Volumen: 4, Número: 4, Año: 2026 páginas 496-511
E-ISSN: 3103-1536
Bajo licencia: CC BY-SA 4.0

REVISTA CIENTÍFICA VISIÓN ACADÉMICA https://visionacademica.com/

DOI: https://doi.org/10.70577/9h18zj36

# Las transferencias bancarias electrónicas y el delito de estafa en ecuador: un análisis dogmático, regulatorio y procesal

## *Electronic Bank Transfers and Fraud in Ecuador: A Dogmatic, Regulatory and Procedural Analysis*

**Ab. Jonathan Rodrigo Gómez Ramos**[1]
Maestrante de la MAESTRIA EN DERECHO CON MENCION EN DERECHO PENAL Y CRIMINOLOGIA de la Universidad Iberoamericana del Ecuador, Ecuador
jonarodrig.24@gmail.com
https://orcid.org/0009-0001-3726-3678

**Dr. Raúl Franklin Reinoso Rojas PhD**[2]
Docente Tutor de la Universidad Iberoamericana del Ecuador, Ecuador
rreinoso@doc.unibe.edu.ec
https://orcid.org/0009-0001-4749-5413

**Cómo citar**

Gómez Ramos, A. J. R. ., & Reinoso Rojas , D. R. F. (2026). Las transferencias bancarias electrónicas y el delito de estafa en ecuador: un análisis dogmático, regulatorio y procesal. *Visión Académica*, *4*(4), 496-511. https://doi.org/10.70577/9h18zj36

Fecha de recepción: 2026-09-30

Fecha de aceptación: 2026-10-14

Fecha de publicación: 2026-11-17

**RESUMEN**

Este artículo examina la relación entre las transferencias bancarias electrónicas y la estafa en Ecuador desde tres planos: la construcción dogmática del engaño y la disposición patrimonial; la regulación del sistema de pagos, los prestadores y la información del usuario; y las exigencias procesales para incorporar evidencia digital. Se desarrolló una investigación cualitativa, documental, analítica y hermenéutica, con contraste de escenarios jurídicos y fuentes legislativas e institucionales. Los resultados sostienen que el uso de una transferencia no define por sí mismo el tipo penal aplicable: debe diferenciarse la transferencia inducida mediante error, el desplazamiento sin consentimiento mediante manipulación informática y la controversia contractual sin dolo inicial probado. Además, la trazabilidad bancaria resulta relevante, aunque insuficiente sin corroboración de autoría, contexto comunicacional y cadena de custodia. Se concluye que la respuesta jurídica debe coordinar la clasificación penal, las obligaciones de las entidades financieras, la preservación de evidencia y las garantías de usuarios e investigados, evitando tanto la impunidad derivada de obstáculos técnicos como la ampliación indebida del derecho penal.

**Palabras clave:** estafa; transferencias electrónicas; prueba digital; sistema financiero; Ecuador.

Volumen: 4, Número: 4, Año: 2026 páginas 496-511
E-ISSN: 3103-1536
Bajo licencia: CC BY-SA 4.0

**ABSTRACT**

This article examines the relationship between electronic bank transfers and fraud in Ecuador through criminal-law doctrine, financial regulation, and criminal procedure. It employs a qualitative documentary and interpretative method, comparing legal sources and hypothetical transactional patterns without claiming new interview or survey evidence. The findings distinguish transfers induced by deceptive representations from unauthorized transfers produced by computer manipulation and from disputes in which criminal intent has not been established. Banking records can establish transaction sequences, but they do not independently identify the offender or explain the circumstances of consent. The paper argues for coordinated evidentiary preservation, proportionate banking safeguards, and a legally reasoned classification of offenses. It concludes that adequate protection of financial users depends on proof of each offense element, respect for due process, and a clear separation between criminal responsibility and institutional or contractual liability.

**Keywords:** fraud; electronic bank transfers; digital evidence; financial regulation; Ecuador.

## INTRODUCCIÓN

La orden de transferencia se ha convertido en una forma ordinaria de disponer de recursos depositados en entidades financieras. Su rapidez facilita intercambios, pagos de servicios y operaciones entre particulares, pero reduce el margen temporal para advertir una instrucción obtenida mediante falsedades. Esa transformación no modifica por sí misma la estructura del delito de estafa: el problema consiste en determinar cuándo la intervención tecnológica constituye solamente el medio del desplazamiento patrimonial y cuándo altera la propia mecánica del hecho punible.

