



Doi: <https://doi.org/10.70577/asce.v5i4.1132>

Recibido: 2026-09-11

Aceptado: 2026-09-25

Publicado: 2026-10-28

La funcionalidad informática como bien jurídico penal y su recepción en el Código Orgánico Integral Penal Ecuatoriano

Computer System Functionality as a Protected Criminal Law Interest and Its Reception in Ecuador's Comprehensive Organic Criminal Code

Autor(s)

Rosario Guillermina Franco Jaramillo¹

1 Jueza provincial de la Sala Especializada de lo Penal
de la Corte Provincial de Justicia del Guayas.

Magíster en Derecho Constitucional y Derecho Penal.

drarosariofranco1964@gmail.com

<https://orcid.org/0009-0005-7701-7817>

Corte Provincial de Justicia del Guayas

Guayaquil - Ecuador

Cómo citar

Franco Jaramillo, R. G. (2026). La funcionalidad informática como bien jurídico penal y su recepción en el Código Orgánico Integral Penal ecuatoriano. *ASCE MAGAZINE*, 5(4), 322–353. <https://doi.org/10.70577/asce.v5i4.1132>

Resumen

Que una conducta se cometa mediante un sistema informático no basta para saber qué bien jurídico lesiona. De esa constatación partió el artículo, que examinó si la funcionalidad informática operaba como bien jurídico penal en el Código Orgánico Integral Penal ecuatoriano (COIP) y con qué alcance. Fue un estudio jurídico doctrinal y documental, de alcance descriptivo y analítico. Sus materiales fueron los artículos 229 a 234.4, las reformas de 2021 y 2026 y las relaciones de esas normas con otros tipos penales, leídos con interpretación literal, sistemática y teleológica. La propuesta de Mayer Lux (2017) sirvió para separar el interés protegido de los datos y sistemas sobre los que recayó la conducta. El análisis distinguió el interés predominante, su relación con la funcionalidad y la forma de protección del bien jurídico. La protección resultó implícita y parcial. Donde más se notó fue en el artículo 232 y en la agravación del 234.2. El acceso no autorizado del artículo 234 se leyó como tutela del control legítimo del sistema, anterior a cualquier daño operativo. En las demás modalidades pesaron más la intimidad, el patrimonio, la autenticidad o la información pública reservada. Tres ejemplos hipotéticos marcaron la frontera entre estafa, manipulación informática y ataque a servicios críticos. El trabajo concluyó que la sección del COIP respondía a un modelo híbrido y que la funcionalidad podía servir como criterio de interpretación, siempre dentro de la legalidad y de la presunción de inocencia. Su aplicación en los procesos penales quedó fuera del estudio.

Palabras clave: Derecho penal; Derecho de la informática; Protección de datos; Integridad de la información; Ecuador



Abstract

Committing an offence through a computer system does not, by itself, reveal which legal interest the offence harms. This article examined whether computer system functionality operated as a protected legal interest under Ecuador's Comprehensive Organic Criminal Code (COIP), and to what extent. The study followed a doctrinal and documentary legal design with a descriptive and analytical scope. It read Articles 229 to 234.4, the 2021 and 2026 amendments and their links with other offences through literal, systematic and purposive interpretation. Mayer Lux's (2017) work served to separate the protected interest from the data and systems targeted by the conduct. For each modality, the study distinguished the predominant interest, its relationship with functionality and the form of protection. The result was implicit and partial protection. Functionality appeared most clearly in Article 232 and in the aggravating provision of Article 234.2; unauthorised access under Article 234 was read as protecting legitimate control over the system prior to any operational damage. In the remaining modalities, privacy, property, authenticity or classified public information carried more weight. Three hypothetical cases helped draw the line between fraud, computer manipulation and attacks on critical services. The study concluded that the provisions reflected a hybrid model and that functionality could serve as an interpretive criterion, always within the limits of legality and the presumption of innocence. It did not assess the application of these criteria in criminal proceedings.

Keywords: Criminal law; Computer law; Data protection; Information integrity; Ecuador

Introducción

Que un sistema informático intervenga en un hecho no resuelve cómo debe calificarse penalmente, aunque esos sistemas sostengan buena parte de la vida personal, económica e institucional. A veces el medio digital solo sirve para lesionar la intimidad o el patrimonio. En otros casos la operación informática forma parte de la ejecución, y hay conductas que se dirigen contra las condiciones que permiten funcionar al propio sistema. La expresión delito informático agrupa, por eso, problemas de clasificación muy diferentes. Miró Llinares (2012) advierte la amplitud de la criminalidad que se desarrolla en el ciberespacio, mientras que Navarro-Dolmestch (2023a) propone examinar si el procedimiento informático es esencial en la descripción de la conducta. Aun así, la tecnología presente en el hecho no dice qué bien jurídico se protege. Eso depende de la estructura del tipo y del interés protegido, que deben mirarse a la vez.

En Ecuador, la pregunta tiene una ubicación precisa. Los artículos 229 a 234.4 del Código Orgánico Integral Penal (COIP) integran la Sección Tercera del Capítulo III, dedicada a los delitos contra la seguridad de los activos de los sistemas de información y comunicación (Asamblea Nacional del Ecuador, 2014). Esa ubicación plantea un problema dogmático. Hay que determinar si la funcionalidad de los sistemas explica por igual todas las figuras de la sección o si su tutela concurre con intereses diferentes. La pregunta alcanza también a los artículos 178, 186 y 190, que están fuera de esa sección pero pueden coincidir con las figuras informáticas. Su respuesta se nota en la práctica. De ella depende qué tipo se aplica, cómo se resuelven las coincidencias entre normas y hasta dónde puede llegar la interpretación sin incurrir en la analogía que prohíbe el artículo 13 del COIP (Asamblea Nacional del Ecuador, 2014, art. 13). Sin un criterio claro, la elección de la norma puede acabar por depender de la herramienta utilizada.

La reforma de 2021 sustituyó los artículos 230, 232 y 234. Incorporó también la falsificación informática, la agravación vinculada con funciones sociales críticas, la responsabilidad de personas jurídicas y las definiciones de la sección (Asamblea Nacional del Ecuador, 2021, arts. 12–15). La de 2026 añadió al artículo 232 una exclusión para el acceso, la prueba o la evaluación consentidos expresamente con fines de verificación o fortalecimiento de la seguridad, siempre que se sigan los procedimientos y registros aplicables (Asamblea Nacional del Ecuador, 2026, art. 11). Esta cláusula obliga a precisar cómo se relacionan la autorización y la tipicidad.

El marco internacional también cambió. Ecuador se adhirió al Convenio de Budapest el 12 de diciembre de 2024, y el tratado entró en vigor para el país el 1 de abril de 2025 (Consejo de Europa, 2024, 2026). El Convenio gira en torno a la confidencialidad, la integridad y la disponibilidad de datos y sistemas. Es un punto de comparación útil. Pero sus categorías no se convierten en bienes jurídicos autónomos ni sustituyen los elementos que el legislador ecuatoriano exige para cada infracción (Consejo de Europa, 2001a, 2001b).

La doctrina ya ha trabajado la funcionalidad informática como interés protegido. Mayer Lux (2017, 2018b) la propone para explicar un núcleo de la protección penal. Su propuesta vincula las condiciones de operación de los sistemas con los intereses que estos hacen posibles, y admite que una misma conducta afecte, además, otros bienes. La doctrina sobre la Ley chilena n.º 21.459 ha estudiado la esencialidad del procedimiento informático y los límites del acceso autorizado (Mayer Lux y Vera Vega, 2022; Navarro-Dolmestch, 2023a, 2023b), aunque sobre tipos penales cuya estructura no coincide necesariamente con la ecuatoriana. En Ecuador, Ponce Tubay (2024) cuestiona la precisión de las definiciones legales y su alineación con los estándares internacionales. Ramos Mera (2026) propone la funcionalidad de los sistemas como fundamento dogmático común, con atención a los artículos 230, 232 y 234, sin desconocer que concurren otros intereses.

Con esos antecedentes, la pregunta sigue abierta. Falta saber cómo se distribuye la protección de la funcionalidad entre las distintas modalidades del COIP y qué límites resultan de esa distribución. Este trabajo toma como punto de partida la distinción que Ramos Mera (2026, p. 39) hace entre grupos de modalidades del artículo 230 y amplía la comparación al conjunto de los artículos 229 a 234.4. Examina, además, la agravación del artículo 234.2, el límite incorporado en 2026 y las relaciones con los artículos 178, 186 y 190. La funcionalidad sirve aquí como herramienta de reconstrucción dogmática, y su utilidad debe probarse modalidad por modalidad. En cada una, el análisis busca qué elementos justifican atribuirle predominio y cuáles obligan a explicarla desde otro interés, sobre todo en los tipos patrimoniales, las falsedades y la información reservada. Los supuestos hipotéticos que acompañan el análisis muestran los límites de las interpretaciones propuestas.

La pregunta de investigación es directa. ¿En qué medida la funcionalidad informática constituye un bien jurídico protegido en el COIP? El objetivo general es determinar el alcance de esa categoría a partir de los artículos 229 a 234.4 y de sus relaciones con otros delitos que pueden cometerse mediante tecnologías digitales. Los objetivos específicos son cuatro: delimitar el concepto de delito

informático; distinguir el bien jurídico del objeto material; identificar los intereses tutelados por las disposiciones examinadas; y formular criterios interpretativos y de política criminal compatibles con la legalidad, la lesividad, la proporcionalidad y la presunción de inocencia. Después de la fundamentación teórica y la metodología, el artículo expone los resultados, los discute según esos cuatro objetivos y cierra con las conclusiones.

