación financiera o contratistas, será sancionada con pena privativa de libertad de tres a cinco años.²⁵

Intercepción ilegal de datos. - Será sancionada con pena privativa de libertad de tres a cinco años: 1. La persona que, sin orden judicial previa, en provecho propio o de un tercero, intercepte, escuche, desvíe, grabe u observe, en cualquier forma, contenido digital en su origen, destino o en el interior de un sistema informático o dispositivo electrónico, una señal o una transmisión de datos o señales. 2. La persona que ilegítimamente diseñe, desarrolle, ejecute, produzca, programe o envíe contenido digital, códigos de accesos o contraseñas, certificados

²⁴ Consejo de Europa, Convenio sobre la Ciberdelincuencia, art.10, núm. 3.

²⁵ Ecuador, *Código Orgánico Integral Penal*, art. 229.

de seguridad o páginas electrónicas, enlaces o ventanas emergentes o modifique el sistema de resolución de nombres de dominio de un servicio financiero o pago electrónico u otro sitio personal o de confianza, de tal manera que induzca a una persona a ingresar a una dirección o sitio de internet diferente al que quiere acceder. 3. La persona que posea, venda, distribuya o, de cualquier otra forma, disemine o introduzca en uno o más sistemas informáticos, dispositivos electrónicos, programas u otros contenidos digitales destinados a causar lo descrito en el número anterior. 4. La persona que a través de cualquier medio copie, clone o comercialice información contenida en las bandas magnéticas, chips u otro dispositivo electrónico que esté soportada en las tarjetas de crédito, débito, pago o similares. 5. La persona que produzca, fabrique, distribuya, posea o facilite materiales, dispositivos electrónicos, o programas o sistemas informáticos destinados a la comisión del delito descrito en el inciso anterior.²⁶

Ataque a la integridad de sistemas informáticos.- La persona que destruya, dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento o comportamiento no deseado, o suprima total o parcialmente contenido digital, sistemas informáticos, sistemas de tecnologías de la información y comunicación, dispositivos electrónicos o infraestructura tecnológica necesaria para la transmisión, recepción o procesamiento de información en general, con el propósito de obstaculizar de forma grave, deliberada e ilegítima el funcionamiento de un sistema informático, será sancionada con pena privativa de libertad de tres a cinco años. Con igual pena será sancionada la persona que diseñe, desarrolle, programe, adquiera, envíe, introduzca, ejecute, venda o distribuya de cualquier manera, dispositivos, programas o sistemas informáticos maliciosos o destinados a causar los efectos señalados en el primer inciso de este artículo. Si la infracción se comete sobre bienes informáticos destinados a la prestación de un servicio público o vinculado con la seguridad ciudadana, la pena será de cinco a siete años de privación de libertad.²⁷

Delitos contra la información pública reservada legalmente. - La persona que destruya o inutilice información clasificada de conformidad con la Ley, será sancionada con pena privativa de libertad de cinco a siete años. La o el servidor público que, utilizando cualquier medio electrónico o informático, obtenga este tipo de información, será sancionado con pena privativa de libertad de tres a cinco años. Cuando se trate de información reservada, cuya revelación pueda comprometer gravemente la seguridad del Estado, la o el servidor público encargado de la custodia o utilización legítima de la información que sin la autorización correspondiente revele dicha información, será sancionado con pena privativa de libertad de siete a diez años y la inhabilitación para ejercer un cargo o función pública por seis meses, siempre que no se configure otra infracción de mayor gravedad.²⁸

Acceso no consentido a un sistema informático, telemático o de telecomunicaciones. 1. La persona que sin autorización acceda en todo o en parte a un sistema informático o sistema telemático o de telecomunicaciones o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho sobre dicho sistema, será sancionada con la pena privativa de la libertad de tres a cinco años. 2. Si la persona que accede al sistema lo hace para explotar ilegítimamente el acceso logrado, modificar un portal web, desviar o redireccionar el tráfico de datos o voz u ofrecer servicios que estos sistemas proveen a terceros, sin pagarlos a las o los proveedores de servicios legítimos, será sancionada con la pena privativa de la libertad de tres a cinco años.²⁹

En conjunto, estas figuras penales en el Código Orgánico Integral Penal establecen conductas típicas para quienes lesionan o ponen en peligro la confidencialidad, integridad y

²⁶ Ecuador, *Código Orgánico Integral Penal*, art. 230.

²⁷ Ecuador, *Código Orgánico Integral Penal*, art. 232.

²⁸ Ecuador, *Código Orgánico Integral Penal*, art. 233.

²⁹ Ecuador, *Código Orgánico Integral Penal*, art. 234.

disponibilidad de los datos y sistemas informáticos. Funcionalmente es equivalente al primer bloque de criminalidad informática previsto en el Convenio de Budapest. Este conjunto normativo establece así el núcleo duro del derecho penal sustantivo ecuatoriano en materia de ciberdelincuencia.

Sobre esta base, la doctrina ha precisado que la tutela penal de los sistemas informáticos se proyecta sobre ciertas funciones informáticas básicas, cuya afectación justifica la intervención del ius puniendi. Sobre la confidencialidad, integridad y disponibilidad ha señalado:

Tales funciones informáticas son las siguientes: a) La confiabilidad/confidencialidad, esto es, el derecho a que los datos o la información no sean divulgados y los sistemas espiados. b) La integridad, exactitud y ausencia de alteraciones ilegales de los datos, la información, los sistemas informáticos y los procesos de tratamiento de información, busca garantizar la calidad, pureza, idoneidad y corrección de estos elementos. c) La disponibilidad de los datos e infraestructuras permite garantizar su funcionamiento, administración y acceso adecuado. En otras palabras, el derecho que tienen los usuarios para que el uso y acceso a datos y sistemas informáticos se dé sin perturbaciones o inhibiciones violentas o abusivas por parte de terceros o incluso de injerencias por los mismos proveedores de servicios.³⁰

Asumir explícitamente estas tres funciones como eje dogmático permite delimitar con mayor precisión el bien jurídico “seguridad de los activos de los sistemas de información y comunicación”. Para la Fiscalía General del Estado, ello implica que la calificación jurídica, y la construcción de la teoría del caso en este primer bloque de criminalidad informática deben partir de la identificación concreta de cuál o cuáles de estas funciones, confidencialidad, integridad o disponibilidad, han sido comprometidas, y en qué medida ese menoscabo justifica una determinada respuesta penal.

3.2.2. Delitos informáticos de carácter patrimonial y falsificación informática

En coherencia con el segundo bloque del Convenio de Budapest, el Código Orgánico Integral Penal incorpora tipos penales orientados a sancionar la afectación del patrimonio mediante la manipulación de sistemas y datos informáticos, en particular el fraude informático y la falsificación informática. En este marco, y en correspondencia con las obligaciones de tipificación penal previstas en dicho instrumento, el catálogo punitivo ecuatoriano contempla, los siguientes delitos:

Transferencia electrónica de activo patrimonial. - La persona que, con ánimo de lucro, altere, manipule o modifique el funcionamiento de programa o sistema informático o telemático o mensaje de datos, para procurarse la transferencia o apropiación no consentida de un activo

³⁰ Ricardo Posada “El cibercrimen y sus efectos en la teoría de la tipicidad: de una realidad física a una realidad virtual”, Nuevo Foro Penal, Nro. 33 (2017) 72-112, ISSN 0120-8179.

patrimonial de otra persona en perjuicio de esta o de un tercero, será sancionada con pena privativa de libertad de tres a cinco años. Con igual pena, ser sancionada la persona que facilite o proporcione datos de su cuenta bancaria con la intención de obtener, recibir o captar de forma ilegítima un activo patrimonial a través de una transferencia electrónica producto de este delito para sí mismo o para otra persona.³¹

Falsificación informática: 1. La persona que, con intención de provocar un engaño en las relaciones jurídicas, introducir, modificar, o suprimir contenido digital, o interferir de cualquier otra forma en el tratamiento informático de datos, produzca datos o documentos no genuinos, será sancionada con pena privativa de libertad de tres a cinco años. 2. Quien, actuando con intención de causar un perjuicio a otro o de obtener un beneficio ilegítimo para sí o para un tercero, use un documento producido a partir de contenido digital que sea objeto de los actos referidos en el número 1, será sancionado con la misma pena.³²

Si bien en el Convenio de Budapest el fraude informático y la falsificación informática se ubican en el segundo bloque, relativo a los delitos informáticos de carácter patrimonial y de falsificación, el legislador ecuatoriano ha optado por incorporarlos en la sección tercera de delitos contra la seguridad de los activos de los sistemas de información y comunicación del Código Orgánico Integral Penal. Esta ubicación sistemática evidencia que, pese a su marcado contenido patrimonial, se privilegia la protección de la integridad, confidencialidad y disponibilidad de los sistemas y de los datos que procesan, de modo que el perjuicio económico y la desvalorización jurídica de los documentos digitales se conciben como consecuencias de ataques a la seguridad de dichos activos.

3.2.3. Delitos relativos con el contenido

Respecto del tercer bloque del Convenio de Budapest, el Código Orgánico Integral Penal recoge y desarrolla un conjunto de tipos penales que sancionan la producción y comercialización de pornografía con utilización de niñas, niños o adolescentes, mediante tecnologías de la información y comunicación, estos tipos penales, son los siguientes:

Art. 103.- Pornografía con utilización de niñas, niños o adolescentes.- La persona que fotografíe, filme, grabe, produzca, transmita o edite materiales visuales, audiovisuales, informáticos, electrónicos o de cualquier otro soporte físico o formato que contenga la representación visual de desnudos o semidesnudos reales o simulados de niñas, niños o adolescentes en actitud sexual, aunque el material tenga su origen en el extranjero o sea desconocido, será sancionada con pena privativa de libertad de trece a dieciséis años. Si la víctima, además, sufre algún tipo de discapacidad o enfermedad grave o incurable, se sancionará con pena privativa de libertad de dieciséis a diecinueve años. Cuando la persona infractora sea el padre, la madre, pariente hasta el cuarto grado de consanguinidad o segundo de afinidad, tutor, representante legal, curador o pertenezca al entorno íntimo de la familia; ministro de culto, profesor, maestro, o persona que por su profesión o actividad haya abusado de la víctima, será sancionada con pena privativa de libertad de veintidós a veintiséis años.³³

³¹ Ecuador, *Código Orgánico Integral Penal*, art. 231.

³² Ecuador, *Código Orgánico Integral Penal*, art. 234.1.

³³ Ecuador, *Código Orgánico Integral Penal*, art. 103.

En primer lugar, ambos instrumentos comparten la misma lógica: proteger a niñas, niños y adolescentes frente a la utilización de su imagen con fines sexuales, mediante la incriminación de la categoría que Budapest denomina “pornografía infantil” y que el Código Orgánico Integral Penal formula como “pornografía con utilización de niñas, niños o adolescentes”. El artículo 9 del Convenio de Budapest obliga a los Estados a tipificar, al menos, la producción, oferta o puesta a disposición, difusión o transmisión, adquisición y posesión de pornografía infantil a través de un sistema informático, mientras que el artículo 103 Código Orgánico Integral Penal sanciona a quien fotografíe, filme, grabe, produzca, transmita o edite materiales que contengan desnudos o semidesnudos de NNA en actitud sexual, cualquiera sea el soporte, incluyendo expresamente los medios informáticos. Es decir, el Código Orgánico Integral Penal no solo cubre el entorno digital, sino también los soportes analógicos o físicos, de manera más amplia que el mínimo convencional.

El Código Orgánico Integral Penal tipifica en el artículo 104 la comercialización de pornografía con utilización de niñas, niños y adolescentes, bajo el siguiente contenido típico:

Comercialización de pornografía con utilización de niñas, niños o adolescentes. - La persona que publicite, compre, posea, porte, transmita, descargue, almacene, importe, exporte o venda, por cualquier medio, para uso personal o para intercambio pornografía de niños, niñas y adolescentes, será sancionada con pena privativa de libertad de diez a trece años.³⁴

El artículo 104 de la norma penal ecuatoriana, desplaza el foco hacia la circulación y consumo del material, al tipificar la conducta de la persona que publicite, compre, posea, porte, transmita, descargue, almacene, importe, exporte o venda pornografía con utilización de niñas, niños o adolescentes, por cualquier medio, sea para uso personal o para intercambio. Con ello, el legislador nacional da cumplimiento a las obligaciones de tipificar el adquirir y poseer pornografía infantil mediante sistemas informáticos o dispositivos de almacenamiento de datos contempladas en las letras d) y e) del artículo 9.1 del Convenio de Budapest, pero nuevamente con un alcance más amplio, al no restringir la punibilidad al entorno digital, sino abarcar también la tenencia y comercio del material en soportes analógicos.