En la investigación que sirve como antecedente documental, Gómez Ramos (2025) estudió la banca virtual, el artículo 186 del Código Orgánico Integral Penal y la respuesta administrativa de varias instituciones financieras. El presente trabajo adopta otra delimitación: somete a contraste los elementos dogmáticos de la estafa, la regulación de pagos y el tratamiento procesal de la evidencia, sin reproducir como propios los resultados de entrevistas de aquella tesis.

La pregunta central es bajo qué condiciones una transferencia bancaria electrónica vinculada a un perjuicio patrimonial permite sustentar una imputación por estafa en Ecuador y qué papel cumplen la regulación financiera y la prueba tecnológica para diferenciar otros supuestos. Se sostiene que el canal electrónico no reemplaza los elementos del tipo: si el titular ordena el pago engañado, resulta decisiva la disposición provocada por error; si un tercero manipula el sistema para transferir fondos sin consentimiento, debe examinarse el tipo especial correspondiente.

El objetivo general consiste en analizar los criterios dogmáticos, regulatorios y procesales que permiten calificar y acreditar hechos patrimoniales asociados a transferencias electrónicas. Como objetivos específicos se plantean distinguir modalidades fácticas relevantes; examinar las funciones del marco monetario y de protección del usuario; y desarrollar un itinerario probatorio compatible con legalidad,

Volumen: 4, Número: 4, Año: 2026 páginas 496-511
E-ISSN: 3103-1536
Bajo licencia: CC BY-SA 4.0

contradicción y protección de datos. La relevancia de esta distinción no reside en proponer castigos automáticos, sino en evitar errores de subsunción y mejorar la calidad de las decisiones.

## MATERIAL Y MÉTODOS

### Materiales y corpus documental

El corpus documental comprendió el Código Orgánico Integral Penal (arts. 186, 190, 456 y 500), la Constitución de la República (arts. 76 y 308), el Código Orgánico Monetario y Financiero, las normas de protección de datos personales y de servicios financieros tecnológicos, así como la investigación universitaria de Gómez Ramos (2025). La selección respondió a cuatro criterios: relación directa con el hecho patrimonial, identificación de obligaciones financieras, regulación de la prueba digital y protección de derechos. Se excluyeron expedientes reservados, estadísticas sin metodología verificable y materiales que no permitían establecer su autoría o procedencia.

El examen se organizó en una ficha por disposición, con registro de fuente, año, artículo, contenido normativo, problema abordado y alcance interpretativo. Las fuentes legales se utilizaron para identificar los elementos de cada institución; la tesis precedente únicamente como antecedente académico, sin trasladar a este artículo sus entrevistas como si fueran trabajo de campo propio. No se desarrolló una muestra jurisprudencial exhaustiva; por ello, los resultados no describen tendencias de juzgamiento ni acreditan frecuencia de conductas.

### Enfoque, diseño y procedimiento

El enfoque fue cualitativo y de investigación jurídica documental. Se aplicó el método analítico para descomponer engaño, error, disposición patrimonial, perjuicio, dolo y nexo causal; el hermenéutico para interpretar las normas en relación con el sistema jurídico; y el sistemático para articular regulación financiera, protección de datos y procedimiento penal. El diseño no comprende experimentación, medición de incidencia criminal ni análisis estadístico. En consecuencia, los resultados son inferencias normativas y matrices de calificación, no porcentajes obtenidos en trabajo de campo.

El procedimiento comprendió cuatro etapas: identificar modalidades de disposición patrimonial; extraer los elementos de las normas seleccionadas; elaborar supuestos de contraste diferenciando engaño, ausencia de consentimiento e incumplimiento; y establecer qué hechos y registros serían pertinentes para cada hipótesis. En cada escenario se examinó quién dispuso los fondos, qué información recibió, cómo intervino el sistema y qué inferencias podían justificarse. El procedimiento permite comparar criterios jurídicos; no sustituye la comprobación de hechos en una investigación penal.

Volumen: 4, Número: 4, Año: 2026 páginas 496-511
E-ISSN: 3103-1536
Bajo licencia: CC BY-SA 4.0

**Consideraciones éticas y límites**

No se recolectaron datos personales ni testimonios. Los ejemplos son hipotéticos y no representan casos judiciales comprobados. No se atribuyen tasas de comisión delictiva ni porcentajes de recuperación, porque el corpus no ofrece una base uniforme para medirlos. Las conclusiones no pretenden resolver casos particulares sin acceso a los expedientes. Las referencias al marco legal están sujetas a comprobar el texto consolidado vigente al momento de su aplicación, especialmente cuando existen reformas posteriores a las versiones oficiales consultadas.