Fundamentación teórica

Delito informático, objeto material y bien jurídico

El concepto de delito informático puede construirse con distintos criterios. Mayer Lux (2018b, pp. 160–161) distingue un sentido amplio y otro estricto. En el estricto incluye las conductas que afectan el soporte lógico, como el sabotaje, el espionaje y el fraude informático. La autora limita además su estudio a conductas realizadas mediante redes, un recorte que este trabajo no adopta como requisito de los tipos ecuatorianos. Navarro-Dolmestch (2023a, pp. 674–675) prefiere otro criterio, que el procedimiento informático sea esencial en la conducta o en sus modalidades de ejecución. Visto así, una infracción es informática aunque su bien jurídico principal no sea nuevo, de modo que la estructura tecnológica del delito y el interés que protege deben examinarse por separado. En este estudio el derecho comparado se usa solo como contraste, y para ello recurrimos a Ojeda-Pérez et al. (2010). Los autores reconstruyen el cambio de la noción de delito informático y su incorporación a la legislación colombiana. Lo construido allí responde a los tipos penales de Colombia y no puede trasladarse al COIP sin revisar cómo describe cada conducta la ley ecuatoriana. Algo parecido ocurre con los estándares internacionales que reúne Gercke (2014). Sirven para comparar y armonizar. Sin embargo, no indican qué exigen los artículos 232 o 234 para que exista delito, y esa respuesta solo está en el texto del Código.

Los datos, los programas, los dispositivos y los sistemas, en este tipo de delitos, se constituyen en el objeto material, es decir, aquello sobre lo que recae la conducta. El bien jurídico es el interés que la norma protege frente a una lesión o un peligro, y no debe confundirse con el objeto material. Si esto ocurriera, cualquier soporte digital parecería un interés penal autónomo (Mir Puig, 2016). En el COIP, el artículo 229 lo señala con suma claridad. Quien revela información registrada lesiona la intimidad, aunque actúa sobre un archivo informático. En el fraude informático del artículo 231 puede predominar el patrimonio, aunque sin manipular el sistema informático la conducta no podría

ejecutarse. En cuanto a la estafa, Mayer Lux y Oliver Calderón (2020) insisten en separarla del fraude informático, porque en ella interviene el error de una persona. Aun así, el fraude no pierde su carácter de delito informático. Lo que cambia es el bien jurídico, y de él depende cómo se leen los elementos del tipo y cómo se resuelven las relaciones entre normas. Pero el bien jurídico tiene también un límite. Ningún interés, por valioso que sea, permite sancionar una conducta que la ley no describe (Mir Puig, 2016).

En el delito de acceso no autorizado, separar el objeto material del bien jurídico es de suma importancia. En ese terreno, Medina Schulz (2014) examina la estructura típica del acceso y la necesidad de delimitarla. Ese planteamiento lleva a separar el ingreso o la permanencia ilegítimos de lo que pueda ocurrir después, sea una copia de información, una transferencia patrimonial o una interrupción. Cada uno de esos hechos requiere su propia prueba y su propia subsunción. Ninguno puede presumirse por la capacidad técnica de la persona investigada. Así lo exigen la presunción de inocencia y el deber de probar los elementos de la infracción aplicable (Asamblea Nacional del Ecuador, 2014, art. 5).

La funcionalidad informática como interés protegido

Según Mayer Lux (2017, p. 255), la funcionalidad informática comprende las condiciones que permiten almacenar, tratar y transferir datos dentro de un riesgo tolerable. Su protección es instrumental, porque sostiene actividades e intereses que dependen de los sistemas. Esa protección posee, además, una dimensión colectiva, que puede concurrir con la lesión de bienes jurídicos individuales. Partimos de esa noción para examinar cómo opera en cada modalidad del COIP, y debemos dejar en claro que, aunque un sistema falle, eso no significa que se haya cometido un delito. Una falla en la actualización del sistema puede ocasionar que un servidor deje de funcionar, pero ese fallo es propio de su funcionamiento y no constituye una conducta típica. Como advierte la misma autora, valorar la funcionalidad exige mirar el sistema comprometido, la entidad de la afectación y los elementos de la norma aplicable.

Este trabajo usa la confidencialidad, la integridad y la disponibilidad como dimensiones técnicas de la protección funcional, en diálogo con Mayer Lux (2017, pp. 251–252) y Ramos Mera (2026, p. 38). La confidencialidad tiene que ver con el control sobre el acceso, el uso y la divulgación de la información, y puede verse afectada aunque el sistema siga en operación. Con la integridad se preservan los datos y el procesamiento frente a alteraciones no autorizadas. Y la disponibilidad

significa poder acceder a los recursos y usarlos cuando se necesitan. Estas dimensiones sirven para precisar la afectación técnica, pero no deciden cuál es el bien jurídico predominante ni si alguna merece autonomía jurídica. Eso hay que justificarlo a partir de cada tipo. El informe explicativo del Convenio de Budapest permite contrastar estas condiciones técnicas con las actividades legítimas que quedan fuera del reproche penal (Consejo de Europa, 2001b).

La disponibilidad pesa más en los sistemas de los que dependen servicios continuos. El informe ENISA Threat Landscape 2025 analizó 4.875 incidentes ocurridos en el contexto europeo entre el 1 de julio de 2024 y el 30 de junio de 2025 (European Union Agency for Cybersecurity [ENISA], 2025). Es un dato europeo. Muestra cuánto importa la continuidad operativa, pero no permite estimar la criminalidad informática ni el funcionamiento de la justicia penal en Ecuador. El Cybersecurity Framework 2.0 del NIST apunta en la misma dirección. Organiza la gestión del riesgo en seis funciones (gobernar, identificar, proteger, detectar, responder y recuperar), y con ello confirma que la protección de los sistemas va mucho más allá de la sanción (National Institute of Standards and Technology [NIST], 2024). El alcance penal de la funcionalidad depende, entonces, de cómo cada tipo conecta la conducta con el uso legítimo del sistema y con intereses como la intimidad, el patrimonio o la autenticidad.

Convenio de Budapest y dimensión constitucional

El Convenio de Budapest es más que un catálogo de delitos: además de los tipos penales, regula definiciones, reglas procesales y la cooperación entre los Estados. En su parte sustantiva separa dos grupos: los artículos 2 a 6 reúnen, bajo la confidencialidad, la integridad y la disponibilidad, el acceso y la interceptación ilícitos, los ataques a los datos y a los sistemas y el abuso de dispositivos; los artículos 7 y 8 recogen la falsificación y el fraude informáticos (Consejo de Europa, 2001a). Su informe explicativo señala el riesgo propio de cada conducta y advierte que el derecho penal no debe alcanzar las actividades legítimas vinculadas con los sistemas informáticos, pero no adopta una sola postura sobre el bien jurídico protegido (Consejo de Europa, 2001b).

El artículo 2 del Convenio deja a cada Estado la decisión de exigir condiciones adicionales para el acceso ilícito, como la infracción de medidas de seguridad o una intención específica (Consejo de Europa, 2001a). Hay ordenamientos que exigen romper una barrera técnica y otros que no. El numeral 1 del artículo 234 del COIP se construye sobre la falta de autorización y la permanencia contraria a la voluntad del titular legítimo, y no menciona la vulneración de medidas de seguridad.

En cuanto al derecho comparado, ningún requisito ajeno puede trasladarse a nuestro tipo, porque el artículo 13 del COIP exige una interpretación estricta y prohíbe la analogía desfavorable (Asamblea Nacional del Ecuador, 2014, art. 13). El Convenio, más bien, orienta al legislador y ayuda en el análisis sistemático, pero no autoriza al juzgador a crear delitos ni a ampliar las condiciones de una sanción.

La sentencia del Tribunal Constitucional Federal de Alemania, de fecha 27 de febrero de 2008, conocida como BVerfGE 120, 274, es relevante, puesto que allí el Tribunal reconoció que el derecho general de la personalidad comprende la protección de la confidencialidad y la integridad de los sistemas de tecnologías de la información, y vinculó esa garantía con la vida privada y con la autonomía personal frente a una infiltración estatal encubierta dirigida a obtener datos (Bundesverfassungsgericht, 2008). Se trata de una garantía de la persona frente al Estado, y su aporte a nuestro estudio es mostrar que la confidencialidad y la integridad de los sistemas tienen también una dimensión constitucional. Para el juzgador ecuatoriano, este fallo puede considerarse un referente cuando se encuentren en juego la intimidad y los datos personales. En cuanto al bien jurídico protegido en relación con cada delito informático, y si tiene o no carácter colectivo, deberá recurrirse a nuestra legislación penal vigente.

La jurisprudencia de la Corte Constitucional del Ecuador ofrece dos referencias para delimitar este análisis. En la Sentencia 2064-14-EP/21, dictada en un hábeas data, la Corte examinó el alcance de la protección de los datos personales, el consentimiento de su titular y el derecho a la intimidad. El caso nació del tratamiento y la divulgación no consentidos de unas fotografías íntimas, que la Corte reconoció como datos personales (Corte Constitucional del Ecuador, 2021). Un año después, en la Sentencia 77-16-IN/22, analizó el régimen de la interceptación de comunicaciones y datos informáticos y su relación con los derechos a la intimidad y a la inviolabilidad de las comunicaciones (Corte Constitucional del Ecuador, 2022). Las dos decisiones importan aquí por lo que dicen sobre datos, intimidad y comunicaciones. Ninguna reconoce la funcionalidad como bien jurídico penal autónomo, ni define su alcance en los artículos del COIP que examina este trabajo.