Es necesario tomar en cuenta que el Código Orgánico Integral Penal también introduce elementos que refuerzan la protección de las víctimas de estas infracciones penales. El artículo 103 incorpora agravantes específicas cuando la víctima presenta discapacidad o enfermedad grave o incurable, así como cuando el autor es el padre, la madre o pariente hasta el cuarto grado de consanguinidad o segundo de afinidad, tutor, representante legal, curador o pertenezca

³⁴ Ecuador, *Código Orgánico Integral Penal*, art. 104.

al entorno íntimo de la familia; ministro de culto, profesor, maestro, o persona que por su profesión o actividad haya abusado de la víctima; y prevé penas más severas en estos supuestos.

Estos elementos reflejan una posición político-criminal orientada a reconocer la especial vulnerabilidad de niñas, niños y adolescentes frente a estas infracciones penales tanto en el entorno físico como en el digital. Desde la perspectiva de la Fiscalía General del Estado, ello permite afirmar que, la legislación ecuatoriana cumple y en ciertos aspectos supera el estándar mínimo convencional.

Sin embargo, la constante evolución de las tecnologías de la información y comunicación plantea desafíos significativos para garantizar una protección efectiva frente a la pornografía infantil y la explotación sexual digital de NNA. Resulta necesario adecuar permanentemente el marco normativo y los criterios de persecución penal, de modo que estas categorías abarquen de forma expresa y suficiente las nuevas formas de producción, manipulación, difusión y circulación de contenidos en entornos tecnológicos, evitando vacíos de tutela o zonas de impunidad.

En esta misma línea, la respuesta penal frente a la violencia sexual en entornos digitales no se agota en los delitos de pornografía con utilización de niñas, niños o adolescentes y su comercialización. El Código Orgánico Integral Penal contempla otras figuras típicas en las que el contenido digital opera como vehículo de agresión o instrumentalización de la sexualidad, como la difusión no consentida de material íntimo, las formas de acoso o extorsión sexual mediadas por tecnologías, el contacto con fines sexuales con personas menores de edad a través de medios electrónicos y otras conductas afines, que también inciden de manera directa en la libertad e indemnidad sexual y en la intimidad de las víctimas. En los apartados siguientes se presentan de forma sistemática estas infracciones penales, a fin de integrarlas en un mismo marco de análisis sobre violencia sexual digital.

El artículo 168 Código Orgánico Integral Penal, sobre distribución de material pornográfico a niñas, niños y adolescentes, sanciona a: La persona que difunda, venda o entregue a niñas, niños o adolescentes, material pornográfico, será sancionada con pena privativa de libertad de uno a tres años.³⁵

Aunque el tipo no limita el medio de comisión, su estructura abierta permite abarcar tanto la entrega física de material como su envío o puesta a disposición mediante redes sociales, plataformas de mensajería instantánea, servicios de streaming, videojuegos en línea u otros

³⁵ Ecuador, *Código Orgánico Integral Penal*, art. 168.

entornos digitales. Desde la perspectiva de política criminal, este precepto cumple una función complementaria a los artículos 103 y 104: mientras estos se orientan a la producción y circulación del material que instrumentaliza sexualmente a NNA, el artículo 168 protege de forma directa el derecho de niñas, niños y adolescentes a no ser expuestos a contenido pornográfico, incluyendo aquel que circula masivamente en el ecosistema digital.

El artículo 169 de la norma penal, relativo a la corrupción de niñas, niños y adolescentes, señala:

Corrupción de niñas, niños y adolescentes. - 1. La persona que permita el acceso o exposición de niñas, niños o adolescentes de forma intencionada a contenido nocivo sexualizado, violento o que llame a cometer actos de odio será sancionada con pena privativa de libertad de uno a tres años. 2. La persona que incite, conduzca o permita la entrada de niñas, niños o adolescentes a prostíbulos o lugares en los que se exhibe pornografía, será sancionada con pena privativa de libertad de tres a cinco años.³⁶

Este tipo penal amplía el foco desde la producción y distribución de material pornográfico hacia la exposición intencional de NNA a contenidos y dinámicas sexuales inadecuadas, entre ellas aquellas que se desarrollan en entornos digitales. A través de sus distintos numerales, el tipo penal sanciona conductas como facilitar el acceso o exponer a niñas, niños y adolescentes a material de carácter sexual o introducirlos en espacios donde se exhibe pornografía o se practican actos de índole sexual.

Desde una perspectiva de política criminal, el artículo 169 cumple una función puente entre los delitos centrados en la producción y circulación de pornografía infantil (arts. 103, 104 y 168) y los delitos de violencia sexual digital más directamente vinculados al grooming y al contacto con fines sexuales mediante medios electrónicos. Mientras los primeros se concentran en el contenido como objeto material del delito, la corrupción de NNA se orienta a sancionar la utilización de ese contenido y de los entornos digitales como mecanismo de iniciación, normalización o banalización de la sexualidad adulta frente a personas menores de edad, afectando su indemnidad sexual y su desarrollo integral.

En consecuencia, la investigación y persecución de las conductas previstas en el artículo 169 deben incorporar de forma sistemática el análisis de la mediación tecnológica (dispositivos, aplicaciones, plataformas, algoritmos de recomendación, etc.), así como su vinculación con otras figuras de violencia sexual digital que veremos a continuación.

Hasta este punto, los tipos penales analizados se han centrado primordialmente en la protección de niñas, niños y adolescentes frente a la pornografía, su comercialización, la

³⁶ Ecuador, *Código Orgánico Integral Penal*, art. 169.

distribución de material pornográfico y la corrupción mediante exposición a contenidos sexualizados. No obstante, el artículo 166 del catálogo punitivo ecuatoriano, incorpora una figura de alcance más amplio en razón de sus víctimas, al tipificar el acoso sexual y, dentro de él, el ciberacoso sexual, como modalidad en la que la conducta descrita en el inciso principal se realiza utilizando tecnologías de la información y comunicación, medios tecnológicos, electrónicos o digitales.

La referida infracción penal esta tipificada bajo el siguiente contenido típico:

Acoso sexual.- La persona que solicite algún acto de naturaleza sexual, para sí o para un tercero, prevaliéndose de situación de autoridad laboral, docente, religiosa o similar, sea tutora o tutor, curadora o curador, ministros de culto, profesional de la educación o de la salud, personal responsable en la atención y cuidado del paciente o que mantenga vínculo familiar o cualquier otra forma que implique subordinación de la víctima, con la amenaza de causar a la víctima o a un tercero un mal relacionado con las legítimas expectativas que pueda tener en el ámbito de dicha relación de subordinación, será sancionada con pena privativa de libertad de uno a cinco años. Se considerará ciberacoso sexual cuando la conducta descrita en el inciso anterior se realice utilizando cualquiera de las tecnologías de la información y comunicación, medios tecnológicos, electrónicos o digitales, y será sancionado con una pena privativa de libertad de uno a cinco años.³⁷

El ciberacoso sexual extiende el espectro de protección más allá de las víctimas niños, niñas y adolescentes, abarcando también a personas adultas que sufren solicitudes, presiones o chantajes de índole sexual en contextos de subordinación, dependencia, autoridad o asimetría de poder, cuando estas conductas se canalizan por correo electrónico, mensajería instantánea, redes sociales, plataformas de videoconferencia u otros entornos digitales. Si bien el propio artículo prevé una respuesta agravada cuando la víctima es menor de dieciocho años o persona con discapacidad, su configuración básica se erige como un tipo general de violencia sexual digital.

Cabe señalar que la inclusión expresa de esta modalidad de ciberacoso sexual fue incorporada mediante la reforma publicada en el Registro Oficial Suplemento 526 de 30 de agosto de 2021.³⁸

Manteniendo como eje el tercer bloque del Convenio de Budapest relativo al contenido, el ordenamiento ecuatoriano configura también un grupo de infracciones penales en las que la violencia sexual se materializa a través de contenidos y comunicaciones digitales dirigidos a las víctimas. Se trata de delitos en los que las tecnologías de la información y comunicación

³⁷ Ecuador, *Código Orgánico Integral Penal*, art. 166.

³⁸ Ecuador, *Ley Orgánica Reformatoria al Código Orgánico Integral Penal para prevenir y combatir la violencia sexual digital y fortalecer la lucha contra delitos informáticos*, Registro Oficial 526, Cuarto Suplemento, 30 de agosto de 2021.

dejan de ser un mero soporte de almacenamiento de material y pasan a convertirse en el canal principal de aproximación, hostigamiento o dominación sexual, como ocurre en el ciberacoso sexual, que ya lo analizamos. La extorsión sexual basada en imágenes íntimas, el contacto con fines sexuales con personas menores de edad mediante medios electrónicos y la oferta de servicios sexuales con menores a través de plataformas digitales. Estos tipos penales permiten proyectar el estándar de Budapest hacia una respuesta más amplia frente a la violencia sexual digital basada en contenido, en la que el foco ya no se limita a la existencia del material pornográfico, sino a la dinámica de interacción, presión y control ejercida sobre la víctima en entornos virtuales.

En este mismo marco, el artículo 170 del Código Orgánico Integral Penal tipifica el delito de abuso sexual y constituye el punto de partida para comprender cómo los actos de naturaleza sexual pueden adquirir una dimensión digital cuando son registrados o difundidos mediante tecnologías de la información y comunicación. En su tipo básico, el precepto establece:

Abuso sexual. - La persona que, en contra de la voluntad de otra, ejecute sobre ella o la obligue a ejecutar sobre sí misma u otra persona, un acto de naturaleza sexual, sin que exista penetración o acceso carnal, será sancionada con pena privativa de libertad de tres a cinco años.³⁹

Y posteriormente el inciso cuarto especifica:

Se sancionará con el máximo de las penas establecidas en los incisos precedentes, cuando dicho abuso sexual fuese grabado o transmitido en vivo de manera intencional por la persona agresora, por cualquier medio digital, dispositivo electrónico o a través de cualquiera de las tecnologías de la información y comunicación.⁴⁰

Esta previsión agrava de forma expresa el injusto cuando la violencia sexual trasciende el momento de la agresión física y se proyecta al plano digital, ya sea mediante la grabación del hecho o su transmisión en vivo. El legislador ha reconocido en esta infracción penal que la utilización de medios digitales no solo facilita la comisión del abuso, sino que multiplica exponencialmente el daño a la víctima, al posibilitar la reproducción, almacenamiento y eventual difusión ulterior del contenido. La conducta deja de ser un acto aislado para convertirse en un hecho potencialmente permanente y globalizable, en el que la víctima corre el riesgo de revictimización continua cada vez que el material circula o es visualizado. En consecuencia, esta modalidad agravada integra plenamente al abuso sexual dentro del grupo de delitos de violencia sexual digital basada en contenido, y exige a la Fiscalía una atención particular a la preservación de la evidencia digital, la identificación de cadenas de difusión y la adopción de medidas urgentes para limitar la circulación del material vinculado al delito.

³⁹ Ecuador, *Código Orgánico Integral Penal*, art. 166.

⁴⁰ Ecuador, *Código Orgánico Integral Penal*, art. 166 cuarto inciso.

Asimismo, el quinto inciso del artículo 170 del referido delito, refuerza este vínculo entre violencia sexual y tecnologías de la información y comunicación, al prever el máximo de las penas cuando, además de la grabación o transmisión digital del abuso sexual, la persona agrede físicamente a la víctima y también registra o transmite dicha agresión. Este inciso reafirma que la utilización de las tecnologías de la información y comunicación en estos contextos no son un mero agravante formal, sino un factor de amplificación del daño y de prolongación en el tiempo de la victimización.

Algo similar ocurre con el delito de violación previsto en el artículo 171 del Código Orgánico Integral Penal⁴¹, cuyos numerales 6 y 7 agravan la pena cuando la agresión sexual se traslada al plano digital. En el primero de ellos, se dispone el máximo de la sanción cuando la violación es grabada o transmitida en vivo, de manera intencional, por la persona agresora mediante cualquier medio digital, dispositivo electrónico o tecnología de la información y comunicación; en el segundo, la agravación se intensifica si, además, se registra o transmite una agresión física adicional contra la víctima. De este modo, la legislación reconoce que la captación y circulación digital de la violación no solo documenta el hecho, sino que multiplica su lesividad al convertirlo en un contenido susceptible de reproducción ilimitada, reutilización para amenazar o coaccionar, lo que sitúa también a estas modalidades de violación dentro del núcleo de los delitos de violencia sexual digital basada en contenidos.