## RESULTADOS

### 1. Delimitación de escenarios y calificación jurídica

#### 1.1. La transferencia electrónica como acto de disposición

Una transferencia bancaria comprende una orden, su validación por el prestador y el movimiento de fondos hacia la cuenta receptora. Estos momentos cumplen funciones distintas para la calificación penal. La orden acredita una operación iniciada con determinadas credenciales, pero no demuestra que el titular conociera las circunstancias de la transacción ni que hubiese aceptado una representación falsa de la realidad. Para examinar la estafa, la cuestión jurídica no es únicamente quién pulsó la opción de pago, sino qué información motivó ese acto y qué perjuicio se produjo. Según la Asamblea Nacional del Ecuador (2014a, art. 186), el error provocado mediante hechos simulados, deformados u ocultados debe relacionarse con un acto que afecte al patrimonio.

En un supuesto hipotético de venta inexistente, el comprobante permite situar la fecha, la cuantía y la cuenta de destino; las conversaciones previas permiten valorar la conducta que llevó al comprador a transferir. Ninguno de estos elementos, aislado, identifica al responsable. La reconstrucción del hecho requiere confrontar la orden, la disponibilidad de los fondos, el mensaje que precedió al pago y las explicaciones alternativas. De esta forma se evita equiparar la ejecución de una operación con la prueba completa de un delito.

#### 1.2. Engaño relevante y creación del error

El engaño exige una representación de hechos susceptible de inducir a una decisión patrimonial equivocada. En medios electrónicos puede consistir en una identidad comercial simulada, una oferta de bienes inexistentes o información falsa sobre la titularidad de un servicio. La relevancia de la conducta depende de lo comunicado, del momento de recepción y de su relación con la decisión de pago. Según la Asamblea Nacional del Ecuador (2014a, art. 186), la simulación, deformación u ocultamiento de hechos debe inducir a error; no basta que la comunicación resulte imprecisa o que un negocio termine sin cumplimiento.

Volumen: 4, Número: 4, Año: 2026 páginas 496-511
E-ISSN: 3103-1536
Bajo licencia: CC BY-SA 4.0

Para distinguir fraude de incumplimiento deben examinarse los actos anteriores a la transferencia: existencia del bien ofrecido, capacidad de entrega, autenticidad de los datos proporcionados y conducta de la contraparte. La creación deliberada de un perfil falso antes del cobro puede respaldar una hipótesis de engaño inicial. En cambio, una demora posterior no demuestra por sí sola que la oferta fuera falsa desde el principio. Esta diferencia determina qué evidencia debe recogerse y limita el uso del derecho penal en controversias contractuales.

### 1.3. Error, causalidad y desplazamiento de activos

No toda falsedad explica una pérdida patrimonial. La relación causal exige establecer que el destinatario de la comunicación aceptó como cierto un dato falso y, a partir de ese error, dispuso de sus recursos. Si la transferencia obedeció a una razón independiente, la secuencia requerida para la estafa no quedaría demostrada. La formulación del artículo 186 del COIP vincula expresamente el error inducido con el acto que perjudica el patrimonio (Asamblea Nacional del Ecuador, 2014a, art. 186).

La comprobación exige ordenar cronológicamente publicaciones, mensajes, confirmaciones de pago y eventuales reclamaciones. Cuando existen varios abonos, cada uno puede responder a una información diferente: por ejemplo, un primer pago por la compra y otro por un supuesto gasto de transporte. La causalidad debe justificarse respecto de cada disposición; una transferencia posterior no adquiere automáticamente el mismo fundamento penal que la anterior.

### 1.4. Perjuicio patrimonial y promesa incumplida

La disminución del saldo bancario no basta para caracterizar el perjuicio propio de una estafa. Debe considerarse si existió una contraprestación, si se recibió un bien de valor equivalente o si el desembolso fue inducido mediante una falsedad. El artículo 186 del COIP relaciona el acto de disposición con una afectación patrimonial; por eso, el análisis comprende el intercambio en su conjunto y no únicamente el movimiento de dinero (Asamblea Nacional del Ecuador, 2014a, art. 186).

Una entrega tardía, una discrepancia sobre la calidad o la imposibilidad sobrevenida de cumplir pueden generar consecuencias civiles o administrativas. Para sostener una imputación penal se necesitan indicios de que, al recibir el pago, el receptor había desplegado un engaño destinado a provocar la entrega de dinero. La diferencia no depende del nombre de la reclamación presentada por el usuario, sino de la comprobación de los hechos que precedieron a la obligación incumplida.

### 1.5. Dolo y propósito de obtener beneficio

El análisis subjetivo de la estafa requiere establecer que la persona conoció el carácter engañoso de su conducta y actuó para conseguir un beneficio patrimonial propio o ajeno. Esta finalidad forma parte de la descripción del artículo 186 del COIP (Asamblea Nacional del Ecuador, 2014a, art. 186). No puede deducirse de manera automática del ingreso de fondos en una cuenta, porque la recepción material y la participación dolosa son circunstancias distintas.