En el ámbito internacional, la Asamblea General de las Naciones Unidas aprobó el 24 de diciembre de 2024, mediante la Resolución 79/243, la Convención de las Naciones Unidas contra la Ciberdelincuencia. En este apartado, su importancia es de contexto, ya que su título anuncia dos ejes: la lucha contra determinados delitos cometidos mediante sistemas de tecnología de la

información y las comunicaciones, y la transmisión de pruebas en forma electrónica de delitos graves (Asamblea General de las Naciones Unidas, 2024). El primero identifica las conductas según el medio empleado, un criterio que, como ya señalamos, no basta para saber qué bien jurídico se protege. El segundo es relevante, ya que Ecuador firmó la Convención en Hanói el 25 de octubre de 2025, aunque aún no la ha ratificado, y el tratado tampoco está en vigor (Naciones Unidas, 2026). Cuando lo esté, ampliará la cooperación entre Estados para obtener y compartir pruebas electrónicas. Dichas pruebas deberán cumplir con las mismas exigencias de legalidad, contradicción y cadena de custodia que cualquier otra prueba. No debemos dejar de advertir que ninguno de esos ejes autoriza a ampliar los tipos penales que establece el COIP.

Material y Métodos

En este trabajo se planteó una investigación jurídica de tipo doctrinal y documental, con enfoque cualitativo y alcance descriptivo y analítico. Su objetivo fue observar qué interés protegía cada uno de los delitos informáticos de la Sección Tercera del COIP, artículos 229 a 234.4, y en qué medida ese interés coincide con la funcionalidad informática. Para ello reunimos legislación, doctrina, sentencias publicadas y documentos institucionales. El criterio de selección fue uno solo: que cada norma, obra doctrinal, sentencia o documento institucional tratara de manera directa el concepto de delito informático, la funcionalidad, el acceso no autorizado o la frontera entre fraudes e interferencias.

El análisis se centró en los artículos 229 a 234.4 del COIP, que se examinaron numeral por numeral e inciso por inciso. Se incorporaron, además, los artículos 5 y 13, que aportaron los principios procesales y las reglas de interpretación, y los artículos 20 y 21, que regulaban el concurso de infracciones. Los artículos 178, 186, 190 y 366 se revisaron por contener conductas que podían coincidir con las informáticas, desde la violación de la intimidad hasta el terrorismo. La fecha de corte fue el 22 de mayo de 2026, día en que se publicó en el Registro Oficial la Ley Orgánica para el Fortalecimiento de la Ciberseguridad. Como ningún documento recogía completo el texto vigente a esa fecha, este se reconstruyó a partir del texto consolidado del COIP, con última reforma general indicada al 18 de septiembre de 2024, de la ley reformativa de 2021 y del artículo 11 de la ley de 2026.

En el ámbito internacional se consultaron el Convenio de Budapest, su informe explicativo y el registro de adhesiones del Consejo de Europa, así como la Resolución 79/243 de la Asamblea General de las Naciones Unidas y el registro de firmas y ratificaciones de la Convención que esa resolución aprobó. En cuanto a la jurisprudencia, se analizaron la sentencia alemana BVerfGE 120, 274 y las sentencias 2064-14-EP/21 y 77-16-IN/22 de la Corte Constitucional del Ecuador. La doctrina incluyó a autores cuyos trabajos tenían como base el concepto de delito informático, la funcionalidad de los sistemas y el bien jurídico en estos delitos. De los quince trabajos doctrinales considerados, nueve procedían de Chile (Lara et al., 2014; Mayer Lux, 2017, 2018a, 2018b; Mayer Lux y Oliver Calderón, 2020; Mayer Lux y Vera Vega, 2022; Medina Schulz, 2014; Navarro-Dolmestch, 2023a, 2023b). Su peso respondió a que en ese país la Ley 21.459, de 2022, sustituyó a la ley de delitos informáticos de 1993 y dio lugar a nuevos estudios (Mayer Lux y Vera Vega, 2022, p. 267). Completaron esta selección una obra general de derecho penal (Mir Puig, 2016), una monografía española sobre cibercrimen (Miró Llinares, 2012), dos estudios ecuatorianos (Ponce Tubay, 2024; Ramos Mera, 2026), uno colombiano (Ojeda-Pérez et al., 2010) y el informe de Gercke (2014) para la Unión Internacional de Telecomunicaciones. La revisión bibliográfica, que no se cerró con el corte normativo, incorporó el estudio de Ramos Mera, publicado en 2026.

En este trabajo se formularon cinco preguntas sobre cada artículo: qué conducta describía, sobre qué recaía, qué intención exigía, qué afectación requería y qué interés protegía con preferencia. Con sus respuestas, cada modalidad se clasificó en dos ejes, que se examinaron por separado. El primero fue su vínculo con la funcionalidad. Se calificó de directo cuando el uso u operación legítimos del sistema explicaban el núcleo del injusto, como ocurrió en el artículo 232. Fue instrumental cuando la funcionalidad servía a la protección de otro interés, como el patrimonio en el artículo 231, y concurrente cuando su afectación podía acompañar un injusto de fundamento distinto, como en el artículo 229, cuyo núcleo era la intimidad. El segundo eje fue la forma en que cada tipo protegía el bien jurídico predominante: si exigía que ese bien resultara afectado o si sancionaba actos anteriores a cualquier daño. Esa clasificación se volcó en la Tabla 2.

El análisis de cada artículo se realizó con tres criterios: literal, sistemático y teleológico. Desde el punto de vista literal, se examinaron los verbos y lo que el tipo exigía, como el «acceda» y el «se mantenga» del artículo 234. En el plano sistemático, cada artículo se comparó con otras normas del COIP, de la misma sección y de fuera de ella; el fraude del artículo 231, por ejemplo, se



contrastó con la estafa del 186 y con la apropiación fraudulenta del 190. Desde el criterio teleológico, y con apoyo en la doctrina, se propuso qué interés protegía cada uno.

A lo largo del análisis se evitaron dos confusiones frecuentes. La primera, entre la finalidad y el resultado. En el numeral 2 del artículo 234 se consideró suficiente que el autor accediera con alguna de las intenciones allí previstas, como desviar el tráfico de datos, aunque no llegara a hacerlo; en el artículo 234.2, en cambio, se exigió comprobar que el sistema sufrió una perturbación grave o duradera. La segunda, entre lo informático y la funcionalidad: una manipulación del sistema hecha para obtener dinero era, en el fondo, un ataque al patrimonio. Cuando dos normas coincidían, se compararon sus elementos hasta establecer si había concurso aparente o concurso de infracciones. Para mostrar esas decisiones en la práctica se construyeron tres casos hipotéticos: la alteración de un programa bancario que produjo una transferencia no consentida, un correo engañoso que llevó a la víctima a disponer de su patrimonio y el bloqueo deliberado del sistema informático de un hospital. Ninguno provino de un expediente judicial; su función fue argumentativa.

El trabajo presentó límites claros, puesto que no midió la cantidad de delitos informáticos cometidos ni perseguidos, y tampoco revisó expedientes ni informes periciales. Sus conclusiones se formularon en el plano normativo y doctrinal, y no permitieron pronunciarse sobre la impunidad, los errores forenses ni los sesgos. La doctrina se seleccionó de forma intencional, por lo que la revisión bibliográfica no fue exhaustiva. La revisión normativa se ciñó a las disposiciones examinadas y no reconstruyó la historia completa de las reformas del COIP.

Resultados

Las reformas de 2021 y 2026 como puntos de inflexión

La Tabla 1 sintetizó los cambios de 2021 y 2026 relevantes para examinar la funcionalidad y sus límites.

Tabla 1

Cambios introducidos por las reformas de 2021 y 2026 en la sección de delitos informáticos del COIP

Disposición	Cambio normativo	Relevancia para el análisis
230	Sustitución en 2021; cinco numerales de estructura heterogénea.	Exigió distinguir captación, direccionamiento engañoso, información de tarjetas e instrumentos.
232	Sustitución en 2021; conductas de afectación y propósito de obstaculización grave.	Permitió identificar protección funcional directa sin confundir finalidad y resultado.
232 inciso final	Adición en 2026 para ciertas prácticas de seguridad consentidas.	Delimitó la tipicidad bajo las condiciones expresas de la reforma.
234	Sustitución en 2021; acceso o permanencia y modalidades con finalidad ulterior.	Permitió separar los requisitos de cada numeral.
234.1	Incorporación de falsificación informática en 2021.	Vinculó esencialidad informática y tutela predominante de autenticidad.
234.2	Agravación incorporada en 2021 para los delitos de los artículos 232, 234 y 234.1.	Exigió distinguir la perturbación grave o duradera de los elementos del delito cometido.
234.3	Responsabilidad de personas jurídicas incorporada en 2021.	Remitió a las reglas de los artículos 49 y 71.
234.4	Definiciones incorporadas en 2021.	Precisó nociones técnicas relevantes para los tipos.