En coherencia con las infracciones señaladas de abuso sexual y violación que se encuentran en la sección cuarta denominada delitos contra la integridad sexual y reproductiva, el artículo 172 de la norma penal, sobre utilización de personas para exhibición pública con fines de naturaleza sexual, determina:

Utilización de personas para exhibición pública con fines de naturaleza sexual.- La persona que utilice a niñas, niños o adolescentes, a personas mayores de sesenta y cinco años o personas con discapacidad para obligarlas a exhibir su cuerpo total o parcialmente con fines de naturaleza sexual, será sancionada con pena privativa de libertad de siete a diez años.⁴²

Aunque el tipo no menciona expresamente las tecnologías de la información y comunicación, su referencia a la “exhibición pública” permite comprender que dicha exposición puede producirse tanto en espacios físicos tradicionales como mediante transmisiones, presentaciones o exhibiciones en línea (por ejemplo, cámaras web, plataformas

⁴¹ Ecuador, *Código Orgánico Integral Penal*, art. 171 numerales 6 y 7.

⁴² Ecuador, *Código Orgánico Integral Penal*, art. 172.

de streaming o redes sociales), en las que la persona es convertida en objeto de exhibición sexual frente a una audiencia potencialmente masiva.

En esta misma sección cuarta de delitos contra la integridad sexual y reproductiva, fue agregado el 30 de agosto del 2021, el delito de extorsión sexual⁴³. Con esta infracción penal se positiviza de manera expresa lo que en la práctica se conoce como *sextorsión*. La norma sanciona a la persona que, mediante violencia, amenazas o chantaje, induzca, incite u obligue a otra a exhibir su cuerpo desnudo, semidesnudo o en actitudes sexuales, con el propósito de obtener un provecho personal o para un tercero, ya sea de carácter sexual o de cualquier otro tipo. Aunque el precepto no hace una referencia explícita a las tecnologías de la información y comunicación, en la realidad criminológica contemporánea estas conductas se realizan de forma predominante a través de dispositivos electrónicos, redes sociales, aplicaciones de mensajería instantánea, videollamadas y plataformas de contenidos, en las que el sujeto activo explota la asimetría de poder y la capacidad de registrar o difundir imágenes íntimas para forzar la exhibición sexual de la víctima.

La extorsión sexual prevista en el artículo 172.1 se integra plenamente en el grupo de delitos de violencia sexual digital basada en contenidos y comunicaciones, pues el núcleo del injusto radica en la utilización de la amenaza explícita o implícita de exposición o divulgación de imágenes o actitudes sexuales para obtener un beneficio.

Dentro del módulo 8 “Corrupción y Género”, la Oficina de la Naciones Unidas contra la Droga y el Delito, referente a la extorsión sexual, ha señalado que:

(...) la extorsión sexual puede asociarse con una forma de acoso cibernético que ocurre cuando un perpetrador amenaza con difundir... [Imágenes y / o videos] sexualmente explícitos de la víctima a menos que se cumplan las demandas sexuales y / o se envíen imágenes o videos sexualmente explícitos al perpetrador.⁴⁴

En la referida sección del Código Orgánico Integral Penal, también se encuentra el artículo 173, que describe al denominado delito de *child grooming*. El texto vigente del referido delito señala:

Contacto con finalidad sexual con menores de dieciocho años por medios electrónicos. - La persona que a través de un medio electrónico o telemático proponga concertar un encuentro con una persona menor de dieciocho años, siempre que tal propuesta se acompañe de actos materiales encaminados al acercamiento con finalidad sexual o erótica, será sancionada con pena privativa de libertad de uno a tres años.

⁴³ Ecuador, *Código Orgánico Integral Penal*, art. 172.1.

⁴⁴ Marie Helen Maras, “Corrupción y Género”. Oficina de las Naciones Unidas contra la Droga y el Crimen”, Accedido 24 de julio del 2024, https://grace.unodc.org/grace/uploads/documents/academics/Anti-Corruption_Module_8_Corruption_and_Gender_ESP.pdf.

Cuando el acercamiento se obtenga mediante coacción o intimidación, será sancionada con pena privativa de libertad de tres a cinco años.

La persona que suplantando la identidad de un tercero o mediante el uso de una identidad falsa por medios electrónicos o telemáticos, establezca comunicaciones de contenido sexual o erótico con una persona menor de dieciocho años o con discapacidad, será sancionada con pena privativa de libertad de tres a cinco años.⁴⁵

El artículo 173 del Código Orgánico Integral Penal, incorpora de forma expresa el denominado delito de child grooming y sitúa en el centro del injusto la utilización de medios electrónicos o telemáticos como canal de aproximación sexual hacia personas menores de dieciocho años. En su primer inciso, el tipo penal sanciona la propuesta de encuentro con un menor, siempre que vaya acompañada de actos materiales dirigidos al acercamiento con finalidad sexual o erótica, lo que implica la incriminación de una fase preparatoria avanzada del abuso, antes de que se concrete cualquier contacto físico.

El segundo inciso agrava la respuesta cuando este acercamiento se obtiene mediante coacción o intimidación, reconociendo que la asimetría de poder puede manifestarse no solo por la edad sino también por el uso de amenazas, chantajes o presiones psicológicas en el entorno digital.

Finalmente, el tercer inciso extiende la tutela a los supuestos en los que la persona agresora suplanta identidades o utiliza perfiles falsos para entablar comunicaciones de contenido sexual o erótico con menores de dieciocho años o personas con discapacidad, captando así una de las formas más frecuentes de engaño en plataformas de mensajería y redes sociales. Este tipo penal cumple una función preventiva esencial: desplaza el umbral de intervención estatal hacia etapas anteriores al abuso o explotación sexual, reconoce la centralidad de las tecnologías de la información y comunicación en la captación de víctimas y exige a la Fiscalía General del Estado, desarrollar capacidades específicas para la detección temprana, la preservación de evidencias de conversación en línea, el trabajo encubierto digital y la cooperación con proveedores de servicios y autoridades extranjeras cuando las comunicaciones se canalizan por plataformas ubicadas fuera del territorio nacional.

En este punto es necesario precisar que, mientras en la extorsión sexual el sujeto pasivo carece de una calificación específica y puede ser cualquier persona, en el delito de contacto con finalidad sexual con menores de dieciocho años por medios electrónicos el propio tipo penal exige que la víctima sea, necesariamente, una persona menor de dieciocho años, sobre

⁴⁵ Ecuador, *Código Orgánico Integral Penal*, art. 173.

quien recae directamente la lesión del bien jurídico protegido⁴⁶. Además, a diferencia de la extorsión sexual, en la que los medios comisivos son variados, en este delito el legislador ha restringido expresamente el canal de comisión, disponiendo que el contacto típico debe realizarse exclusivamente a través de medios electrónicos o telemáticos, lo que refuerza su carácter de figura específicamente vinculada a la criminalidad sexual en entornos digitales.

En estrecha relación con este tipo de delitos, el artículo 174 del Código Orgánico Integral Penal, sobre oferta de servicios sexuales con menores de dieciocho años por medios electrónicos, profundiza la tutela penal de niñas, niños y adolescentes en entornos digitales.⁴⁷ El tipo sanciona a quien utilice o facilite el correo electrónico, chat, mensajería instantánea, redes sociales, blogs, fotoblogs, juegos en red o cualquier otro medio electrónico o telemático para ofrecer servicios sexuales con menores de dieciocho años; esto supone, de nuevo, un sujeto pasivo necesariamente menor de dieciocho años, pero ahora ya no solo como destinatario de comunicaciones con finalidad sexual (como en el artículo 173), sino como objeto de una oferta dirigida a terceros. La detallada enumeración de herramientas tecnológicas, seguida de la cláusula abierta “cualquier otro medio electrónico o telemático”, demuestra que el legislador ha querido anclar este delito de forma exclusiva al espacio digital, cerrando posibles lagunas frente a nuevas plataformas y modalidades de anuncio o intermediación en línea.

Este precepto se ubica en una fase más avanzada del iter criminis respecto del contacto con finalidad sexual por medios electrónicos⁴⁸: ya no se trata solamente de preparar o facilitar un encuentro con la víctima, sino de ofrecerla activamente como servicio sexual, muchas veces en contextos de redes de explotación⁴⁹ o trata de personas⁵⁰. Ello exige a la Fiscalía dirigir su atención no solo al emisor directo de la oferta, sino también a quienes “faciliten” los medios tecnológicos para esa finalidad, así como desplegar estrategias de investigación proactiva en sitios web, redes sociales, servicios de mensajería y juegos en línea, articulando la cooperación con proveedores de servicios y autoridades extranjeras para desactivar anuncios, identificar responsables y proteger de forma inmediata a las víctimas involucradas.

En los delitos de violencia sexual en los que se utilizan las tecnologías de la información y comunicación, el componente digital no es un elemento accesorio, sino estructural del injusto

⁴⁶ Ecuador Fiscalía General del Estado, Dirección de Política Criminal, “*El Delito de Extorsión y la Delincuencia Organizada – Un Estudio Dogmático Penal – Fenomenológico*” (Quito: Fiscalía General del Estado, 2024), 46.

⁴⁷ Ecuador, *Código Orgánico Integral Penal*, art. 174.

⁴⁸ Ecuador, *Código Orgánico Integral Penal*, art. 173.

⁴⁹ Ecuador, *Código Orgánico Integral Penal*, art. 100.

⁵⁰ Ecuador, *Código Orgánico Integral Penal*, art. 91.

y de respuesta institucional. Esto implica que, como criterio general de actuación, la o el fiscal deberá: 1.- Identificar desde el inicio la existencia de contenidos, dispositivos, plataformas y canales digitales involucrados; 2.- Disponer de forma inmediata su preservación, aseguramiento y análisis forense con estricta cadena de custodia; 3.- Utilizar de manera estratégica las herramientas procesales internas, la normativa internacional aplicable y los mecanismos de cooperación y asistencia penal mutua para acceder a datos alojados en otros territorios o bajo control de proveedores de servicios digitales; y 4.- Promover medidas orientadas a limitar la circulación del material ilícito y a reducir la revictimización continuada de las personas afectadas. Es indispensable tomar en consideración la dimensión tecnológica en todas las fases de la investigación y el juzgamiento de estos delitos, esto permite evitar espacios de impunidad, garantiza la protección reforzada de las víctimas, y con ello se da cumplimiento efectivo a los estándares fijados por el Código Orgánico Integral Penal y el Convenio de Budapest en materia de violencia sexual digital basada en contenidos.

En definitiva, es necesario acotar que los delitos de violencia sexual digital basada en contenidos no agotan ni circunscriben el problema de la criminalidad mediada por tecnologías de la información y comunicación en el Código Orgánico Integral Penal. La misma lógica de instrumentalización de las tecnologías de la información y comunicación que se observa en la pornografía con utilización de niñas, niños y adolescentes, en la corrupción de niños, niñas y adolescentes, en el ciberacoso sexual, en la extorsión sexual, en el grooming y en la oferta de servicios sexuales con menores, se proyecta transversalmente sobre otras infracciones en las que se tutelan bienes jurídicos distintos, como la intimidad, el secreto profesional o la información personal de terceros, el patrimonio (a través de apropiaciones y fraudes electrónicos), la libertad y la integridad personal (en contextos de acoso sistemático) o incluso la seguridad pública y el orden constitucional (cuando las plataformas digitales se emplean para incitar, organizar o financiar conductas terroristas).

En este escenario, la Fiscalía General del Estado no puede limitar el uso de herramientas de investigación digital a los delitos contra la seguridad de los activos de los sistemas de información y comunicación, sino que debe asumir que, en un número creciente de causas penales, la cadena de custodia, la preservación de la evidencia digital, la trazabilidad de las comunicaciones y las técnicas de atribución de identidades en línea constituyen condiciones mínimas de una persecución eficaz. Ello exige consolidar, de manera sistemática, metodologías y protocolos de tratamiento de evidencia digital en investigaciones relativas a violación de la intimidad, revelación de secretos, apropiación fraudulenta por medios electrónicos, delitos de

acoso y terrorismo, entre otros, de modo que la mediación tecnológica sea analizada como un eje transversal del injusto y no como un mero dato instrumental, garantizando así la protección integral de los diversos bienes jurídicos comprometidos y aumentando las posibilidades reales de identificación, juzgamiento y sanción de las personas responsables.