Volumen: 4, Número: 4, Año: 2026 páginas 496-511
E-ISSN: 3103-1536
Bajo licencia: CC BY-SA 4.0

La inferencia del dolo puede apoyarse en la creación previa de identidades ficticias, la reiteración de ofertas inexistentes, las instrucciones para ocultar el destino del dinero y la coordinación con otros participantes. También deben valorarse los datos que contradigan esa hipótesis: utilización no autorizada de una cuenta, intermediación sin conocimiento del origen o devolución documentada. El propósito de beneficio necesita una explicación sustentada en conductas comprobables, no en la sola sospecha de ventaja económica.

### 1.6. Autoría, cooperación y cuentas receptoras

La identificación del titular de la cuenta beneficiaria constituye una línea de investigación, pero no equivale a identificar al autor del engaño. Pueden intervenir quien diseña la oferta falsa, quien mantiene contacto con la víctima, quien facilita datos bancarios y quien finalmente retira los valores. Cada participación debe examinarse de manera individual, atendiendo al aporte concreto y al conocimiento del plan. La atribución de responsabilidad debe respetar los principios de culpabilidad y presunción de inocencia reconocidos por el ordenamiento ecuatoriano.

Un registro de movimientos bancarios puede revelar el destino inicial de los fondos; las comunicaciones y otras diligencias permitirán examinar si existió coordinación entre intervinientes. En el supuesto de una cuenta utilizada sin autorización, la titularidad formal no bastaría para concluir cooperación. Por ello, las diligencias deberían contrastar acceso efectivo, capacidad de disposición y relaciones entre los participantes antes de formular una imputación.

### 1.7. Estafa frente a apropiación fraudulenta electrónica

Los artículos 186 y 190 del COIP describen mecanismos de afectación patrimonial que no son intercambiables. En la estafa, el sujeto activo simula, deforma u oculta hechos para inducir a una persona a error y lograr que ejecute un acto perjudicial, con finalidad de beneficio patrimonial. El artículo 190 se refiere al uso fraudulento de sistemas o redes para facilitar una apropiación o procurar transferencias no consentidas mediante alteración, manipulación o modificación de su funcionamiento; también contempla determinados medios de vulneración de seguridades. La diferencia se ubica, por tanto, en la forma de obtener el desplazamiento y no en el uso común de internet o banca móvil (Asamblea Nacional del Ecuador, 2014a, arts. 186 y 190).

Si una persona paga a un supuesto proveedor porque creyó una oferta ficticia, la hipótesis inicial se examina desde el engaño que produjo su decisión. Si un tercero altera el funcionamiento de un sistema para transferir recursos sin intervención consentida de su titular, corresponde revisar los elementos del artículo 190. La existencia de credenciales válidas no resuelve por sí sola la cuestión: debe determinarse si hubo una decisión engañada, un acceso ilegítimo o una manipulación técnica. La selección del tipo penal requiere prueba de ese mecanismo y revisión de la redacción legal aplicable al hecho.

### 1.8. Conductas informáticas conexas y concurso

Volumen: 4, Número: 4, Año: 2026 páginas 496-511
E-ISSN: 3103-1536
Bajo licencia: CC BY-SA 4.0

La obtención de claves, la suplantación de páginas o la alteración de registros pueden formar parte de una secuencia de hechos patrimoniales, pero no autorizan a acumular tipos penales sin identificar los elementos propios de cada conducta. Debe verificarse qué comportamiento constituye el medio para producir el perjuicio y cuál expresa una lesión autónoma. El criterio de legalidad impide calificar un mismo acto varias veces únicamente por intervenir herramientas digitales.

En una hipótesis de captación de credenciales seguida de transferencia, la investigación debe distinguir la obtención de acceso, la orden bancaria y la apropiación resultante. La eventual concurrencia de infracciones exige aplicar las reglas del COIP sobre concurso, atendiendo a los hechos y no solo a la cantidad de dispositivos utilizados. La documentación técnica de cada fase facilita ese examen y reduce las imputaciones sustentadas en descripciones generales.

### 1.9. La función constitucional del sistema financiero

El artículo 308 de la Constitución ecuatoriana sitúa las actividades financieras en un régimen de interés público y exige autorización estatal para ejercerlas. Esta calificación ofrece un fundamento para el control y la protección de usuarios, pero no convierte cualquier operación irregular en responsabilidad penal de la entidad que la procesa (Asamblea Constituyente, 2008, art. 308). Las obligaciones financieras y la determinación del autor de un delito corresponden a planos jurídicos diferentes.