Nota. *Elaboración propia a partir del COIP y de las reformas de 2021 (arts. 12–15) y 2026 (art. 11). La columna final recoge resultados interpretativos de este estudio.*

El examen de la reforma de 2021 identificó tres cambios sustantivos para este análisis. La reforma cambió la estructura de los artículos 230, 232 y 234, incorporó la falsificación informática y añadió la agravación por perturbaciones en sistemas vinculados con funciones sociales críticas. En el artículo 232, el análisis separó las conductas materiales de afectación del propósito de obstaculizar gravemente el funcionamiento. Así, distinguió la finalidad del resultado de perturbación grave o duradera que exigía el artículo 234.2 (Asamblea Nacional del Ecuador, 2021, arts. 12–15). A eso se suma que la reforma de 2026 agregó al artículo 232 un inciso final, por el cual dejaron de constituir delito el acceso, la prueba o la evaluación consentidos de forma expresa por el titular o

responsable del sistema, con fines de verificación o fortalecimiento de la seguridad y conforme a los procedimientos y registros de la Ley Orgánica para el Fortalecimiento de la Ciberseguridad. Es el caso de la empresa que contrata una prueba de penetración, es decir, un ataque simulado contra su propio sistema para detectar sus fallas de seguridad. Aunque el inciso agregado mencionaba el acceso consentido, no se usó para redefinir el artículo 234 (Asamblea Nacional del Ecuador, 2026, art. 11).

El artículo 234 presentó dos numerales. Al contrastarlos se descartó que toda modalidad de acceso exigiera un fin común. El numeral 1 contempló el acceso sin autorización o la permanencia contraria a la voluntad del titular legítimo. El numeral 2 añadió cuatro finalidades concretas: explotar el acceso, modificar un portal web, desviar el tráfico de datos o voz u ofrecer servicios sin pagarlos. En la práctica, en cuanto al primer numeral no hizo falta probar qué buscaba quien ingresó al sistema informático. En relación con el segundo, la finalidad concreta debió acreditarse, porque formaba parte del tipo. El solo ingreso no demostraba para qué se había entrado; esa intención tuvo que probarse con hechos externos, como registros que mostraran el desvío del tráfico o la modificación del portal. Si no se probaba, la conducta solo podía encuadrarse en el numeral 1 (Asamblea Nacional del Ecuador, 2021, art. 14).

En el artículo 234.1 predominaron la autenticidad y la confianza en el tráfico jurídico, aunque el tratamiento informático fuera esencial para cometer la falsificación. El artículo distinguió dos conductas: producir datos o documentos no genuinos con intención de engañar en las relaciones jurídicas, y usar esos documentos con intención de causar un perjuicio u obtener un beneficio ilegítimo. Un contrato electrónico alterado para aparentar una deuda inexistente sirvió para ilustrar la primera; presentarlo ante un juez para cobrarla, la segunda. El artículo 234.2, en cambio, no creó un delito nuevo. Agravó en un tercio de su pena máxima los hechos de los artículos 232, 234 y 234.1 cuando lograban perturbar de forma grave o duradera un sistema que apoyaba funciones sociales críticas, como la salud o los servicios públicos. De ahí que, en cada caso, hubiera que probar primero el delito cometido y después, por separado, dos hechos más: que la perturbación fue grave o duradera y que el sistema sostenía una de esas funciones, como la atención de un hospital (Asamblea Nacional del Ecuador, 2021, art. 15).

Como contraste de lo señalado, recurrimos al Convenio de Budapest. El acceso no consentido del artículo 234 se relacionó con el artículo 2 del Convenio; el ataque a la integridad de los sistemas informáticos del artículo 232, con la interferencia en el sistema del artículo 5, y la falsificación

informática del artículo 234.1, con el artículo 7. El fraude informático del artículo 231 encontró en el artículo 8 del Convenio su equivalente, aunque ese delito ya figuraba en el COIP desde 2014 y no provino de la reforma de 2021. Estas semejanzas no significaron igualdad de normas. El artículo 2 del Convenio, por ejemplo, permitía exigir la vulneración de medidas de seguridad, y el artículo 234 no la exigió; por ende, cada tipo penal del COIP se interpretó de forma independiente, con sus propios elementos y no con los del Convenio de Budapest (Consejo de Europa, 2001a, 2001b).

Bienes jurídicos predominantes en los artículos 229 a 234.4

La Tabla 2 distinguió el interés predominante, el vínculo funcional y la forma de protección del bien jurídico. Estas categorías expresaron una interpretación del corpus. No se trataron como grados de una misma escala, porque la protección anticipada pudo coexistir con un vínculo funcional directo o instrumental.

Tabla 2

Bien jurídico predominante y protección de la funcionalidad en los artículos 229 a 234.4 del COIP

Norma	Modalidad examinada	Interés predominante	Vínculo funcional	Forma de protección
229	Revelar información registrada, con provecho y con afectación intencional de la intimidad.	Secreto, intimidad y privacidad.	Concurrente, porque la información estaba reservada.	Bastaba revelar; no exigía dañar el sistema.
230.1	Interceptar datos sin orden judicial, en provecho propio o ajeno.	Intimidad y secreto de las comunicaciones.	Concurrente, por la reserva de la comunicación.	Bastaba interceptar; no exigía interrumpir el servicio.
230.2–3	Desviar a la víctima hacia sitios falsos y distribuir los medios para hacerlo.	Funcionalidad, como confianza de llegar al sitio correcto.	Directo.	El numeral 2 exigía inducir a la persona; el 3 sancionaba actos previos.
230.4–5	Clonar tarjetas y producir o poseer los medios para hacerlo.	Patrimonio, a través de los medios de pago.	Instrumental, al servicio del patrimonio.	Anticipada; no exigía que la víctima perdiera dinero.
231 inciso 1	Manipular un sistema con ánimo de lucro para lograr una transferencia no consentida.	Patrimonio.	Instrumental, porque la manipulación servía a la transferencia.	Exigía la manipulación y la finalidad patrimonial.

Norma	Modalidad examinada	Interés predominante	Vínculo funcional	Forma de protección
231 inciso 2	Prestar la propia cuenta para recibir el dinero transferido, la llamada cuenta puente.	Patrimonio.	Instrumental, por la transferencia de la que provenía el dinero.	Exigía facilitar la cuenta con intención de recibir el dinero.
232	Dañar un sistema para obstaculizar su funcionamiento, o distribuir programas maliciosos.	Funcionalidad.	Directo.	Exigía el daño; el inciso 2 sancionaba actos previos.
233	Destruir, obtener o revelar información pública clasificada.	Información reservada y seguridad del Estado, según inciso.	Concurrente si compromete datos o sistemas.	Distinta en cada inciso, según la conducta y el autor.
234	Entrar al sistema o permanecer en él sin autorización, y las finalidades del numeral 2.	Control legítimo sobre el sistema.	Directo.	Anticipada; bastaba el acceso, aunque no hubiera daño.
234.1	Crear datos o documentos falsos y usarlos para engañar o perjudicar.	Autenticidad y confianza jurídica.	Concurrente, por la alteración de los datos.	Exigía la creación o el uso con las finalidades de la ley.
234.2	Perturbar de forma grave o duradera un sistema que sostenía funciones sociales críticas.	Los del delito cometido, más la funcionalidad colectiva.	Directo; reforzaba la protección de la funcionalidad.	Resultado grave o duradero que se suma al delito cometido.
234.3–4	Responsabilidad de personas jurídicas y definiciones.	Reglas complementarias, no tipos autónomos.	Sin protección independiente.	Se aplicaban a los delitos de la sección.

Nota. *Elaboración propia a partir de los artículos 229 a 234.4 del COIP y sus reformas, con apoyo en Mayer Lux (2017) y Ramos Mera (2026, pp. 36–39). La distribución del interés predominante y del vínculo funcional constituye la propuesta interpretativa de este estudio. La última columna identifica la estructura de protección sin añadir resultados que la ley no exige.*

El artículo 229 mostró una protección vinculada con el secreto, la intimidad y la privacidad, y el análisis consideró la revelación de información registrada, el provecho propio o ajeno y la afectación intencional de esos intereses. La base de datos actuó como soporte u objeto de la conducta. De su carácter informático no se dedujo que hiciera falta un daño a la operación del sistema (Asamblea Nacional del Ecuador, 2014, art. 229).

El artículo 230 reunió cinco numerales de distinto fundamento. En el primero predominaron la intimidad y el secreto de las comunicaciones, por las conductas de captación, la falta de orden judicial previa y el provecho exigido. En cuanto a los numerales 2 y 3, su núcleo fue la fiabilidad del acceso digital, tal como lo desarrolló Ramos Mera (2026, p. 39). Dicho de forma simple, y a

modo de ejemplo, lo protegido fue que quien ingresaba a la dirección electrónica de su banco, o abría el enlace de un correo que le solicitaba ingresar para una consulta o transacción, no terminara en una dirección falsa. El numeral 2 no se limitó a los servicios financieros, porque incluyó también los sitios personales o de confianza; de ahí que no se atribuyera al conjunto un predominio patrimonial general. El numeral 3 sancionó una etapa previa, la posesión, venta o distribución de programas o contenidos destinados a provocar ese desvío, antes de que alguien fuera engañado (Asamblea Nacional del Ecuador, 2014, art. 230).