3.2.4. Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines

Finalmente, en relación con el cuarto bloque del Convenio de Budapest, el Código Orgánico Integral Penal, tipifica los actos lesivos a la propiedad intelectual y los actos lesivos a los derechos de autor. En este marco, se contemplan, los siguientes preceptos jurídicos:

Actos lesivos a la propiedad intelectual.- Será sancionada con pena privativa de libertad de seis meses a un año, comiso y multa de ocho hasta trescientos salarios básicos unificados del trabajador en general, la persona que, a sabiendas, en violación de los derechos de propiedad intelectual contemplados en la normativa aplicable, realice uno o más de los siguientes actos con fines de lucro y a escala comercial: 1. Fabrique, comercialice o almacene etiquetas, sellos o envases que contengan marcas o denominaciones de origen registradas en el país. 2. Separe, arranque, reemplace o utilice etiquetas, sellos o envases que contengan marcas registradas en el país, para utilizarlos en productos de distinto origen. 3. Rellene con productos espurios envases identificados con marca ajena. 4. Almacene, fabrique, utilice, oferte en venta, venda, importe o exporte: a) Un producto amparado por una patente de invención o modelo de utilidad registrado en el país; b) Un producto fabricado mediante la utilización de un procedimiento amparado por una patente de invención registrada en el país; c) Un producto amparado por un dibujo o modelo industrial registrado en el país; d) Una obtención vegetal registrada en el país, así como su material de reproducción, propagación o multiplicación; e) Un esquema de trazado (topografía) registrado en el país, un circuito semiconductor que incorpore dicho esquema de trazado (topografía) o un artículo que incorpore tal circuito semiconductor; f) Un producto o servicio que utilice un signo distintivo no registrado idéntico o similar a un signo distintivo registrado en el país; y, g) Un producto o servicio que utilice un signo distintivo o denominación de origen no registrada, idéntica o similar a una denominación de origen registrada en el país. En los casos de los literales f) y g) de este cuarto numeral los productos o servicios que utilicen el signo no registrado, deberán ser idénticos o que guarden conexión competitiva a los productos o servicios protegidos por las marcas o indicaciones geográficas registradas en el país.⁵¹

En contraste con el presente contenido típico, el artículo 10 del Convenio de Budapest remite a las infracciones de propiedad intelectual definidas por el derecho interno e internacional, pero condiciona su tipificación penal a que sean realizadas deliberadamente, a escala comercial y “por medio de un sistema informático”. De este modo, mientras el Código Orgánico Integral Penal ofrece una protección más amplia desde el punto de vista del bien jurídico, pues incrimina estas conductas con independencia del medio utilizado, el Convenio de Budapest introduce un criterio tecnológico específico (la utilización de un sistema informático) como elemento de conexión con la ciberdelincuencia. La armonización pasa, por

⁵¹ Ecuador, *Código Orgánico Integral Penal*, art. 208.A.

tanto, por interpretar que las conductas descritas en la norma penal ecuatoriana comprenden también las realizadas a través de plataformas digitales y redes telemáticas.

En complemento al delito de actos lesivos a la propiedad intelectual, el artículo 208B del Código Orgánico Integral penal tipifica de manera específica los actos lesivos a los derechos de autor y derechos conexos, bajo el siguiente contenido:

Actos lesivos a los derechos de autor.- Será sancionada con pena privativa de libertad de seis meses a un año, comiso y multa de ocho hasta trescientos salarios básicos unificados del trabajador en general, la persona que, a sabiendas, en violación de los derechos de autor o derechos conexos contemplados en la normativa aplicable, realice uno o más de los siguientes actos a escala comercial: a) Altere o mutile una obra, inclusive a través de la remoción o alteración de información electrónica sobre el régimen de derechos aplicables; b) Inscriba, publique, distribuya, comunique o reproduzca, total o parcialmente, una obra ajena como si fuera propia; c) Reproduzca una obra sin autorización del titular o en un número mayor de ejemplares del autorizado por el titular, siempre que el perjuicio económico causado al titular sea mayor a cincuenta salarios básicos unificados del trabajador en general; d) Comunique públicamente obras o fonogramas, total o parcialmente; e) Introduzca al país, almacene, ofrezca en venta, venda, arriende o de cualquier otra manera ponga en circulación o a disposición de terceros reproducciones ilícitas de obras o en número que exceda del autorizado por el titular; f) Reproduzca un fonograma o en general cualquier obra protegida, así como las actuaciones de intérpretes o ejecutantes, total o parcialmente, imitando o no las características externas del original, así como quien introduzca al país, almacene, distribuya, ofrezca en venta, venda, arriende o de cualquier otra manera ponga en circulación o a disposición de terceros tales reproducciones ilícitas; g) Retransmita sin autorización, por cualquier medio, las emisiones de radiodifusión, televisión y en general cualquier señal que se transmita por el espectro radioeléctrico y que esté protegida por derechos de autor o derechos conexos; salvo que dicha retransmisión provenga de una obligación normativamente impuesta; y, h) Fabrique, importe, exporte, venda, arriende o de cualquier forma distribuya al público un dispositivo, sistema o software que permita descifrar una señal de satélite cifrada portadora de programas o en general de telecomunicaciones, sin autorización del distribuidor legítimo de esa señal; o, de cualquier forma, eluda, evada, inutilice o suprima un dispositivo, sistema o software que permita a los titulares del derecho controlar la utilización de sus obras o prestaciones, el cual posibilite impedir o restringir cualquier uso no autorizado de estos.

Este precepto refuerza la tutela penal de la creación intelectual en su dimensión clásica y, al mismo tiempo, incorpora explícitamente supuestos vinculados al entorno digital y a las telecomunicaciones, lo que permite articularlo coherentemente con el estándar del artículo 10 del Convenio de Budapest, en cuanto a las infracciones a derechos de autor y derechos afines cometidas deliberadamente, a escala comercial y mediante el uso de sistemas informáticos y redes de comunicación.

4. Contenido Digital

Desde la perspectiva de la configuración típica, los delitos contra la seguridad de los activos de los sistemas de información y comunicación presentan una tipicidad objetiva fuertemente atravesada por elementos normativos y valorativos. No se trata solo de acciones materiales (acceder, destruir, alterar, revelar), sino de conductas que recaen sobre categorías técnico y jurídicas definidas por el propio Código Orgánico Integral Penal, como contenido digital, datos de tráfico, proveedor de servicios o sistema informático, y que, a su vez, remiten a marcos regulatorios especializados. La norma en referencia conceptualiza los referidos términos en el artículo 234.4 del Código Orgánico Integral Penal, cuyas definiciones se incorporan a continuación como parámetro obligatorio para la correcta delimitación del alcance de estos tipos penales.

a. Contenido digital. - El contenido digital es todo dato informático que representa hechos, información o conceptos de la realidad, almacenados, procesados o transmitidos por cualquier medio tecnológico o canal de comunicación que se preste a tratamiento informático, incluidos los programas diseñados para un equipo tecnológico aislado, interconectado o relacionados entre sí.

b. Datos de tráfico. - Contenido digital relativo a una comunicación efectuada por medio de un sistema informático o canal de comunicación, generados por este sistema como elemento de una cadena de comunicación, indicando su origen, su destino, su trayecto, la hora, la fecha, el tamaño, la duración o el tipo de servicio subyacente.

c. Proveedor de servicios. - Cualquier entidad, pública o privada, nacional o internacional, que proporciona a los usuarios de sus servicios la capacidad de comunicarse a través de un sistema informático, o de cualquiera de las tecnologías de la información y comunicación, así como cualquier otra entidad que procese o almacene contenido digital en nombre y por cuenta de aquella entidad proveedora o de sus usuarios.

d. Sistema informático. - Cualquier dispositivo o conjunto de dispositivos interconectados o asociados, en que uno o varios de ellos desarrolla, ejecutando un programa, el tratamiento automatizado de contenido digital.⁵²

El artículo 500 del Código Orgánico Integral Penal también define a lo que debe entenderse como contenido digital, señalando que:

Contenido digital. - El contenido digital es todo dato informático que representa hechos, información o conceptos de la realidad, almacenados, procesados o transmitidos por cualquier medio tecnológico que se preste a tratamiento informático, incluidos los programas diseñados para un equipo tecnológico aislado, interconectado o relacionados entre sí.⁵³

En este punto cabe hacer una puntualización, si bien el Código Orgánico Integral Penal contiene dos definiciones de contenido digital, una de alcance general en el artículo 234.4 y otra incorporada en el artículo 500 con reforma en el año 2023, en el contexto de los medios de prueba, esta duplicidad no debe entenderse como la existencia de dos conceptos autónomos

⁵² Ecuador, *Código Orgánico Integral Penal*, art. 234.4.

⁵³ Ecuador, *Código Orgánico Integral Penal*, art. 500.

o contradictorios. La definición del artículo 234.4 conserva su carácter de cláusula general “*para los efectos del presente Código*”, mientras que la del artículo 500 cumple una función estrictamente instrumental, orientada a precisar el tratamiento probatorio del contenido digital.

En consecuencia, la o el fiscal, al calificar jurídicamente los hechos y al valorar la pertinencia, licitud y autenticidad de la prueba digital, debe partir del concepto general del artículo 234.4 e interpretar el artículo 500 de forma coherente y complementaria con aquel, evitando que una formulación más limitada o imprecisa de la definición probatoria implique una restricción indebida del ámbito de protección de los tipos penales informáticos ni del reconocimiento del contenido digital como objeto de tutela y como medio de prueba.

Esta exigencia interpretativa se proyecta directamente sobre la labor de calificación jurídica de los hechos punibles. La correcta subsunción demanda que la o el fiscal verifique si las conductas investigadas se inscriben efectivamente en el significado técnico de esos elementos normativos, tarea que no puede agotarse en la sola lectura del tipo penal. Es indispensable acudir por remisión, de forma sistemática, a normas extrapenales que desarrollan el régimen de datos y de infraestructuras digitales, entre ellas, la Ley Orgánica de Protección de Datos Personales, la normativa sobre transparencia y acceso a la información, las regulaciones sectoriales de telecomunicaciones y de servicios financieros, así como estándares técnicos de seguridad de la información, para determinar cuándo un dato constituye contenido digital protegido, qué información califica como dato personal o dato de tráfico, quién actúa como proveedor de servicios o qué sistemas se consideran críticos. Este contraste entre la descripción fáctica y los conceptos técnico-jurídicos aplicables es un ejercicio ineludible de la actividad fiscal, pues solo a partir de esa verificación integral es posible realizar una subsunción perfecta de las conductas penalmente relevantes al tipo y garantizar, al mismo tiempo, la protección del bien jurídico y el respeto al principio de legalidad.

4.1. Características del contenido digital

El contenido digital presenta ciertas características inherentes⁵⁴ que profundizan estas diferencias frente a los soportes tradicionales:

1. Volátil: se refiere a datos que son transitorios y pueden perderse o alterarse fácilmente, especialmente durante la transmisión o en caso de pérdida de energía.⁵⁵

⁵⁴ Ecuador Fiscalía General del Estado, *Manual de actuación para la recolección, preservación y análisis del contenido digital* (Quito: Fiscalía General del Estado, 2025), 45.