Ante una transferencia cuestionada, el análisis institucional se orienta a establecer si se aplicaron los controles exigibles, si hubo información suficiente y si el reclamo fue atendido conforme al régimen correspondiente. La investigación penal, en cambio, debe comprobar la conducta atribuida a una persona. La coincidencia de un mismo hecho no elimina la necesidad de justificar de forma independiente cada consecuencia jurídica.

### 1.10. Infraestructura de pagos y participantes

Las operaciones electrónicas involucran entidades ordenantes y receptoras, canales de autenticación y sistemas destinados a procesar o liquidar órdenes. El Código Orgánico Monetario y Financiero regula la estructura institucional y las competencias sobre la actividad monetaria y financiera (Asamblea Nacional del Ecuador, 2014b). En una investigación jurídica conviene separar la evidencia que conserva el canal utilizado de aquella que registra el movimiento entre entidades.

La distinción afecta la trazabilidad: un reporte de acceso puede indicar el uso de una aplicación, mientras que los registros de transacción muestran el procesamiento y el destino contable de la orden. Para reconstruir una operación controvertida es necesario establecer qué participante generó cada registro, su alcance y las posibilidades legales de requerirlo. La falta de un documento no se suple presumiendo que todos los sistemas conservaron la misma información.

### 1.11. Autenticación, diligencia y alertas

Volumen: 4, Número: 4, Año: 2026 páginas 496-511
E-ISSN: 3103-1536
Bajo licencia: CC BY-SA 4.0

La autenticación permite comprobar el cumplimiento de un mecanismo de acceso o validación, pero no acredita necesariamente que la voluntad patrimonial estuviera libre de engaño. Una persona puede confirmar con su clave una instrucción que considera legítima por información falsa recibida antes del ingreso al sistema. En contraste, el empleo de credenciales ajenas puede hacer relevante una hipótesis de transferencia no consentida. El dato técnico debe interpretarse con la secuencia factual y con el tipo penal considerado.

Las alertas y controles de seguridad pueden contribuir a prevenir operaciones irregulares y a documentar decisiones del sistema. Su suficiencia debe evaluarse conforme a la normativa y a las condiciones del servicio, sin concluir que la ausencia de una alerta acredita dolo de un tercero ni que su emisión exonera automáticamente a la entidad. La relación entre deberes de diligencia y responsabilidad individual requiere un examen separado.

### 1.12. Irrevocabilidad y recuperación de fondos

La ejecución de una transferencia y la posibilidad de revertirla son cuestiones diferentes. Que el sistema haya asentado una operación no significa que el origen del dinero sea lícito o que exista una potestad general para deshacerla sin procedimiento. El análisis debe atender las reglas operativas del sistema de pagos, los contratos y las competencias de las autoridades, en lugar de presumir que todo monto puede recuperarse tras presentar una denuncia.

La rapidez de la notificación puede influir en las posibilidades de conservación de registros y en las gestiones permitidas frente a entidades participantes. Sin embargo, la recuperación, el bloqueo y la restitución requieren fundamentos jurídicos propios. El artículo distingue estas medidas de la prueba de la estafa: demostrar una operación irregular no acredita, por sí mismo, a quién corresponde responder civil o penalmente.

### 1.13. Protección del usuario y reclamos

Los mecanismos de reclamación financiera permiten examinar prestaciones, información entregada, medidas de seguridad y respuestas institucionales. Su finalidad no coincide necesariamente con la investigación de un delito. Una reclamación puede prosperar en el ámbito de protección de usuarios sin que se haya demostrado engaño penal, y una hipótesis delictiva puede subsistir aunque la entidad haya aplicado los procedimientos internos previstos.

Según la Asamblea Nacional del Ecuador (2022b), el examen de la normativa de defensa de los clientes financieros debe vincular cada obligación alegada con la conducta institucional correspondiente. En este marco, las constancias del reclamo, la respuesta de la entidad y los registros conservados pueden aportar a la reconstrucción, sin sustituir la acreditación de los elementos del artículo 186 del COIP (Asamblea Nacional del Ecuador, 2014a, art. 186).

Volumen: 4, Número: 4, Año: 2026 páginas 496-511
E-ISSN: 3103-1536
Bajo licencia: CC BY-SA 4.0

### 1.14. Datos personales y límites de acceso

Los registros financieros y de autenticación pueden contener información personal del ordenante, del receptor y de terceros. La Ley Orgánica de Protección de Datos Personales establece un marco para el tratamiento de esos datos, mientras que las diligencias penales deben sujetarse a las facultades y garantías previstas en la ley (Asamblea Nacional del Ecuador, 2021). La utilidad investigativa de un registro no constituye por sí sola autorización para difundirlo o acceder a todo su contenido.