Analizados los numerales 4 y 5, observamos que predominó la protección del patrimonio. Ambos se refirieron a tarjetas de crédito, débito o pago: el 4 sancionó a quien copiaba, clonaba o comercializaba la información de sus bandas magnéticas o chips, y el 5, a quien producía, distribuía o poseía los dispositivos o programas destinados a hacerlo, la conducta conocida como clonación de tarjetas. Ninguno exigió que la víctima perdiera dinero; bastó con actuar sobre la información o sobre los medios para obtenerla, de modo que esa protección se adelantó. En este punto coincidimos con Ramos Mera (2026, p. 39) en cuanto a que estos numerales tenían relación con la fiabilidad de las transacciones, pero no en el lugar que asignó al patrimonio, al que ubicó entre las afectaciones posteriores. Como el objeto de la conducta eran las tarjetas de débito o crédito y los medios de pago, consideramos que el patrimonio estaba protegido desde el inicio, aunque de forma anticipada. Con esto se hizo evidente que el título del artículo, «Interceptación ilegal de datos», no describía bien sus cinco numerales: la clonación de una tarjeta, por ejemplo, no intercepta ninguna comunicación (Asamblea Nacional del Ecuador, 2014, art. 230).

En el artículo 231 predominó el patrimonio, pero al realizar nuestro análisis encontramos dos conductas que no podían tratarse igual. El primer inciso reprimía a quien, con ánimo de lucro, alteraba, manipulaba o modificaba el funcionamiento de un programa o sistema para procurarse la transferencia o apropiación no consentida de un activo ajeno. El segundo ya involucraba a la persona que facilitaba los datos de su propia cuenta bancaria para recibir el dinero de esa transferencia, la llamada cuenta puente. Quien prestaba su cuenta no manipulaba ningún sistema, así que su responsabilidad exigió probar su intención de captar ilegítimamente el activo, no la manipulación. Aun con predominio patrimonial, el artículo 231 no dejó de ser un delito informático, ya que lo que hizo posible la transferencia fue la manipulación del sistema (Asamblea Nacional del Ecuador, 2014, art. 231; Mayer Lux y Oliver Calderón, 2020).

El artículo 232 ofreció el núcleo más directo de protección funcional. En él la funcionalidad pasó a ser lo protegido. Su primer inciso reprimió a quien dañaba, borraba, alteraba, suspendía o causaba el mal funcionamiento de contenido digital, sistemas, dispositivos o infraestructura tecnológica, con el propósito de obstaculizar de forma grave, deliberada e ilegítima su funcionamiento. Un programa que cifrara los archivos de una empresa para paralizarla, el conocido *ransomware*, encajaría de manera perfecta en esa descripción. Para condenar por este delito hubo que probar por separado la conducta sobre el sistema y el propósito de obstaculizarlo, y los efectos concretos dependieron de cada modalidad.

El segundo inciso sancionó una etapa previa al ataque: diseñar, vender o distribuir programas maliciosos destinados a esos efectos, aunque todavía no se hubieran usado contra ningún sistema. El tercero fijó una pena de cinco a siete años cuando el ataque recaía sobre bienes informáticos de un servicio público o vinculados con la seguridad ciudadana. Este artículo visibilizó dos de las dimensiones técnicas que ya analizamos en el apartado 2.2, la integridad y la disponibilidad: el sistema debía conservarse completo y en funcionamiento (Asamblea Nacional del Ecuador, 2014, art. 232).

Al examinar el artículo 233, observamos que predominaron la información pública legalmente reservada y, en el tercer inciso, la seguridad del Estado. Sus tres incisos diferenciaron tanto la conducta como quién podía cometerla. El primero alcanzó a cualquier persona que destruyera o inutilizara información clasificada conforme a la ley. El segundo, al servidor público que obtuviera esa información por un medio electrónico o informático. El tercero, al servidor encargado de custodiarla o usarla que la revelara sin autorización, cuando esa revelación pudiera comprometer gravemente la seguridad del Estado, conducta reprimida con una pena de siete a diez años, además de la inhabilitación para ejercer un cargo o función pública por seis meses.

En los tres casos hubo que probar primero que la información había sido clasificada según la ley, porque sin esa calificación no existía el delito. Los deberes de custodia sirvieron para identificar al autor del tercer inciso, pero no se trataron como un bien jurídico distinto. La informática, además, solo apareció como exigencia en el segundo inciso: destruir un expediente reservado en papel también encajaba en el primero. En consecuencia, una eventual afectación informática no bastó para explicar lo que este artículo protegía (Asamblea Nacional del Ecuador, 2014, art. 233).

El artículo 234 protegió el control legítimo sobre el sistema, es decir, el derecho de su titular a decidir quién entraba y quién se quedaba en él. Coincidimos en esto con Ramos Mera (2026, p.

36), y creemos que esa es la protección que el tipo debe brindar, por lo que el delito se cometió en el momento del acceso sin permiso o de la permanencia contra la voluntad del titular, aunque no se perdiera ningún dato ni se interrumpiera ningún servicio. Pensemos en un expleado que, tras su despido, ingresó varias veces al sistema de la empresa con su antigua clave y que, aunque no copiara ni dañara nada, habría cometido el delito. Que no hubiera daño no eximía de probar el ingreso, de modo que había que demostrar que hubo acceso o permanencia y quién lo hizo, algo que una dirección IP no resolvía, porque mostraba desde qué conexión se entró, pero no quién estaba frente al equipo. Las finalidades del segundo numeral, explicadas en el apartado 4.1, se analizaron aparte y no se exigieron para el primero (Asamblea Nacional del Ecuador, 2021, art. 14).

En el artículo 234.1, tal como se señaló en el apartado 4.1, predominaron la autenticidad y la confianza jurídica, porque lo que la norma reprimió fue la creación de datos o documentos falsos con intención de engañar y su uso para perjudicar a otro o beneficiarse, y no el daño al sistema. La informática formó parte de la figura, ya que sin intervenir en el tratamiento de los datos no había falsificación, pero la funcionalidad del sistema no alcanzaba para explicar por qué una falsedad merecía pena. Los artículos siguientes tuvieron otra naturaleza, puesto que el 234.2 agravó la pena de los delitos de los artículos 232, 234 y 234.1 cuando se perturbaba de forma grave o duradera una función social crítica, el 234.3 remitió la responsabilidad de las personas jurídicas a los artículos 49 y 71 y el 234.4 fijó las definiciones de la sección, de modo que ninguno se clasificó como delito autónomo ni permitió atribuir una responsabilidad objetiva (Asamblea Nacional del Ecuador, 2021, art. 15).

Un modelo de recepción implícita, parcial e híbrida

El COIP protegió la funcionalidad informática, aunque no la señaló como bien jurídico. Sin embargo, no todos los delitos de la Sección Tercera del COIP giraron en torno a ella, ya que en varios lo que estaba en juego era la intimidad, el patrimonio o la confianza en los documentos. Por esta razón, a nuestro criterio, el modelo del COIP puede considerarse híbrido, es decir, combina la funcionalidad con otros bienes jurídicos. Donde ese bien jurídico protegido se observó con más claridad fue en el artículo 232, que sancionó dañar un sistema con el propósito de obstaculizar su funcionamiento, y en el 234.2, que agravó la pena cuando ese daño perturbaba de forma grave o duradera un servicio esencial, como el de un hospital. El 234 se centró en el control sobre quién

entraba al sistema y los numerales 2 y 3 del 230, en la confianza de llegar al sitio correcto, mientras que la revelación de datos, las transferencias de dinero y las falsificaciones se sancionaron por afectar otros bienes jurídicos. Con esta clasificación ordenamos los intereses de cada norma, sin pretender separar los delitos en informáticos y tradicionales.

Concurso de normas y especialidad

Al comparar los delitos de la Sección Tercera con otros del COIP surgieron dos situaciones distintas. En la primera, un mismo hecho parecía encajar en dos normas, pero solo una debía aplicarse porque lo describía de forma más completa, y eso es lo que se conoce como concurso aparente, mientras que en la segunda el hecho configuraba realmente más de un delito y correspondían las reglas del concurso de infracciones de los artículos 20 y 21 del COIP. Aclaramos, además, que el artículo 26 del COIP solo definía el dolo, es decir, cuándo una persona actúa con conocimiento de los elementos del delito y con voluntad de realizarlo, por lo que no servía para decidir cuál de dos normas debía aplicarse, ya que esa elección dependía de comparar los elementos de cada delito. Las coincidencias y diferencias que encontramos al hacer esa comparación quedaron resumidas en la Tabla 3 (Asamblea Nacional del Ecuador, 2014; Mir Puig, 2016).

Tabla 3

Coincidencias entre los delitos de la Sección Tercera y otros delitos del COIP

Normas comparadas	En qué coincidieron	En qué se diferenciaron	Cómo se resolvió
178 y 229	Ambos sancionaban la revelación de información personal.	El 229 exigía además que la información estuviera registrada, que hubiera provecho y que se afectara de forma intencional el secreto, la intimidad o la privacidad.	Se compararon todos los elementos, porque ninguna norma desplazaba siempre a la otra.
190 y 231	Ambos se referían a apropiaciones o transferencias logradas mediante manipulación informática.	El 190 incluía el uso fraudulento de sistemas y una modalidad sobre las seguridades; el 231 exigía ánimo de lucro y sancionaba también a quien prestaba su cuenta.	Se decidió si había concurso aparente o concurso ideal, y solo cuando dos normas sancionaban el mismo hecho se aplicó la más favorable (art. 5.2).
186 y 231	Ambos afectaban el patrimonio en entornos tecnológicos.	En la estafa del 186 la víctima entregaba el bien por error; en el 231 no se engañaba a una persona, se manipulaba el sistema.	Se identificó cómo se ejecutó el hecho y qué elementos quedaron probados.