⁵⁵ Science direct, “Evidencia volátil”, *Science direct*, 2013, https://www-sciencedirect-com.translate.goog/topics/computer-science/volatile-evidence?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=tc

2. Duplicable: es susceptible de ser copiado y transferido sin límite, esto debido a que presentan copia directa del contenido, problemas técnicos por ejemplo en la configuración de sitios web, o por rasping⁵⁶ de contenido.⁵⁷
3. Eliminable: al no existir en un soporte físico, puede ser borrado total o parcialmente dentro del entorno digital, lo que en muchos casos dificulta su recuperación o rastreo.⁵⁸
4. Alterable: su contenido no es inmutable, ya que puede ser editado, manipulado o transformado mediante herramientas tecnológicas accesibles, lo que no implica su desaparición, sino un cambio en su forma, estructura o información original.⁵⁹

Ahora bien, una vez comprendido el concepto de contenido digital y sus principales características, resulta fundamental explicar por qué, en la actualidad, este tipo de contenido es aprovechado por los grupos de delincuencia organizada (GDO). Estas estructuras actúan bajo esquemas jerárquicos o de células, lo que les permite dividir funciones, reducir riesgos y adaptarse rápidamente al entorno. En ese marco, recurren a tecnologías de la información y la comunicación para comunicarse, coordinar operaciones y evadir controles, mediante el uso de sistemas cifrados, aplicaciones de mensajería, drones, GPS y otros medios que facilitan el monitoreo de rutas, el movimiento de bienes ilícitos y la captación de personas. Su operatividad se articula a través de rutas terrestres, marítimas y aéreas que se ajustan según el nivel de control estatal o los conflictos con otros grupos, y suele incluir la infiltración de actividades lícitas como: comercio, transporte o construcción, para movilizar recursos sin levantar sospechas.⁶⁰

De igual manera, se ha identificado que una de las tendencias en expansión dentro de las economías criminales es el uso de monedas digitales. Estas resultan atractivas porque funcionan en línea sin requerir intermediarios financieros tradicionales, operan en plataformas abiertas y presentan bajos niveles de exigencia para verificar la identidad de los usuarios. Estas

⁵⁶ Rasping de contenido es la copia no autorizada de contenido de un sitio web mediante bots automatizados o software, VPN Unlimited. “Extracción de contenido Definición y Proceso del Raspado de Contenido” <https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://www.vpnunlimited.com/es/help/cybersecurity/content-scraping%3Fsrsltid%3DAfmBOooM9O1GrGG-3yVjwUhbuqVbZrHGwWkvMriUDw41oF88GcVJLA0R&ved=2ahUKEwiIuce094WQAxVeZjABHfZwHnEQFnoECBUQAQ&usg=AOvVaw1q7SIUz1syf7nsuTwE5gFn>

⁵⁷ SEO, “¿Qué es el contenido duplicado y cómo afecta a su SEO?”, *SEO*, 10 de abril de 2025, <https://www.seo.com/es/basics/glossary/duplicate-content/>

⁵⁸ Paúl Ochoa, “*El tratamiento de la evidencia digital una guía para su adquisición y/o recopilación*” (Cuenca: Universidad de Cuenca, 2018), 36 - 43.

⁵⁹ Paúl Ochoa, “*El tratamiento de la evidencia digital una guía para su adquisición y/o recopilación*,” 36 - 43.

⁶⁰ Ecuador Ministerio del Interior, *Boletín de Análisis de la Ciberdelincuencia* (Quito: Ministerio del Interior, 2025), 25.

características convierten a las criptomonedas en un medio idóneo para ocultar, transferir o almacenar recursos ilícitos.⁶¹

4.2. Manejo de evidencia en referencia al contenido digital

En el período desde agosto 2014 hasta julio 2025, se registraron 8.256 NDD a escala nacional⁶² en los principales tipos penales vinculados a delitos informáticos, evidenciando una tendencia ascendente sostenida, con dos picos notables, la primera en 2022 donde se visibiliza un incremento relevante por digitalización post-pandemia y mayor actividad delictiva transfronteriza. La segunda en el periodo de 2024–2025 que muestra un máximo histórico, con 1.606 NDD en 2024 y 1.007 NDD solo en los primeros siete meses de 2025.⁶³

Aquello significa que, el crecimiento de los delitos informáticos ha aumentado de manera exponencial, evidenciando cómo los delincuentes aprovechan la transformación tecnológica para atacar a través de los puntos vulnerables del internet, como redes, infraestructuras y sistemas, generando graves repercusiones económicas y sociales.⁶⁴ Frente a este contexto, resulta fundamental conocer cómo manejar adecuadamente el contenido digital, de modo que pueda ser utilizado como evidencia en una investigación que conduzca a la identificación y captura de los responsables.

Para comprender de forma adecuada el tratamiento de este tipo de evidencia, es necesario destacar que es de uso y cumplimiento obligatorio lo dispuesto en el Manual de actuación para la recolección, preservación, tratamiento y análisis del contenido digital⁶⁵, emitido por la Fiscalía General del Estado, el Consejo de la Judicatura y el Ministerio de la Mujer y Derechos Humanos (hoy Ministerio de Gobierno).⁶⁶

Dicho Manual establece que, antes de iniciar cualquier procedimiento, se debe considerar que el contenido digital está compuesto por:

⁶¹ Ecuador Ministerio del Interior, *Boletín de Análisis de la Ciberdelincuencia*, 25.

⁶² Fiscalía General del Estado, *pedido de información realizado a la Dirección de Estadísticas y Sistemas de la Información con período de agosto 2014 hasta julio de 2025*, 2025.

⁶³ Fiscalía General del Estado, *pedido de información realizado a la Dirección de Estadísticas y Sistemas de la Información con período de agosto 2014 hasta julio de 2025*, 2025.

⁶⁴ INTERPOL, “Ciberdelincuencia”, INTEPROL, accedido el 7 de noviembre de 2025, <https://www.interpol.int/es/Delitos/Ciberdelincuencia>.

⁶⁵ Ecuador Fiscalía General del Estado, *Manual de actuación para la recolección, preservación, tratamiento y análisis del contenido digital* (Quito: Fiscalía General del Estado, Consejo de la Judicatura y Ministerio de la Mujer y Derechos Humanos, 2025).

⁶⁶ Ecuador Fiscalía General del Estado, *Manual de actuación para la recolección, preservación, tratamiento y análisis del contenido digital* (Quito: Fiscalía General del Estado, Consejo de la Judicatura y Ministerio de la Mujer y Derechos Humanos, 2025).

1. Indicio físico: llamado como equipo o contenedor
2. Información digital: constituye la evidencia digital.⁶⁷

Asimismo, el referido instrumento determina que debe entenderse por evidencia digital: “cualquier tipo de datos en tránsito o en reposo que se encuentra en formato digital y que puede ser utilizada en investigaciones legales, forenses o en otros contextos para respaldar o refutar afirmaciones o acusaciones”.⁶⁸

Con estas consideraciones preliminares, a continuación, se señalan las fases que deben llevarse a cabo para el buen manejo de la evidencia del contenido digital:

1. Fase 1: Intervención en la escena del delito

a.- Protección del lugar.- Observación y valoración del Lugar: En el sitio del suceso analizará el entorno y características del lugar para aplicar las técnicas de protección de la escena con los medios disponibles. Uso del equipo de protección necesario básico. Abstenerse de manipular los indicios, contaminar la escena o ejecutar cualquier acción que ponga en riesgo su integridad y de los elementos materiales probatorios. Restringir el acceso a la zona del incidente, para evitar algún tipo de alteración de la posible evidencia digital a recolectar.

Realizar un recorrido perimetral del lugar del hecho y/o hallazgo, con el propósito de determinar los límites e identificar lugares conexos e indicios. Identificar los riesgos iniciales: identificar si se requiere apoyo para mitigar o neutralizar los riesgos eléctricos, electromagnéticos, presencia de artefactos explosivos, estructurales, naturales, entre otros.

b.- Identificación de indicios. De acuerdo con la tipología del delito, se debe establecer los dispositivos electrónicos y/o elementos contenedores de evidencia digital, que se encuentren involucrados en el hecho a investigar (...)

c.- Ingreso de indicios al centro de acopio. En caso encontrarse en la capacidad de gestionar los dispositivos electrónicos y/o los elementos contenedores de evidencia digital y de no requerir personal técnico se suscribirá el Parte Policial, en el cual constará la descripción narrativa y fotográfica de la escena, incluyendo la ubicación en donde se encuentran los equipos, dispositivos y/ o elementos a ser incautados o secuestrados y el formulario único de cadena de custodia.

d.- Solicita presencia del interventor. En el caso de requerir la presencia del personal técnico se deberá gestionar y coordinar la asistencia de más unidades con capacidades para procesamiento del lugar de la intervención.⁶⁹

2. Fase 2: Intervinientes en el procesamiento de la escena

Una vez definida la tipología del hecho se realiza el procesamiento de la escena, es decir, la aplicación de la metodología inspección ocular técnica en el lugar de los hechos. Esto incluye el aseguramiento y traslado e ingreso de los indicios al centro de acopio. En caso de requerir apoyo técnico específico, se solicitará la intervención del Primer Responsable de Evidencia Digital (DEFER) quien aplicará la metodología detallada en el presente manual, garantizando la integridad de la evidencia recolectada. La secuencia técnica para la recolección de indicios

⁶⁷ Ecuador Fiscalía General del Estado, *Manual de actuación para la recolección, preservación, tratamiento y análisis del contenido digital*, 46.

⁶⁸ Ecuador Fiscalía General del Estado, *Manual de actuación para la recolección, preservación, tratamiento y análisis del contenido digital*, 47.

⁶⁹ Ecuador Fiscalía General del Estado, *Manual de actuación para la recolección, preservación, tratamiento y análisis del contenido digital*, 45-54.

prioriza el levantamiento y exploración de elementos materiales probatorios de interés lofoscópico y no lofoscópico que pudieran encontrarse sobre los medios tecnológicos. El perito en IOT aplicará el procedimiento con la aplicación de reactivos y toma de muestras que resulten menos dañinos para el dispositivo explorado. En caso de considerarlo pertinente, el perito de Inspección Ocular Técnica, podrá solicitar acompañamiento del Primer Responsable de Evidencia Digital (DEFER), a efectos de recolectar y/o preservar la evidencia digital. No se debe manipular innecesariamente ni buscar información en los mismos, excepto cuando se prevea adquirir datos volátiles o se efectúen operaciones urgentes de triaje por parte del personal especialista, debiéndose en todos los casos documentar e informar al operador de justicia el proceso realizado.⁷⁰

3. Fase 3: Procesamiento de evidencia digital en laboratorio

Esta fase supone el paso desde el aseguramiento y traslado del indicio hacia un entorno controlado de laboratorio, donde se realiza la ejecución sistemática de la metodología de tratamiento de evidencia digital prevista en el propio manual, con intervención del personal especializado cuando corresponda, garantizando que la información extraída conserve su integridad y valor probatorio. En esta etapa, la regla técnica es minimizar toda manipulación innecesaria del dispositivo o contenedor y evitar “explorar” o “buscar” información en él, salvo escenarios estrictamente justificados (datos volátiles o triaje urgente), dejando siempre documentación completa de cada acción y reporte al operador de justicia.

Además, el manual ancla esta fase en criterios de calidad forense, relevancia, fidelidad, autenticidad, suficiencia, y en exigencias de integridad y auditabilidad (trazabilidad) para que el procedimiento sea verificable y reproducible, reforzando así la admisibilidad de la evidencia.

Por lo expuesto, el manejo del contenido digital como evidencia exige una actuación estrictamente técnica, documentada y trazable, desde la escena hasta el laboratorio, para asegurar su integridad, autenticidad y valor probatorio. Por ello, en toda intervención deberá observarse de manera obligatoria lo previsto en el Manual de actuación para la recolección, preservación, tratamiento y análisis del contenido digital, a fin de estandarizar procedimientos, evitar contaminaciones o alteraciones y garantizar que la evidencia sea admisible y útil en el proceso investigativo.

⁷⁰ Ecuador Fiscalía General del Estado, *Manual de actuación para la recolección, preservación, tratamiento y análisis del contenido digital*, 45-54.

5. Cooperación internacional en materia de ciberdelincuencia.

El Ecuador dio un paso institucional decisivo al ratificar el Convenio sobre la Ciberdelincuencia (Convenio de Budapest). Con ello, el país consolida su adhesión al principal instrumento internacional en la materia, orientado a armonizar estándares, fortalecer la cooperación internacional y robustecer las capacidades estatales para la investigación y persecución de delitos informáticos, frente a un riesgo creciente para la seguridad nacional.

La incorporación de Ecuador al Convenio de Budapest permite al país:

1. Intercambiar evidencia digital con más de 60 países miembros.
2. Acceder a mecanismos de cooperación internacional en investigaciones de ciberdelincuencia.
3. Integrarse a la red de contacto 24/7, que facilita respuestas rápidas para delitos digitales.⁷¹

En relación con estos aspectos, el capítulo III del Convenio de Budapest regula la cooperación internacional. Este capítulo establece que, mediante la aplicación de los instrumentos internacionales pertinentes en materia de cooperación penal, así como bajo el principio de reciprocidad internacional, los Estados parte se comprometen a brindar asistencia mutua. En particular, el artículo 25 dispone que:

Las Partes se prestarán toda la ayuda mutua posible a efectos de las investigaciones o de los procedimientos relativos a los delitos relacionados con sistemas y datos informáticos o con el fin de obtener pruebas en forma electrónico de un delito⁷².