Una solicitud de información debe justificar pertinencia, necesidad y alcance, diferenciando lo indispensable para comprobar la transferencia de datos ajenos al hecho investigado. También resulta necesario documentar quién recibió los archivos y con qué finalidad. Este procedimiento permite preservar el valor de la evidencia sin desconocer la privacidad de personas que pudieran no tener intervención penal.

### 1.15. La transformación de los servicios financieros tecnológicos

La expansión de servicios financieros tecnológicos introduce nuevos proveedores, interfaces y formas de interacción con el usuario. La Ley Orgánica para el Desarrollo, Regulación y Control de los Servicios Financieros Tecnológicos aborda este ámbito regulatorio; su existencia no implica que toda conducta realizada mediante una plataforma constituya un delito nuevo (Asamblea Nacional del Ecuador, 2022a). La calificación penal sigue dependiendo de los elementos de la disposición correspondiente.

Cuando una operación pasa por diversos prestadores, la cuestión probatoria se amplía hacia la identificación del responsable de cada etapa y la localización de registros. Esta complejidad exige determinar el servicio realmente utilizado y la normativa aplicable a ese actor. Sin esa delimitación sería improcedente atribuir al conjunto de proveedores las mismas obligaciones o asumir que la fragmentación tecnológica elimina las garantías procesales.

### 1.16. Denuncia e hipótesis inicial de investigación

Una denuncia sobre transferencias cuestionadas debe presentar la secuencia conocida, diferenciando manifestaciones del denunciante y datos comprobables. Para orientar la calificación es útil establecer si la persona impartió la orden por una representación falsa, si desconoce la operación o si existe un desacuerdo comercial posterior. Cada hipótesis conduce a diligencias diferentes y ninguna debe considerarse demostrada al inicio.

Las comunicaciones anteriores al pago, comprobantes, avisos del banco y respuestas del destinatario permiten construir una cronología inicial. Deben registrarse sus fuentes y limitaciones; una captura puede mostrar un mensaje, pero no certificar por sí sola la autoría de la cuenta que lo emitió. Así, la denuncia cumple una función de orientación sin reemplazar el posterior contraste probatorio.

### 1.17. Conservación de contenido digital

Volumen: 4, Número: 4, Año: 2026 páginas 496-511
E-ISSN: 3103-1536
Bajo licencia: CC BY-SA 4.0

El artículo 500 del COIP regula el contenido digital como información susceptible de tratamiento informático y contempla reglas para su obtención y análisis. En consecuencia, conservar un archivo implica atender a su procedencia, al dispositivo o sistema de origen y a las circunstancias de adquisición, no únicamente guardar una imagen visible en pantalla (Asamblea Nacional del Ecuador, 2014a, art. 500). La documentación del procedimiento permite examinar si hubo modificaciones posteriores.

En el contexto de transferencias, una conversación exportada, un correo de confirmación y un historial de acceso tienen características distintas. Es necesario preservar los elementos disponibles mediante procedimientos adecuados y dejar constancia de fechas, responsables y soportes. Las copias informales pueden orientar la investigación, pero su valor deberá discutirse a partir de su integridad y correspondencia con los registros originales.

### 1.18. Cadena de custodia y autenticidad

El artículo 456 del COIP prevé la cadena de custodia para elementos físicos y contenido digital con el objeto de garantizar su autenticidad, identidad y estado original mediante el registro de las condiciones y de quienes intervienen en recolección, traslado, manejo, examen y conservación. A su vez, el artículo 500 contiene previsiones específicas para el tratamiento de contenido digital (Asamblea Nacional del Ecuador, 2014a, arts. 456 y 500). Estas disposiciones obligan a explicar cómo ingresó cada elemento al procedimiento probatorio.

Por ejemplo, una conversación extraída de un teléfono debe asociarse con la identificación del soporte, la técnica utilizada, los responsables y las medidas que permitan detectar modificaciones. Un comprobante descargado por la víctima y un registro obtenido directamente de la entidad bancaria no poseen necesariamente el mismo origen ni alcance. La cadena de custodia contribuye a examinar integridad y trazabilidad, pero no demuestra por sí sola que el contenido sea verdadero o que su emisor sea el acusado.