Normas comparadas	En qué coincidieron	En qué se diferenciaron	Cómo se resolvió
234.2 y los delitos que agrava	El 234.2 se aplicaba sobre los delitos de los artículos 232, 234 y 234.1.	No era un delito autónomo, solo aumentaba la pena del delito cometido.	Se probó primero el delito cometido (232, 234 o 234.1) y, además, que el ataque perturbó de forma grave o duradera un sistema que sostenía una función social crítica, como la salud o los servicios públicos.

Nota. *Elaboración propia a partir de los artículos 5, 20, 21, 178, 186, 190, 229, 231, 232, 234, 234.1 y 234.2 del COIP. Los ejemplos usados en el texto para explicar estas comparaciones fueron casos hipotéticos, contruidos con fines académicos, y no provinieron de sentencias reales.*

En un primer supuesto hipotético, la alteración de un programa bancario produjo una transferencia patrimonial no consentida en beneficio del agente. El caso permitió examinar las coincidencias entre los primeros incisos de los artículos 190 y 231. Pero no convirtió todas sus modalidades en una relación de especialidad. Antes de elegir la norma hubo que justificar si una disposición agotaba el desvalor o si subsistían varios tipos aplicables a la misma conducta. Para este último caso, el artículo 21 establecía la regla del concurso ideal. La favorabilidad del artículo 5.2 se reservó al conflicto de normas sancionadoras aplicables al mismo hecho, y no se usó para saltarse aquella distinción (Asamblea Nacional del Ecuador, 2014, arts. 5, 20–21, 190 y 231).

En un segundo supuesto hipotético, una persona recibió un correo engañoso y, bajo error, realizó una disposición patrimonial perjudicial, sin que se acreditaran la manipulación funcional ni la transferencia no consentida que describía el artículo 231. El análisis advirtió que este artículo incluía los mensajes de datos, de modo que la ausencia de alteración del sistema no zanjó la calificación. Que el engaño llegara por correo electrónico tampoco bastaba para aplicar el 231, porque ese artículo exigía manipular el sistema, y en este caso fue la propia víctima, engañada, la que entregó su dinero. Por esa razón el caso se analizó como posible estafa del artículo 186, delito en el que la víctima entregaba su patrimonio porque había sido engañada y creía algo que no era cierto. Si además se había usado una página falsa o algún instrumento del artículo 230, había que comprobar cuál era la modalidad concreta y si tenía una gravedad propia, porque llamar al caso *phishing*, es decir, suplantar a una entidad para engañar a la víctima, no resolvía qué norma correspondía (Mayer Lux y Oliver Calderón, 2020).

Funciones críticas y ciberterrorismo

Cuando el ataque afectaba servicios críticos, el COIP ofrecía dos circunstancias distintas que podían presentarse a la vez. La del tercer inciso del artículo 232 dependía de para qué servía el sistema atacado, es decir, si sus bienes informáticos se destinaban a un servicio público o a la seguridad ciudadana, mientras que la del 234.2 exigía además un resultado, que el ataque perturbara de forma grave o duradera un sistema que sostenía una función social crítica. Si ambas coincidían en un mismo caso, había que explicar qué hecho justificaba cada aumento de pena, para no sancionar dos veces por lo mismo. La lista de funciones críticas del 234.2, que mencionaba las cadenas de abastecimiento, la salud, la seguridad, el bienestar económico y los servicios públicos, se leyó como un ejemplo y no como una lista cerrada, aunque eso no permitió incluir cualquier actividad económica, porque lo decisivo fue la relación entre el sistema, la función social y la gravedad o duración del daño, siempre sin aplicar la analogía en perjuicio del procesado.

Con la finalidad de probar estos criterios se construyó un caso hipotético, el bloqueo deliberado del sistema de un hospital público con el propósito de obstaculizar gravemente su funcionamiento. Para su estudio recurrimos al artículo 232. Si, además, la atención sanitaria que dependía de ese sistema sufría una perturbación grave o duradera, también debíamos dirigir nuestra atención al 234.2, y como el hospital prestaba un servicio público, era necesario revisar el tercer inciso del 232, porque no bastaba con decir que el establecimiento era crítico. Por grave que fuera el bloqueo, tampoco permitía hablar de terrorismo, ya que el artículo 366 exigía probar sus propios elementos, entre ellos que se provocara terror en la población, que se pusiera en peligro la vida, la integridad o la libertad de las personas y que se usaran medios capaces de causar estragos, es decir, destrucción de gran magnitud. Mayer Lux (2018a), al definir el ciberterrorismo, ayudó a distinguirlo del simple uso de redes para cometer un delito. El ejemplo mostró una respuesta penal posible ante un ataque grave, sin pretender que todos los casos estuvieran cubiertos ni descartar vacíos que quedaron fuera de este análisis (Asamblea Nacional del Ecuador, 2014, art. 366).

Discusión

En esta discusión retomamos, uno por uno, los cuatro objetivos específicos, y ponemos cada hallazgo frente a lo que sostienen los autores revisados para señalar en qué coincidimos y en qué nos apartamos.

El concepto de delito informático

El primer objetivo nos llevó a separar dos preguntas que suelen mezclarse, la de si un delito es informático y la de qué bien jurídico protege. En la primera coincidimos con Mayer Lux (2018b, pp. 160–161), que incluye el fraude en su concepto estricto de delito informático, y con Navarro-Dolmestch (2023a, pp. 674–675, 680–684), que estudia el fraude y la falsificación a partir de su estructura tecnológica. Es decir, aunque en el artículo 231 predomine el patrimonio y en el 234.1 la autenticidad, ninguna de las conductas descritas en esos artículos deja de configurar un delito informático, y la clasificación híbrida que proponemos solo describe cómo se reparten los intereses dentro de ese campo. Ponce Tubay (2024, pp. 121–122) cuestiona la precisión de las definiciones y su ajuste a los estándares internacionales, pero su análisis del artículo 232 reproduce la redacción anterior a la reforma de 2021, de modo que nuestras diferencias con ese trabajo no se explican solo por cambios legales posteriores a su publicación. Debemos señalar que el texto reformado muestra avances, pero parte de su crítica sigue vigente, porque todavía persisten la mezcla de conductas distintas en el artículo 230 y las superposiciones entre los delitos patrimoniales.

Bien jurídico y objeto material

El segundo objetivo dio lugar a una clasificación que separa tres cosas, el interés protegido, el soporte sobre el que recae la conducta y la forma de protección del bien jurídico. En la Tabla 2 cuidamos de no confundir dos ideas cercanas. Una es la anticipación, que ocurre cuando la ley sanciona antes de que se produzca el daño, como en el artículo 234, donde basta el acceso sin permiso para afectar el control del sistema. La otra es la concurrencia, que ocurre cuando la funcionalidad acompaña a otro interés que es el que justifica la pena, como en el artículo 231, donde la manipulación informática está al servicio de un fin patrimonial. Con esta distinción llevamos al COIP los problemas que Mayer Lux y Oliver Calderón (2020) estudiaron en el fraude informático, Medina Schulz (2014) en el acceso no autorizado y Ramos Mera (2026, p. 36) en el control del sistema.

Intereses protegidos y modelo híbrido

El tercer objetivo nos permitió explicar qué protege cada una de las infracciones de la Sección Tercera del COIP, dedicada a los delitos contra la seguridad de los activos de los sistemas de información y comunicación. Que en ella convivan varios intereses no es un defecto, porque esto nos permite reconocer que no todas las conductas tienen la misma gravedad ni lesionan lo mismo. La funcionalidad otorga unidad a algunos ataques, como el daño del 232 o el acceso del 234, mientras que otros obligan a mirar el patrimonio, la intimidad o la autenticidad. Esta lectura es compatible con el carácter instrumental que Mayer Lux (2017) atribuye a la funcionalidad, es decir, con la idea de que protegerla sirve para resguardar las actividades que dependen de los sistemas, siempre que se diga con claridad cuándo es el centro de la protección y cuándo solo acompaña a otro interés.

Ramos Mera (2026, pp. 33, 36, 38–39, 41) reconoce que estos delitos son pluriofensivos, es decir, que una misma conducta puede lesionar varios intereses a la vez, y analiza por separado los numerales del artículo 230. Partimos de ese antecedente y lo ampliamos a toda la Sección Tercera, de los artículos 229 a 234.4. Nuestro aporte consiste en separar el vínculo de cada delito con la funcionalidad de la forma en que protege el bien jurídico, y en justificar por qué en ciertas modalidades predomina otro interés, como ocurre en los numerales 4 y 5 del 230, donde vemos una protección anticipada del patrimonio a través de los medios de pago, aunque todavía no exista un perjuicio. A eso sumamos el examen del 234.2, del inciso agregado en 2026 al artículo 232 y de las comparaciones entre delitos que desarrollamos con casos hipotéticos.