Asimismo, el numeral 3 de dicho artículo establece que:

Cada parte podrá en caso de urgencia formular una solicitud de asistencia mutua, o realizar las comunicaciones relativas a la misma a través de medios de comunicación rápidos, como el fax o el correo electrónico, siempre que esos medios ofrezcan niveles suficientes de seguridad y de autenticación con confirmación oficial posterior si el Estado requerido así lo exige. El Estado requerido aceptará la solicitud y responderá a la misma por cualquiera de esos medios rápidos de comunicación⁷³.

Se complementa con el numeral 4 del mismo artículo que señala:

Salvo en caso de que se disponga expresamente otra cosa en los artículos del presente capítulo, la asistencia mutua está sujeta a las condiciones establecidas en el derecho interno de la Parte requerida o en los tratados de asistencia mutua aplicables, incluidos los motivos sobre la base de los cuales la Parte requerida puede rechazar la cooperación. La parte requerida no deberá ejercer su derecho a rehusar la asistencia mutua en relación con los delitos previstos en los

⁷¹ Ecuador Ministerio del Interior, *Boletín de Análisis de la Ciberdelincuencia*, 28.

⁷² Consejo de Europa, *Convenio sobre la Ciberdelincuencia*, art.25 numeral 1.

⁷³ Consejo de Europa, *Convenio sobre la Ciberdelincuencia*, art.25.

artículos 2 a 11 únicamente porque la solicitud se refiera a un delito que dicha Parte considere de carácter fiscal⁷⁴.

A partir de lo expuesto, resulta indispensable analizar las características fundamentales del procedimiento para solicitar asistencia mutua. El referido instrumento internacional en su artículo 27 establece lo siguiente:

1.- En ausencia de tratado de asistencia mutua o de acuerdo basado en legislación uniforme o recíproca en vigor entre la Parte requirente y la Parte requerida, se aplicarán las disposiciones del 2 a 9 del presente artículo. Dichas disposiciones no se aplicarán cuando exista un tratado, acuerdo o legislación de este tipo a menos que las Partes implicadas decidan aplicar en su lugar la totalidad o una parte del resto del presente artículo.⁷⁵

En relación con este numeral, resulta indispensable que los agentes fiscales, junto con sus equipos misionales, conozcan los tratados de asistencia mutua suscritos por el Ecuador, a fin de poder invocarlos adecuadamente al momento de presentar una asistencia penal en esta materia:

TRATADOS BILATERALES
Tratado entre el Gobierno de la República del Ecuador y el Gobierno de Australia sobre Asistencia Penal Mutua en Asuntos Penales.
Convenio de Cooperación Judicial y Asistencia Mutua en Materia Penal entre la República de Ecuador y la República de Colombia.
Memorando de Entendimiento entre la República del Ecuador y la República de Colombia para Prevención e Investigación del Delito de la Trata de Personas y la Asistencia y Protección de las Víctimas.
Convenio de Cooperación sobre Asistencia Jurídica Mutua en Materia Penal entre el Gobierno de la República del Ecuador y el Gobierno de la República de Cuba.
Tratado entre la República del Ecuador y la República Popular China sobre Asistencia Legal mutua en Temas Penales.
Tratado de Asistencia Judicial en Materia Penal entre la República del Ecuador y el Reino de España.
Tratado de Asistencia Jurídica en Materia Penal entre el Gobierno de la República del Ecuador y el Gobierno de la República de Italia.
Convenio sobre Asistencia Jurídica en Materia Penal entre los Estados Unidos Mexicanos y la República del Ecuador
Convenio sobre Asistencia Judicial en Materia Penal con Paraguay
Acuerdo de Asistencia Judicial en Materia Penal entre la República del Perú y la República del Ecuador
Acuerdo de Asistencia Legal Mutua en Materia Penal entre el Gobierno del Reino de Suecia y el gobierno de la República de Ecuador
Tratado de Cooperación Judicial en Materia Penal entre la Confederación Suiza y la República del Ecuador
Acuerdo de Asistencia Jurídica Mutua en Asuntos Penales entre la República del Ecuador y la República Oriental de Uruguay
Convenio de Prevención, Tráfico Ilícito de Drogas entre Ecuador y Venezuela.

Elaborado por: Dirección de Política Criminal

Fuente: Fiscalía General del Estado, Dirección de Cooperación y Asuntos Internacionales.

⁷⁴ Consejo de Europa, *Convenio sobre la Ciberdelincuencia*, art.25.

⁷⁵ Consejo de Europa, *Convenio sobre la Ciberdelincuencia*, art.27.

Acuerdos Interinstitucionales
Memorando de Entendimiento entre la Fiscalía General de la República del Ecuador y la Fiscalía General del Principado de Andorra
Memorando de Entendimiento entre la Fiscalía Especial contra la Corrupción y Crimen Organizado de Albania y la Fiscalía General de la República del Ecuador
Convenio de Cooperación Interinstitucional entre el Ministerio Público Fiscal de la República de Argentina y la Fiscalía General del Estado de la República del Ecuador.
Memorando de Entendimiento para Intensificar la Cooperación Jurídica Mutua entre el Ministerio Público Federal de la República Federativa del Brasil y la Fiscalía General del Estado de la República del Ecuador
Declaración de Brasilia sobre Cooperación Jurídica Internacional contra la Corrupción
Protocolo Adicional al Memorando de Entendimiento para Intensificar la Cooperación Jurídica Mutua entre el Ministerio Público Federal de la República Federativa del Brasil y la Fiscalía General del Estado de la República del Ecuador
Protocolo entre la Fiscalía General del Estado de la República del Ecuador y la Fiscalía General de la Nación de Colombia para Reforzar la Prevención y Persecución Penal de los Delitos que Afectan la Zona Fronteriza
Protocolo Bilateral de Procedimientos para el Intercambio de Información en Telecomunicaciones entre Ecuador y Colombia
Memorando de Entendimiento para el Intercambio de Información, Experiencias y Cooperación Técnico-Jurídica en Materia Penal Ambiental
Memorando de Entendimiento en materia de Cooperación Judicial Internacional entre la Fiscalía General de la Nación de Colombia y la Fiscalía General del Estado de Ecuador
Protocolo de Confidencialidad en materia de Cooperación Judicial Internacional entre la Fiscalía General de la República del Ecuador y la Fiscalía General de la Nación de Colombia
Memorando de Entendimiento de Cooperación entre la Fiscalía General de la República del Ecuador y la Fiscalía Popular Suprema de la República de Corea
Memorando de Entendimiento para la Cooperación Interinstitucional entre el Ministerio Público de la República de Costa Rica y la Fiscalía General del Estado de Ecuador
Memorando de Entendimiento en materia de Cooperación entre la Fiscalía General del Estado de la República del Ecuador y la Fiscalía Popular Suprema de la República Popular China
Memorando de Entendimiento en materia de Cooperación entre la Fiscalía General de la República de Ecuador y la Fiscalía General del Estado del Reino de España
Convenio Interinstitucional de Asistencia mutua en Materia Penal entre la Fiscalía General de la República de Ecuador y la Fiscalía General de la República de China (Taiwán)
Convenio de Cooperación Interinstitucional entre el Ministerio Público de Chile y la Fiscalía General del Estado de la República de Ecuador
Memorando de Entendimiento en materia de Cooperación entre la Fiscalía General del Estado de la República del Ecuador y la Procuraduría General de la República de los Estados Unidos Mexicanos
Addendum al Memorando de Entendimiento en materia de Cooperación entre la Fiscalía General de la República de Ecuador y la Fiscalía General del Estado del Reino de España
Convenio sobre Cooperación Técnica entre la Fiscalía General del Estado de la República del Ecuador y el Ministerio Público de la República de Honduras
Memorando de entendimiento entre la Fiscalía General de la República del Ecuador y la Dirección Nacional Antimafia y Antiterrorismo de la República Italiana
Acuerdo de Cooperación sobre Intercambio de Información y Experiencias para el Combate de la Delincuencia Organizada Transnacional, el Tráfico Ilícito de Drogas y Delitos Conexos entre la Fiscalía General del Estado de la República del Ecuador y la Procuraduría General de la República de los Estados Unidos Mexicanos
Memorando de Entendimiento para la Cooperación Interinstitucional entre el Ministerio Público de la República de Panamá y la Fiscalía General del Estado de la República de Ecuador
Memorando de Entendimiento en materia de Cooperación entre la Fiscalía General del Estado de la República del Ecuador y el Ministerio Público de la República de Perú
Protocolo entre la Fiscalía General del Estado de la República del Ecuador y el Ministerio Público de la República del Perú para Reforzar la Prevención y Persecución Penal de los Delitos que Afectan la Zona Fronteriza
Protocolo de Procedimiento sobre Técnicas Investigativas en Delitos Hidrocarburíferos y/o Contrabando de Combustibles y sus Derivados, en el Marco de Indagación Binacional Ecuador-Perú

Elaborado por: Dirección de Política Criminal

Fuente: Fiscalía General del Estado, Dirección de Cooperación y Asuntos Internacionales.

En este punto igualmente debe tomarse en consideración que el Convenio sobre Ciberdelincuencia, en su artículo 27 señala que:

1.- Cada parte designará una o varias autoridades centrales encargadas de enviar las solicitudes de asistencia mutua o de responder a las mismas de ejecutarlas o de remitirlas a las autoridades competentes para su ejecución(...)⁷⁶

Cabe señalar, que la Fiscalía General del Estado ha sido designada por el Ecuador como autoridad central en materia penal para la tramitación de la asistencia judicial internacional. En aquellos casos en los que no exista un instrumento internacional que regule la cooperación entre Estados, la Fiscalía puede fundamentar sus solicitudes de asistencia penal en el principio de reciprocidad internacional.⁷⁷

Las solicitudes de asistencia mutua en virtud del presente artículo se ejecutarán de conformidad con el procedimiento especificado por la Parte requirente salvo cuando dicho procedimiento sea incompatible con la legislación de la Parte requerida.⁷⁸

Además de las condiciones o los motivos de denegación previstos en el párrafo 4 del artículo 25, la asistencia mutua puede ser denegada por la Parte requerida: a. si la solicitud tiene que ver con un delito que la Parte requerida considera de carácter político o vinculado a un delito de carácter política; b. si la Parte requerida estima que acceder a la solicitud podría atentar contra su soberanía, seguridad, orden público u otros intereses esenciales.⁷⁹

La parte requerida podrá aplazar su actuación en respuesta a una solicitud si dicha actuación puede perjudicar a investigaciones o procedimientos llevados a cabo por sus autoridades.⁸⁰

Antes de denegar o aplazar su cooperación, la Parte requerida estudiará, previa consulta con la Parte requirente cuando proceda, si puede atenderse la solicitud parcialmente o bajo las condiciones que considere necesarias.⁸¹

La Parte requirente podrá solicitar que la Parte requerida mantenga confidenciales la presentación y el objeto de cualquier solicitud formulada en virtud del presente capítulo, salvo en la medida en que sea necesario para la ejecución de la misma. Si la Parte requerida no puede acceder a la petición de confidencialidad, deberá informar de ello sin demora a la Parte requirente, quien decidirá a continuación si la solicitud debe ser ejecutada.⁸²

En caso de urgencia, las autoridades judiciales de la Parte requirente podrán dirigir directamente a las autoridades homólogas de la Parte requerida las solicitudes de asistencia y las comunicaciones relativas a las mismas.⁸³

Ahora bien, junto con los artículos generales sobre asistencia mutua, la Convención contempla disposiciones específicas en materia de datos informáticos. En este sentido, el artículo 29 establece que un Estado Parte puede solicitar a otro la adopción de medidas para asegurar la conservación rápida de datos almacenados en sistemas informáticos ubicados en el

⁷⁶ Consejo de Europa, *Convenio sobre la Ciberdelincuencia*, art.27.

⁷⁷ Ecuador Fiscalía General del Estado, *Guía práctica parar la asistencia internacional* (Quito: Fiscalía General del Estado, 2021), 6.

⁷⁸ Consejo de Europa, *Convenio sobre la Ciberdelincuencia*, art.27 núm. 3.

⁷⁹ Consejo de Europa, *Convenio sobre la Ciberdelincuencia*, art.27 núm. 4.

⁸⁰ Consejo de Europa, *Convenio sobre la Ciberdelincuencia*, art.27 núm. 5.