### 1.19. Prueba bancaria y atribución individual

Los registros de una entidad permiten verificar importes, fechas, cuentas y estados de procesamiento dentro del alcance del sistema que los produjo. Su utilidad consiste en documentar la ruta transaccional; no identifican necesariamente a la persona que ideó una oferta falsa o controló un dispositivo. La atribución individual requiere contrastar estos datos con comunicaciones, evidencias de acceso y circunstancias del hecho.

El titular de una cuenta puede coincidir con el beneficiario real o actuar bajo instrucciones de otra persona. También es posible que la cuenta haya sido utilizada sin conocimiento del titular. Una conclusión sobre autoría debe explicar qué registros respaldan cada inferencia y qué hipótesis se descartaron. La coincidencia de nombres y números de cuenta constituye un punto de partida, no la totalidad de la prueba penal.

Volumen: 4, Número: 4, Año: 2026 páginas 496-511
E-ISSN: 3103-1536
Bajo licencia: CC BY-SA 4.0

### 1.20. Pericia y contradicción en juicio

La pericia tecnológica puede examinar metadatos, registros de acceso, integridad de archivos y relaciones temporales entre actividades. Su intervención debe responder a preguntas concretas: qué dispositivo generó un dato, si el archivo conserva signos de alteración y qué límites presenta la técnica empleada. No corresponde pedir al perito una decisión sobre la configuración definitiva de la estafa, que exige valoración jurídica del conjunto probatorio.

La contradicción permite interrogar sobre métodos, fuentes, incertidumbres y explicaciones alternativas. Un registro que vincula una dirección técnica con una sesión no acredita de manera automática la identidad física del usuario. La valoración debe articular resultados periciales y otras pruebas con respeto a las garantías procesales, evitando convertir conclusiones técnicas parciales en presunciones de culpabilidad.

### 1.21. Tutela judicial y presunción de inocencia

La protección de quien denuncia un perjuicio exige acceso a mecanismos de reclamación e investigación, pero ello no reduce las garantías de la persona investigada. La Constitución reconoce la presunción de inocencia y el debido proceso, por lo que las dudas de atribución no pueden suplirse con la facilidad de rastrear una cuenta bancaria (Asamblea Constituyente, 2008, art. 76). La determinación penal debe descansar en hechos probados y en la aplicación del tipo correspondiente.

Es necesario diferenciar medidas de conservación, actuaciones de investigación y decisión sobre responsabilidad. La urgencia de recopilar datos puede justificar solicitudes previstas en la ley, no accesos indiscriminados ni difusión de información privada. La tutela de las partes depende de un procedimiento que permita verificar los hechos y discutir el significado de cada evidencia.

### 1.22. Reparación y responsabilidades concurrentes

La existencia de un perjuicio patrimonial puede dar lugar a vías de reparación distintas según la conducta acreditada y la relación jurídica. La responsabilidad penal de una persona por engaño no debe confundirse con el eventual incumplimiento contractual de un proveedor o con las obligaciones de una entidad financiera. Un mismo movimiento bancario puede ser objeto de valoración en varios ámbitos, pero cada pretensión requiere demostrar sus presupuestos.

La recuperación de fondos, cuando procede, tampoco acredita necesariamente los elementos del delito. Para formular una conclusión es preciso identificar el daño, su relación con la conducta, las vías disponibles y las medidas que la autoridad competente puede disponer. La investigación documental no permite afirmar qué resultados de reparación se obtienen en la práctica sin expedientes o datos empíricos.

### 1.23. Cooperación y temporalidad de la respuesta

La trazabilidad de una transferencia puede involucrar registros conservados por varias entidades, prestadores de comunicación o administradores de plataformas. Su disponibilidad depende de plazos,

Volumen: 4, Número: 4, Año: 2026 páginas 496-511
E-ISSN: 3103-1536
Bajo licencia: CC BY-SA 4.0

capacidades técnicas y autorizaciones de acceso. De ahí que la comunicación oportuna de una operación controvertida pueda favorecer la preservación de documentos, sin garantizar por sí misma el reintegro de los fondos.

La cooperación institucional requiere identificar competencias, objeto de las solicitudes y protección de datos. Una propuesta de intercambio indiscriminado de información no se deriva de la necesidad de investigar con rapidez. El alcance de cualquier protocolo debe justificarse frente a las reglas legales aplicables y a los riesgos de acceso excesivo.

### 1.24. Posibilidades y límites de una reforma penal

El desarrollo de nuevas modalidades tecnológicas no demuestra por sí mismo la existencia de una laguna en la tipificación. Los artículos 186 y 190 del COIP ya ofrecen descripciones que permiten estudiar, respectivamente, el engaño que lleva a una disposición patrimonial y determinadas apropiaciones o transferencias no consentidas mediante intervención de medios electrónicos (Asamblea Nacional del Ecuador, 2014a, arts. 186 y 190). Antes de proponer otro delito debe identificarse una conducta concreta que no pueda subsumirse legítimamente en las disposiciones vigentes.