Criterios interpretativos y propuestas de política criminal

El cuarto objetivo se tradujo en criterios para decidir en qué delito encaja una posible infracción penal y en propuestas para el legislador. El primer criterio es de método, porque la funcionalidad puede ayudar a entender un tipo penal, pero la decisión sobre si una conducta encaja en él tiene que apoyarse en los elementos que la ley describe, y así se respeta la prohibición de la analogía en perjuicio del procesado que establece el artículo 13 del COIP (Asamblea Nacional del Ecuador, 2014, art. 13). Para atribuir la posible infracción a una persona es necesaria la prueba obtenida de forma lícita sobre la conducta y sobre todo lo que el tipo exige, y aunque una cuenta de usuario o una dirección IP aportan indicios cuya pertinencia, origen y contradicción en juicio deben

examinarse, esos indicios no bastan para demostrar quién ejecutó la conducta (Asamblea Nacional del Ecuador, 2014, arts. 5 y 454–457).

Proponemos, además, una secuencia de análisis para decidir en qué delito encaja un hecho. Se empieza por la conducta que quedó probada y, cuando corresponde, por la existencia o no de autorización, para luego revisar el verbo del tipo, el objeto sobre el que recae, la intención exigida y la afectación que la norma pide, y solo al final se comparan los delitos que podrían concurrir. El caso del correo engañoso muestra para qué sirve esta secuencia, porque antes de comparar penas hay que saber si la víctima entregó su dinero engañada o si alguien manipuló el sistema. Queda pendiente comprobar cómo funciona en procesos reales.

El inciso que la Ley Orgánica para el Fortalecimiento de la Ciberseguridad agregó en 2026 al artículo 232, y que excluye del delito ciertas pruebas de seguridad, también debe interpretarse con cuidado, porque se presta a dos interpretaciones, ambas erróneas, la de un permiso amplio para cualquier prueba y la de que su incumplimiento bastaría para probar un delito. Para que no se configure el delito hacen falta tres requisitos, el consentimiento expreso del titular, que la prueba tenga fines de verificación o fortalecimiento de la seguridad y que se cumplan los procedimientos y registros de esa ley. Como el inciso está en el artículo 232, plantea un problema distinto del acceso del 234. Si en una evaluación consentida se incumple alguna formalidad, la excepción no se aplica, pero ese incumplimiento tampoco prueba que existiera el propósito de obstaculizar ni los daños que exige el 232, y tampoco convierte el acceso en no autorizado para efectos del 234 (Asamblea Nacional del Ecuador, 2026, art. 11).

En la doctrina chilena, Mayer Lux y Vera Vega (2022, pp. 282–283) dejan abiertas dos lecturas de la falta de autorización, una que la vincula con la ilicitud de la conducta y otra que la asimila al consentimiento que excluye la tipicidad, mientras que Navarro-Dolmestch (2023b) sostiene que el acceso autorizado ya queda fuera del tipo de acceso ilícito, es decir, que la autorización hace que la conducta no sea delito. Esa lectura no puede trasladarse sin más al COIP, porque nuestra ley está redactada de otra manera. En el artículo 234 la falta de autorización forma parte de la descripción del delito, y la exclusión de las pruebas de seguridad no se ubicó en ese artículo sino en el 232 (Asamblea Nacional del Ecuador, 2026, art. 11).

Para el legislador, sugerimos aclarar la relación entre los artículos 190 y 231 y ordenar mejor el artículo 230. Sus cinco numerales pueden agruparse, para estudiarlos, en cuatro bloques, la captación de datos, el desvío hacia sitios falsos, la información de tarjetas y los instrumentos

destinados a esas conductas, y una eventual reforma debería mantener sus diferencias en lugar de reunirlos bajo un nombre técnico general. En cuanto a los artículos 232 y 234.2, que exigen una afectación grave o duradera sin decir cómo medirla, proponemos que se estudien indicadores para hacerlo, como el tiempo que el servicio estuvo interrumpido, el número de usuarios afectados, la posibilidad de revertir el daño y la dependencia de otros servicios. Esos indicadores no son requisitos de la ley vigente ni pueden convertirse en requisitos nuevos por decisión de los jueces, pero sí pueden ayudar a quien juzga a explicar por qué, en un caso concreto, la afectación fue o no grave o duradera, siempre que se relacionen con los hechos probados y respeten las garantías de legalidad y proporcionalidad (Asamblea Nacional del Ecuador, 2014, arts. 5 y 13; Mayer Lux, 2017).

Queda una última distinción, la de la política de ciberseguridad frente a la política penal, que deben mantenerse separadas, porque la primera busca prevenir los incidentes y restablecer los servicios afectados, mientras que la segunda solo interviene, como último recurso, frente a las conductas que la ley describe como delito. El marco del NIST (2024), que ya citamos en el apartado 2.2, muestra que resguardar los sistemas exige mucho más que sancionar, y aquí lo usamos solo como referencia para ordenar ideas, sin que cree obligaciones penales en Ecuador. Cualquier reforma debería apoyarse, además, en datos del país, y con sentencias ecuatorianas y peritajes obtenidos en condiciones jurídicas y técnicas comparables se podrían examinar las soluciones y los problemas de prueba que este estudio documental no midió. Es lo que Lara et al. (2014) llaman una regulación basada en la evidencia, es decir, decidir las reformas a partir de datos sobre cómo ocurren estos delitos y cómo se resuelven, y no solo a partir de percepciones.

Conclusiones

Con este estudio respondemos a la pregunta de investigación. La funcionalidad informática es un bien jurídico protegido en el COIP, pero solo de manera implícita, porque el Código no la nombra, y parcial, porque explica el núcleo de algunos delitos y no el de toda la Sección Tercera, que la combina con otros bienes jurídicos en un modelo híbrido. Así se cumple el objetivo general, que era determinar el alcance de esa categoría en los artículos 229 a 234.4 y en su relación con otros delitos. Las conclusiones que siguen respetan el orden de los objetivos específicos, y la última recoge los límites del estudio y las líneas de investigación pendientes.



Respecto del primer objetivo, que un hecho se cometa mediante un sistema informático no basta para saber qué bien jurídico lesiona. Una infracción puede ser propiamente informática y proteger sobre todo el patrimonio o la autenticidad, como ocurre con el fraude del artículo 231 y la falsificación del 234.1, que configuran delitos informáticos aunque en ellos la funcionalidad no sea el interés principal. Aun en esos casos, la funcionalidad conserva valor para la interpretación, porque ayuda a precisar qué hace grave cada una de esas conductas.

En cuanto al segundo objetivo, el objeto material y el bien jurídico no deben confundirse. Los datos, los programas y los sistemas son aquello sobre lo que recae la conducta, mientras que el interés protegido depende de cómo está construido cada tipo penal, de ahí que nuestra clasificación atienda a dos criterios, el vínculo de cada infracción con la funcionalidad y la forma en que protege el bien jurídico. El artículo 230 lo muestra con claridad, porque allí el desvío hacia sitios falsos se relaciona con la confianza de llegar al sitio correcto, mientras que la clonación de tarjetas y los instrumentos para realizarla permiten sostener una protección anticipada del patrimonio, sin agregar daños ni finalidades que la ley no exige.

Al identificar los intereses protegidos, que era el tercer objetivo, encontramos que la funcionalidad ocupa el centro en el artículo 232, que sanciona dañar un sistema con el propósito de obstaculizar su funcionamiento, y se refuerza en el 234.2, que aumenta la pena de ese y otros delitos cuando el ataque perturba de forma grave o duradera un servicio esencial. El artículo 234, por su parte, protege el control legítimo sobre quién entra al sistema, y en su primer numeral basta el acceso sin permiso, aunque no se produzca ningún daño. En las demás infracciones pesan más la intimidad, el patrimonio, la información reservada o la autenticidad de los documentos, de modo que cada una debe analizarse con sus propias reglas.

Para el cuarto objetivo, el de los criterios de interpretación, hay que partir de que las reformas que el COIP tuvo en 2021 y en 2026 cambiaron los textos de la Sección Tercera que deben interpretarse. El inciso que en 2026 se agregó al artículo 232 sobre las pruebas de seguridad consentidas obliga a revisar sus requisitos por separado de los elementos de cada delito. El caso del hospital muestra, además, que aplicar los artículos 232 y 234.2 no equivale a probar terrorismo, y que la ausencia de un delito llamado ciberterrorismo tampoco significa que, en general, estos ataques queden sin sanción.

Cuando un mismo hecho parece encajar a la vez en los artículos 178 y 229, o en el 190 y el 231, no basta con elegir una norma y descartar la otra de forma mecánica. Hay que decidir si solo una



debe aplicarse porque describe el hecho de forma más completa, que es el concurso aparente, si el hecho configura realmente más de un delito, que es el concurso de infracciones, o si dos normas sancionan el mismo hecho y corresponde aplicar la más favorable. Los casos de la transferencia bancaria y del correo engañoso muestran que lo que decide el delito aplicable es cómo se cometió el hecho y qué quedó probado, y no la etiqueta tecnológica que se le ponga.

La funcionalidad sirve para interpretar los tipos y para medir la proporcionalidad de la respuesta penal, pero siempre dentro de lo que la ley dice. Además, la presunción de inocencia exige probar quién cometió el hecho y todo lo que el tipo pide, incluidos, cuando corresponda, la falta de autorización, el resultado y la relación de causa entre la conducta y ese resultado, de modo que ningún indicio técnico, como una dirección IP, puede reemplazar esa prueba.