⁸¹ Consejo de Europa, *Convenio sobre la Ciberdelincuencia*, art.27. núm. 6.

⁸² Consejo de Europa, *Convenio sobre la Ciberdelincuencia*, art.27. núm. 8.

⁸³ Consejo de Europa, *Convenio sobre la Ciberdelincuencia*, art.27. núm. 9.a.

territorio del Estado requerido, cuando dichos datos puedan ser objeto de una futura solicitud de asistencia mutua relacionada con su registro, acceso, confiscación o revelación.

Asimismo, la Convención prevé que los Estados Parte podrán requerir asistencia mutua en los siguientes ámbitos:

Conservación rápida de datos informáticos almacenados. Revelación rápida de datos conservados. Asistencia mutua en relación con el acceso a datos almacenados. Acceso transfronterizo a datos almacenados, con consentimiento o cuando sea accesibles al público. Obtención en tiempo real de datos relativos al tráfico. Interceptación de datos relativos al contenido.⁸⁴

Con base en lo expuesto, resulta oportuno precisar de manera práctica cómo la Fiscalía General del Estado puede solicitar cooperación internacional cuando, dentro de un proceso, requiera acceder a contenido digital alojado en otro país mediante asistencia penal internacional. Para ello, es fundamental recordar que, antes de formalizar una solicitud de asistencia, debe gestionarse previamente la obtención de información sobre direcciones IP de proveedores de servicios de internet con sede en Estados Unidos, tales como Google, Facebook, Instagram, Microsoft, Yahoo o Twitter.⁸⁵

En esta etapa inicial, es posible requerir directamente al proveedor mediante correo electrónico, la preservación de datos y la identificación de la ubicación del servidor que los almacena. Una vez recibida la información y confirmada la aceptación del proveedor, se podrá proceder con la solicitud de asistencia penal internacional. Es indispensable considerar la figura de la orden de salvaguarda, la cual permite mantener la información disponible hasta por 180 días. Esto resulta especialmente relevante si se toma en cuenta que los servidores suelen conservar los datos únicamente por un período máximo de 90 días, lo que hace necesario solicitar de manera inmediata dicha salvaguarda.⁸⁶

Antes de emitir una solicitud formal de asistencia penal internacional, es necesario establecer contacto directo con los proveedores de servicios de internet. A continuación, se presentan las direcciones de correo electrónico de los diez principales:

⁸⁴ Consejo de Europa, *Convenio sobre la Ciberdelincuencia*, art.29 - 34.

⁸⁵ Ecuador Fiscalía General del Estado, *Guía práctica para la asistencia penal internacional*, 26.

⁸⁶ Ecuador Fiscalía General del Estado, *Guía práctica para la asistencia penal internacional*, 26.

Internet Service Provider	Primary Contact
Apple Inc.	subpoenas@apple.com
Ask.FM	lawenforcement@ask.fm
Snapchat, Inc	lawenforcement@snapchat.com
Instagram	LLC records@fb.com
Facebook, Inc	records@fb.com
Google Inc.	lis-global@google.com (lis-apac@google.com para los países de la región Asia Pacífico)
Microsoft Corporation	globalco@microsoft.com
Twitter, Inc	Fax: 1-415-222-9958 (Attn: Trust & Safety- Legal Policy) (https://t.co/lr)
Yahoo Inc!	legalpoc@yahoo-inc.com
Flickr.com	legalpoc@yahoo-inc.com
Servidores pequeños	http://www.search.org/resources/isp/list/

Elaborado por: Dirección de Cooperación y Asuntos Internacionales.

Fuente: Oficina de Asuntos Internacionales Departamento de Justicia de los Estados Unidos.

Asimismo, resulta relevante destacar que, ante el incremento de los ciberdelitos, algunos proveedores de servicios de internet han implementado mecanismos de cooperación directa que permiten acceder a información básica de suscriptores sin necesidad de tramitar previamente una solicitud de asistencia penal internacional. Un ejemplo de ello son las plataformas Facebook y WhatsApp, que disponen de portales específicos para este fin, accesibles a través de los siguientes enlaces: 1. <https://www.facebook.com/records/login/> 2. <https://www.whatsapp.com/records/login/>. La Dirección de Investigación Civil, a través del Área de Investigaciones Informáticas de la Fiscalía General del Estado es la unidad encargada de gestionar y colaborar en la ejecución de estas diligencias.⁸⁷

Una vez revisados los aspectos generales sobre la cooperación penal internacional, es preciso recordar los requisitos que deben observarse al momento de elaborar una solicitud de asistencia penal internacional, conocida como API. La Dirección de Cooperación y Asuntos Internacionales de la Fiscalía General del Estado, ha establecido un formato único que debe ser utilizado para tal fin, el cual contempla la siguiente información:

⁸⁷ Ecuador Fiscalía General del Estado, *Guía práctica para la asistencia penal internacional*, 27.

1. Órgano requirente: en este apartado se deberá incluir, en primer lugar, el nombre de la institución, en este caso la Fiscalía Provincial correspondiente a la autoridad que formula la solicitud. En segundo lugar, debe identificarse a la autoridad solicitante, indicando la fiscalía especializada, los datos completos del fiscal a cargo del caso (nombres y apellidos, dirección de la unidad investigativa, número telefónico con código de país y provincia, teléfonos adicionales y correo institucional). Finalmente, se debe incluir el punto de contacto, proporcionando la información completa de la Dirección de Cooperación y Asuntos Internacionales.
2. Autoridad central: se deberá identificar a la autoridad designada como central por el Estado requirente, de conformidad con el instrumento internacional aplicable.
3. Autoridad central del país requerido: corresponde señalar la autoridad central del país al cual se dirige la solicitud.
4. Identificación del caso: se debe precisar el asunto y la naturaleza del caso que motiva la solicitud, incluyendo el número de expediente, año o fecha de inicio de la investigación o instrucción fiscal, nombres de los investigados, procesados y ofendidos, el tipo penal objeto de investigación, el nombre del juez que conoce la causa y la etapa procesal en la que se encuentra.
5. Fundamento legal de la solicitud: se debe citar el marco normativo nacional que otorga competencia a la autoridad requirente para solicitar cooperación internacional.
6. Descripción del hecho investigado: este apartado tiene como finalidad presentar de manera detallada la teoría del caso ante las autoridades extranjeras. Debe incluirse la denuncia con referencias precisas de tiempo y lugar, la identificación de los presuntos partícipes, los resultados de las diligencias efectuadas, así como los informes periciales relevantes.

La exposición debe demostrar la conexidad de los hechos con el país al que se solicita la cooperación y con las diligencias específicas que se requieran (descritas en el numeral 9 del formato de la API). Además, debe contener información suficiente que permita a la autoridad requerida comprender los hechos, identificar que la persona natural o jurídica investigada habría incurrido en una infracción penal y evidenciar los elementos probatorios que sustentan su presunta participación.

También debe incluirse una descripción general de los elementos objetivos del tipo penal conforme al derecho ecuatoriano.

El relato deberá redactarse en tercera persona, de forma clara, precisa y coherente, evitando transcripciones literales de denuncias, versiones o partes policiales, y

cuidando los aspectos formales de redacción, como puntuación, ortografía y estructura de párrafos.

7. Delitos a los que se refiere la investigación: se deberá identificar normativa aplicable, transcribir el artículo que tipifica la infracción, describir la conducta investigada y señalar la sanción prevista en la ley.
8. Fundamento de derecho internacional aplicable: en este punto se detallará el instrumento internacional que sustenta la solicitud, garantizando su aplicabilidad al delito investigado. El fiscal deberá fundamentarse en los tratados multilaterales o bilaterales pertinentes, previamente descritos en los cuadros de referencia.
9. Descripción de la asistencia solicitada: se expondrá de manera clara y específica el tipo de asistencia requerida, manteniendo coherencia entre los hechos investigados con la asistencia solicitada; no se podrá requerir información sobre hechos o personas no mencionadas en la descripción. Además, se recomienda enumerar cada diligencia o información requerida en párrafos separados, explicando su pertinencia para la investigación.
10. Necesidad e importancia de las diligencias: se deberá justificar la relevancia jurídica de las diligencias solicitadas para el proceso penal en Ecuador, explicando la relación entre la asistencia requerida y la hipótesis del caso que se pretende demostrar.
11. Compromiso de confidencialidad: el fiscal requirente deberá garantizar la aplicación del principio de confidencialidad respecto de la información que se intercambie en el marco de la cooperación.
12. Garantías obligatorias: se deberán incorporar las garantías de que la solicitud no tiene fines políticos ni está motivada por razones de raza, religión, nacionalidad o género, y que se respeta el principio non bis in ídem.
13. Plazo de ejecución: se informará al Estado requerido sobre los plazos procesales vigentes en Ecuador para la investigación previa como para la instrucción fiscal según sea el caso y se incluirá una fecha límite tentativa para recibir la respuesta.
14. Información adicional y anexos: se detallará la documentación anexa a la solicitud, la cual deberá guardar relación directa con las diligencias requeridas y deberá presentarse de manera ordenada y foliada.
15. Documentos que no deben adjuntarse: no deben incluirse los siguientes documentos:
 1. El documento de inicio de investigación previa, 2. La denuncia, 3. Informes del agente investigador, 4. Informes periciales.

16. Finalmente, la solicitud debe concluir con una petición dirigida a las autoridades del Estado requerido, solicitando que la información o pruebas remitidas estén debidamente certificadas conforme a la legislación procesal del país de origen, indicando la ciudad, fecha de emisión, y los nombres, apellidos, cargo y firma del fiscal requirente.⁸⁸

Ahora bien, respecto de la Red 24/7, regulada en el artículo 35 del Convenio de Budapest, está se trata de una red de puntos de contacto designados cuya función consiste en estar disponibles las 24 horas del día, los siete días de la semana, con el objetivo de garantizar asistencia inmediata en investigaciones relacionadas con delitos informáticos o con la obtención de pruebas electrónicas vinculadas a un delito. Esta asistencia puede comprender acciones como: a) Asesoramiento técnico; b) conservación de datos, de conformidad con los artículos 29 y 30; y c) obtención de pruebas Suministro de información de carácter jurídico y localización de sospechosos.⁸⁹

Entre los beneficios que esta red ofrece son:

1. Es una red especializada en ciberdelincuencia y evidencia electrónica.
2. La cooperación dentro de la red es rápida, eficiente, en tiempo real y efectiva.
3. El directorio de información de contacto se mantiene actualizado.⁹⁰
4. Los datos electrónicos pueden ser preservados de manera expedita.
5. Los datos electrónicos retenidos mediante el uso de la Red y que posteriormente sean recabados a través de procedimientos de asistencia judicial mutua (API) pueden ser utilizados como evidencia en procesos penales.

En este sentido, conforme a la lista oficial de puntos de contacto, Ecuador cuenta en la Red 24/7 con el agente fiscal coordinador de la Unidad Nacional Especializada en Investigación de Ciberdelito, Roberto Carlos Torres Cáceres.⁹¹ Esta información resulta relevante para los

⁸⁸ Ecuador Fiscalía General del Estado, *Guía práctica para la asistencia penal internacional*, 33.

⁸⁹ Consejo de Europa, *Convenio sobre la Ciberdelincuencia*, art.35 núm.1, a, b, y c.

⁹⁰ Convenio de Budapest, “*Lista de autoridades competentes establecidas de conformidad con el artículo 27 del convenio sobre delitos cibernéticos*”, actualizada el 3 de julio de 2025.

<https://rm.coe.int/competent-authorities-july-2025-web/1680b69201>; Council Europe, “*24/7 Network established under the Convention on Cybercrime*”, Council Europe, 2025, <https://www.coe.int/en/web/cybercrime/24/7-network-new>

⁹¹ Ecuador Fiscalía General del Estado, *Designación de punto de contacto remitida desde la Dirección de Cooperación y Asuntos Internacionales a la Cancillería ecuatoriana*. Oficio No. FGE-DCAI-2024-003049-O, (Quito: Fiscalía General del Estado, 4 de abril de 2024).

agentes fiscales que, en el ejercicio de sus funciones, requieran canalizar solicitudes o comunicaciones a través de dicha red.

6. Conclusiones

La acelerada digitalización de la vida social y la centralidad de las tecnologías de la información y comunicación, reconocidas expresamente en el artículo 16 de la Constitución de la República del Ecuador, imponen al Estado el deber no solo de garantizar el acceso universal a las tecnologías de la información y comunicación, sino también de proteger eficazmente a las personas frente a los riesgos y vulneraciones de derechos que se materializan en el entorno digital.

El Código Orgánico Integral Penal ha seguido una trayectoria de progresiva adecuación a los estándares internacionales en materia de ciberdelincuencia, incorporando categorías típicas que responden a los cuatro bloques de criminalidad definidos por el Convenio de Budapest: delitos contra la confidencialidad, integridad y disponibilidad de sistemas y datos; delitos informáticos patrimoniales y falsificación informática; delitos relativos a contenidos ilícitos; e infracciones contra la propiedad intelectual y derechos de autor.

Las reformas al Código Orgánico Integral Penal de 2021 y 2023 han fortalecido de manera específica la respuesta penal frente a la ciberdelincuencia, al introducir definiciones legales para facilitar la aplicación de los tipos penales informáticos, agravar las conductas que afectan sistemas destinados a funciones sociales críticas, tipificar la falsificación informática y establecer un régimen de actuaciones especiales sobre contenido digital orientado a la preservación, obtención y aseguramiento de evidencia digital conforme a estándares internacionales.

En el plano institucional, la Resolución No. 034-FGE-2022 creó la Unidad Nacional Especializada en Investigación de Ciberdelito, con sede en Quito y competencia a nivel nacional, asignándole la investigación de los delitos de revelación ilegal de base de datos, interceptación de datos, transferencia electrónica de activo patrimonial (primer inciso del artículo 231), ataque a la integridad de sistemas informáticos, delitos contra la información pública reservada legalmente y acceso no consentido a un sistema informático, telemático o de telecomunicaciones; posteriormente, la Resolución No. 003-FGE-2023 reestructuró dicha Unidad y precisó el régimen de asignación de noticias del delito, consolidando la concentración de competencias y la especialización en la investigación de estas infracciones, así como de los

hechos relacionados a pornografía con utilización de niñas, niños o adolescentes y comercialización de pornografía con utilización de niñas, niños y adolescentes.

La correlación sistemática entre los cuatro bloques del Convenio de Budapest y los tipos penales del Código Orgánico Integral Penal demuestra una convergencia sustantiva del derecho penal ecuatoriano con los estándares internacionales, configurando un núcleo normativo que permite abordar las principales manifestaciones de ciberdelincuencia.

La Convención de las Naciones Unidas contra la Ciberdelincuencia, aprobada por la Asamblea General en 2024 y aún no ratificada por el Ecuador, se menciona en la presente Política Criminal únicamente a título de referencia contextual, en la medida en que el marco normativo y operativo vigente para la actuación institucional continúa definido, principalmente, por el Convenio de Budapest sobre ciberdelincuencia y sus estándares de implementación. No obstante, la Fiscalía General del Estado se mantiene atenta a la eventual entrada en vigor de dicho instrumento internacional y a las obligaciones específicas que el Estado ecuatoriano llegue a asumir en el futuro.

La violencia sexual mediada por tecnologías de la información y comunicación exige que la dimensión digital sea asumida como un componente estructural del injusto y de la respuesta institucional, lo que implica para la o el fiscal la identificación temprana de los soportes y canales digitales, su preservación y análisis forense con estricta cadena de custodia, y el uso estratégico de los mecanismos de cooperación nacional e internacional para acceder a datos y limitar la circulación del contenido ilícito.

La dimensión tecnológica constituye un eje transversal en múltiples infracciones penales del Código Orgánico Integral Penal, por lo que la Fiscalía General del Estado debe extender el uso de herramientas de investigación digital, metodologías y protocolos de tratamiento de evidencia electrónica más allá de los delitos informáticos estrictos, incorporándolos de manera sistemática en investigaciones de violación a la intimidad, revelación de secretos, apropiación fraudulenta por medios electrónicos, delitos de acoso, terrorismo y cualquier otra infracción en la que se utilicen tecnologías de la información y comunicación para la comisión del delito y se genere evidencia digital, a fin de garantizar la protección integral de los bienes jurídicos comprometidos y una persecución penal eficaz.

El “contenido digital” no es un simple soporte probatorio, sino un elemento normativo estructural para delimitar tipicidad y alcance de tutela penal; por ello, la calificación jurídica exige una verificación técnica y jurídica (incluida la remisión a normativa extrapenal y

estándares de seguridad) para asegurar subsunción conforme al principio de legalidad. A la vez, sus características de volatilidad, duplicabilidad, eliminabilidad y alterabilidad, obligan a asumir que existe una probabilidad elevada de pérdida, manipulación o reproducción masiva, por lo que la reacción fiscal debe ser temprana y técnicamente orientada desde los primeros actos investigativos.

Dado el crecimiento sostenido de noticias del delito en ciberdelincuencia y la necesidad de que el contenido digital sea utilizable como evidencia, este instrumento reafirma que el tratamiento de la evidencia digital debe ser obligatorio, estandarizado y trazable conforme a los instrumentos normativos nacionales e internacionales inherentes a la materia.

Finalmente, la persecución eficaz de la ciberdelincuencia depende de una arquitectura operativa transfronteriza, y no solo de la respuesta interna. La ratificación del Convenio de Budapest consolida ese andamiaje al habilitar el intercambio de evidencia digital, el acceso a mecanismos de cooperación y la integración a la red 24/7, diseñada para respuestas urgentes y preservación expedita de datos, conforme a la lógica de asistencia mutua del capítulo tres del referido instrumento internacional.

Realizado por:	Jonathan Ramos Mera	Analista de Política Criminal
	William Castañeda Pérez	Analista de Política Criminal
	Genesis Santos Vivanco	Analista de Política Criminal
Revisado y Aprobado por:	Ximena Coello Martínez	Directora de Política Criminal
Aprobado por:	Guido Quezada Minga	Coordinador General de Gestión del Conocimiento

Bibliografía

- Ecuador. *Constitución de la República del Ecuador*. Registro Oficial 44, 20 de octubre de 2008.
- Ecuador. *Código Orgánico Integral Penal*. Registro Oficial 180, Suplemento, 10 de febrero del 2014.
- Hungria. Consejo de Europa. *Convenio sobre la Ciberdelincuencia*. Suplemento, Registro Oficial Nro. 13, 04 de abril del 2025.
- Estados Unidos. Naciones Unidas. Asamblea General. *Convención de las Naciones Unidas contra la Ciberdelincuencia*. Resolución 79/243. 24 de diciembre de 2024.
- Ecuador. *Ley Orgánica Reformatoria al Código Orgánico Integral Penal para prevenir y combatir la violencia sexual digital y fortalecer la lucha contra delitos informáticos*. Registro Oficial 526, Cuarto Suplemento, 30 de agosto de 2021.
- Ecuador. *Ley Orgánica Reformatoria a Varios Cuerpos Legales para el Fortalecimiento de las Capacidades Institucionales y la Seguridad Integral*. Registro Oficial 279, Suplemento, 29 de marzo de 2023.
- Ecuador. Fiscalía General del Estado. *Unidad Nacional Especializada en Investigación de Ciberdelito*. Resolución Nro. 34 – FGE- 2022, 8 de junio del 2022.
- Ecuador. Fiscalía General del Estado. *Unidad Nacional Especializada en Investigación de Ciberdelito*. Resolución Nro. 003 – FGE – 2023, 16 de enero del 2023.
- Maras. Marie Helen. “*Corrupción y Género*”. Oficina de las Naciones Unidas contra la Droga y el Crimen”. Accedido 24 de julio del 2024, https://grace.unodc.org/grace/uploads/documents/academics/Anti-Corruption_Module_8_Corruption_and_Gender_ESP.pdf.
- Ecuador. Fiscalía General del Estado. Dirección de Política Criminal. *El delito de Extorsión y la Delincuencia Organizada – Un Estudio Dogmático Penal – Fenomenológico*. Quito: Fiscalía General del Estado, 2024.
- Posada. Ricardo. “El cibercrimen y sus efectos en la teoría de la tipicidad: de una realidad física a una realidad virtual”. *Nuevo Foro Penal*, Nro. 33 (2017): 72-112, ISSN 0120-8179.
- Ecuador. Fiscalía General del Estado. *Manual de actuación para la recolección, preservación y análisis del contenido digital*. Quito: Fiscalía General del Estado, 2025.
- Science direct. “Evidencia volátil”. Science direct, 2013. https://www-sciencedirect-com.translate.goog/topics/computer-science/volatile-evidence?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=tc

VPN Unlimited. “Extracción de contenido Definición y Proceso del Raspado de Contenido”.

<https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://www.vpnunlimited.com/es/help/cybersecurity/content-scraping%3Fsrsltid%3DAfmBOooM9O1GrGG-3yVjwUhbuqVbZrHGWwKvMriUDw41oF88GcVJLA0R&ved=2ahUKEwiIuce094WQAxVeZjABHfZwHnEQFnoECBUQAQ&usg=AOvVaw1q7SIUz1syf7nsuTwE5gFn>

SEO. “¿Qué es el contenido duplicado y cómo afecta a su SEO?”. SEO, 10 de abril de 2025.

<https://www.seo.com/es/basics/glossary/duplicate-content/>

Ochoa. Paúl. “El tratamiento de la evidencia digital una guía para su adquisición y/o recopilación”. Cuenca: Universidad de Cuenca, 2018.

———Ecuador. Ministerio del Interior. *Boletín de Análisis de la Ciberdelincuencia*. Quito: Ministerio del Interior, 2025.

Ecuador. Fiscalía General del Estado. *Pedido de información realizado a la Dirección de Estadísticas y Sistemas de la Información con período de agosto 2014 hasta julio de 2025*.

INTERPOL. “Ciberdelincuencia”. *INTEPROL*, accedido el 7 de noviembre de 2025.

<https://www.interpol.int/es/Delitos/Ciberdelincuencia>

———Ecuador, Fiscalía General del Estado, *Manual de actuación para la recolección, preservación, tratamiento y análisis del contenido digital*. Quito: Fiscalía General del Estado, Ecuador. Consejo de la Judicatura y Ministerio de la Mujer y Derechos Humanos, 2025.

Ecuador. Ministerio del Interior. *Boletín de Análisis de la Ciberdelincuencia*, 28.

———Ecuador. Fiscalía General del Estado. *Guía práctica para la asistencia internacional*. Quito: Fiscalía General del Estado, 2021.

Convenio de Budapest. “Lista de autoridades competentes establecidas de conformidad con el artículo 27 del convenio sobre delitos cibernéticos”, actualizada el 3 de julio de 2025.

<https://rm.coe.int/competent-authorities-july-2025-web/1680b69201>; Council Europe, “24/7 Network established under the Convention on Cybercrime”, *Council Europe*, 2025, <https://www.coe.int/en/web/cybercrime/24/7-network-new>

Ecuador. Fiscalía General del Estado. *Designación de punto de contacto remitida desde la Dirección de Cooperación y Asuntos Internacionales a la Cancillería ecuatoriana*. Oficio No. FGE-DCAI-2024-003049-O, 4 de abril de 2024.

[1] La Coordinación General de Gestión del Conocimiento mediante Memorando Nro. FGE-CGGC-2025-00755-M, de fecha 30 de diciembre de 2025, remite al Señor Fiscal General del Estado, Encargado, el documento “Instrumento Técnico de Política Criminal - Ciberdelincuencia”, para su consideración y correspondiente autorización, previo a la aprobación por parte de la Coordinación. Una vez autorizado por parte de la Máxima Autoridad, mediante sumilla inserta en el Memorando Nro. FGE-CGGC-2025-00755-M, de fecha 30 de diciembre de 2025, la Coordinación en cumplimiento al Estatuto Orgánico de Gestión Organizacional por Procesos en lo referente a: 1.2.3 Gestión del Conocimiento. Literal g) Aprueba el “Instrumento Técnico de Política Criminal - Ciberdelincuencia”, mediante Memorando Nro. FGE-CGGC-2026-00013-M, de fecha 06 enero de 2026.




Ximena del Carmen Coello Martínez
DIRECTORA DE POLÍTICA CRIMINAL
FISCALÍA GENERAL DEL ESTADO

INSTRUMENTO TÉCNICO DE POLÍTICA CRIMINAL - CIBERDELINCUENCIA

FGE

FISCALÍA GENERAL DEL ESTADO
ECUADOR

FISCALÍA GENERAL DEL ESTADO
COORDINACIÓN GENERAL DE GESTIÓN DEL CONOCIMIENTO
DIRECCIÓN DE POLÍTICA CRIMINAL
QUITO - ECUADOR