Estas conclusiones tienen un alcance normativo y doctrinal, porque nacen del análisis de la ley y de la doctrina, y no de casos reales. De ahí que la secuencia de análisis, las propuestas para reorganizar el artículo 230 y los indicadores de gravedad deban contrastarse con sentencias y peritajes ecuatorianos, ya que los ejemplos hipotéticos muestran el razonamiento, pero no prueban que esas soluciones funcionen ni con qué frecuencia se presentan. Como línea de investigación futura, proponemos estudiar, a partir de expedientes anonimizados, cómo resuelven los tribunales ecuatorianos estos delitos y si en sus decisiones se distingue entre la funcionalidad y los demás bienes jurídicos. En todo caso, la respuesta penal es solo una parte de la protección de los sistemas informáticos, que también requiere prevenir los incidentes, responder a ellos y restablecer el servicio afectado.

Referencias bibliográficas

Asamblea General de las Naciones Unidas. (2024). *Convención de las Naciones Unidas contra la Ciberdelincuencia: Fortalecimiento de la cooperación internacional para la lucha contra determinados delitos cometidos mediante sistemas de tecnología de la información y las comunicaciones y para la transmisión de pruebas en forma electrónica de delitos graves* (Resolución 79/243).

<https://documents.un.org/doc/undoc/gen/n24/426/74/pdf/n2442674.pdf>

Asamblea Nacional del Ecuador. (2014). *Código Orgánico Integral Penal* [Texto consolidado con última reforma general indicada al 18 de septiembre de 2024]. Registro Oficial, Suplemento 180, 10 de febrero de 2014.

<https://www.funcionjudicial.gob.ec/resources/pdf/Codigo%20Organico%20Integral%20Penal.pdf>

Asamblea Nacional del Ecuador. (2021). *Ley Orgánica Reformatoria del Código Orgánico Integral Penal para Prevenir y Combatir la Violencia Sexual Digital y Fortalecer la Lucha contra los Delitos Informáticos*. Registro Oficial, Cuarto Suplemento 526, 30 de agosto de 2021. <https://www.asambleanacional.gob.ec/es/system/files/ro-4s-526-de-30-08-2021.pdf>

Asamblea Nacional del Ecuador. (2026). *Ley Orgánica para el Fortalecimiento de la Ciberseguridad*. Registro Oficial, Quinto Suplemento 290, 22 de mayo de 2026.

https://www.asambleanacional.gob.ec/es/system/files/ro_29.pdf

Bundesverfassungsgericht. (2008, 27 de febrero). *Sentencia 1 BvR 370/07 y 1 BvR 595/07* (BVerfGE 120, 274).

https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2008/02/rs20080227_1bvr037007en.html

Consejo de Europa. (2001a). *Convenio sobre la Ciberdelincuencia* (ETS 185).

<https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185>

Consejo de Europa. (2001b). *Informe explicativo del Convenio sobre la Ciberdelincuencia* (ETS 185). <https://rm.coe.int/16800cce5b>



- Consejo de Europa. (2024, 12 de diciembre). *Convention on Cybercrime: Ecuador becomes the 77th Party and Peru signs the Second Protocol on electronic evidence*.
<https://www.coe.int/en/web/cybercrime/-/convention-on-cybercrime-ecuador-becomes-the-77th-party-and-peru-signs-the-second-protocol-on-electronic-evidence>
- Consejo de Europa. (2026). *Chart of signatures and ratifications of Treaty 185*. Recuperado el 4 de agosto de 2026, de <https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185>
- Corte Constitucional del Ecuador. (2021, 27 de enero). *Sentencia 2064-14-EP/21* (C. Corral Ponce, jueza ponente). <https://www.corteconstitucional.gob.ec/sentencia-2064-14-ep-21/>
- Corte Constitucional del Ecuador. (2022, 27 de enero). *Sentencia 77-16-IN/22* (E. Herrería Bonnet, juez ponente). <https://www.corteconstitucional.gob.ec/sentencia-77-16-in-22/>
- European Union Agency for Cybersecurity. (2025). *ENISA threat landscape 2025*.
<https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025>
- Gercke, M. (2014). *Understanding cybercrime: Phenomena, challenges and legal response*. International Telecommunication Union. <https://www.itu.int/en/ITU-D/Cybersecurity/Documents/cybercrime2014.pdf>
- Lara, J. C., Martínez, M., & Viollier, P. (2014). Hacia una regulación de los delitos informáticos basada en la evidencia. *Revista Chilena de Derecho y Tecnología*, 3(1), 101–137.
<https://doi.org/10.5354/0719-2584.2014.32222>
- Mayer Lux, L. (2017). El bien jurídico protegido en los delitos informáticos. *Revista Chilena de Derecho*, 44(1), 235–260. <https://doi.org/10.4067/S0718-34372017000100011>
- Mayer Lux, L. (2018a). Defining cyberterrorism. *Revista Chilena de Derecho y Tecnología*, 7(2), 5–25. <https://doi.org/10.5354/0719-2584.2018.51028>
- Mayer Lux, L. (2018b). Elementos criminológicos para el análisis jurídico-penal de los delitos informáticos. *Ius et Praxis*, 24(1), 159–206. <https://doi.org/10.4067/S0718-00122018000100159>
- Mayer Lux, L., & Oliver Calderón, G. (2020). El delito de fraude informático: Concepto y delimitación. *Revista Chilena de Derecho y Tecnología*, 9(1), 151–184.
<https://doi.org/10.5354/0719-2584.2020.57149>



- Mayer Lux, L., & Vera Vega, J. (2022). La nueva ley de delitos informáticos. *Revista de Ciencias Penales*, 48(3), 267–336. <https://revistadecienciaspenales.cl/wp-content/uploads/2023/04/RCP-3-2022-Final-273-342.pdf>
- Medina Schulz, G. (2014). Estructura típica del delito de intromisión informática. *Revista Chilena de Derecho y Tecnología*, 3(1), 79–99. <https://doi.org/10.5354/0719-2584.2014.32221>
- Mir Puig, S. (2016). *Derecho penal: Parte general* (10.^a ed.). Reppertor.
- Miró Llinars, F. (2012). *El cibercrimen: Fenomenología y criminología de la delincuencia en el ciberespacio*. Marcial Pons.
- Naciones Unidas. (2026). *Convención de las Naciones Unidas contra la Ciberdelincuencia* [Estado de firmas y ratificaciones, capítulo XVIII-16]. United Nations Treaty Collection. Recuperado el 14 de octubre de 2026, de https://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=XVIII-16&chapter=18&clang=_en
- National Institute of Standards and Technology. (2024). *The NIST Cybersecurity Framework (CSF) 2.0* (NIST CSWP 29). <https://doi.org/10.6028/NIST.CSWP.29>
- Navarro-Dolmestch, R. (2023a). El concepto de delito informático según la nueva legislación chilena (Ley n.º 21.459). *Política Criminal*, 18(36), 666–689. <https://doi.org/10.4067/S0718-33992023000200666>
- Navarro-Dolmestch, R. (2023b). La autorización como causal de atipicidad en el delito de acceso ilícito a un sistema informático en la legislación chilena de delitos informáticos. *Revista Chilena de Derecho y Tecnología*, 12, 1–24. <https://doi.org/10.5354/0719-2584.2023.67546>
- Ojeda-Pérez, J. E., Rincón-Rodríguez, F., Arias-Flórez, M. E., & Daza-Martínez, L. A. (2010). Delitos informáticos y entorno jurídico vigente en Colombia. *Cuadernos de Contabilidad*, 11(28), 41–66. <https://revistas.javeriana.edu.co/index.php/cuacont/article/view/3176>
- Ponce Tubay, M. A. (2024). Delitos informáticos: Caso Ecuador. *Revista San Gregorio*, 1(58), 119–123. <https://doi.org/10.36097/rsan.v1i58.2667>
- Ramos Mera, J. M. (2026). La funcionalidad informática como objeto de tutela penal: Bases dogmáticas para la comprensión del bien jurídico en los delitos informáticos. *Revista Jurídica Crítica y Derecho*, 7(13), 29–42. <https://doi.org/10.29166/cyd.v7i13.10451>

**Conflicto de intereses:**

La autora declara que no existe conflicto de interés posible.

Financiamiento:

No existió asistencia financiera de partes externas al presente artículo.

Agradecimiento:

La autora agradece al Ab. Jaime Eduardo Alvear Franco por su asistencia en la investigación.

Nota:

El artículo no es producto de una publicación anterior. Se desarrolló en los estudios de maestría de la autora en la Universidad ECOTEC.

Declaración sobre el uso de inteligencia artificial:

En la preparación de este manuscrito se utilizó Claude, de Anthropic, como apoyo para revisar y reescribir la redacción con fines de claridad, reorganizar párrafos, proponer ejemplos hipotéticos ilustrativos, traducir el resumen al inglés y verificar el texto de las normas citadas y el formato de las referencias. En otra etapa de revisión se utilizó también una herramienta de OpenAI para apoyar la corrección editorial, el contraste de fuentes, la reorganización de tablas y la propuesta de desarrollos argumentativos y ejemplos hipotéticos. Todas las propuestas de ambas herramientas fueron revisadas, modificadas o descartadas por la autora. Estas herramientas no se consideran autoras. La responsabilidad por el planteamiento del problema, las decisiones interpretativas, la selección y comprobación de fuentes y las conclusiones corresponde a la autora.