Este análisis documental no presenta una muestra de expedientes ni sentencias que demuestre fallas estructurales de punición. Por ello, no permite sostener como resultado una reforma específica. Sí permite formular una cuestión para investigaciones posteriores: determinar si las dificultades descritas provienen de vacíos normativos, de obtención de evidencia o de coordinación entre participantes del sistema financiero.

### 1.25. Prevención compatible con derechos

La prevención de fraudes puede comprender información al usuario, mecanismos de verificación y atención de alertas. Estas actuaciones tienen una finalidad distinta de la persecución penal y deben examinarse dentro del régimen que corresponde a cada prestador. La Constitución y las disposiciones sobre protección de datos ofrecen límites a la utilización de información personal, incluso cuando se persigue la reducción de operaciones irregulares (Asamblea Constituyente, 2008; Asamblea Nacional del Ecuador, 2021).

Las medidas preventivas no deben trasladar sin fundamento al usuario toda la responsabilidad por haber autorizado técnicamente una orden, ni convertir a los intermediarios en garantes penales de cualquier pérdida. Para evaluar su pertinencia harían falta indicadores verificables sobre aplicación y resultados. En ausencia de esos datos, el artículo solo identifica criterios normativos para compatibilizar seguridad, información y derechos.

Volumen: 4, Número: 4, Año: 2026 páginas 496-511
E-ISSN: 3103-1536
Bajo licencia: CC BY-SA 4.0

**Síntesis de resultados: matriz interpretativa**

| Supuesto | Pregunta decisiva | Orientación jurídica |
|---|---|---|
| Pago realizado por oferta falsa | ¿Engaño previo que causó error y disposición? | Examinar estafa, art. 186, con prueba de elementos |
| Fondos trasladados sin orden consentida | ¿Manipulación o intervención informática típica? | Contrastar apropiación fraudulenta electrónica, art. 190 |
| Pago pactado y posterior incumplimiento | ¿Existía dolo y falsedad inicial acreditados? | Evitar criminalizar por sí solo un incumplimiento |
| Uso de cuenta receptora ajena | ¿Qué participación concreta tuvo su titular? | Individualizar conocimiento y aporte |
| Operación autenticada y reclamada | ¿Qué prueba realmente la autenticación? | Examinar consentimiento, controles, registros y reclamo |

La matriz presenta criterios de análisis y no reglas de decisión automáticas. Cada supuesto exige revisar el texto vigente del tipo penal aplicable, la secuencia fáctica y la evidencia admisible. Los resultados se obtienen mediante lectura integrada de normas y categorías, sin atribuirles una validación estadística inexistente.

**Análisis de los resultados**

El primer resultado es la necesidad de delimitar el mecanismo de desapoderamiento antes de seleccionar el tipo penal. Una transferencia electrónica funciona como vehículo de la disposición patrimonial tanto en conductas que pueden constituir estafa como en situaciones sin relevancia penal. Por esta razón, el dato bancario se debe interpretar junto con el discurso que precedió al pago y con la identidad de quienes intervinieron. Una operación autorizada técnicamente puede haber sido inducida por engaño, mientras que una operación no consentida puede revelar una intervención distinta.

El segundo resultado es que las reglas del sistema de pagos y la normativa financiera sirven para esclarecer las obligaciones de custodia informativa y las posibilidades de reconstrucción de la operación, pero no sustituyen las categorías del derecho penal. Esta conclusión también limita las afirmaciones absolutas sobre reversión de pagos. En cada caso deben examinarse estado del movimiento, reglas de aceptación, participación de las entidades y vías de reclamación. La diferencia entre ordenar, aceptar, compensar y liquidar pagos es operativamente relevante.

El tercer resultado concierne a la evidencia. Una captura de pantalla, un comprobante y un número de cuenta pueden ser indicios; su alcance probatorio no es idéntico. La hipótesis acusatoria se fortalece mediante correspondencia entre comunicaciones verificadas, registros bancarios, autenticación,

Volumen: 4, Número: 4, Año: 2026 páginas 496-511
E-ISSN: 3103-1536
Bajo licencia: CC BY-SA 4.0

cronología y elementos que identifiquen a los autores. El control sobre obtención, integridad y cadena de custodia no es una formalidad prescindible, pues condiciona la posibilidad de examinar críticamente los elementos de prueba.

Un cuarto resultado muestra que la intervención estatal debe operar con límites diferenciados. La víctima requiere canales de atención y medidas de conservación oportunas; el investigado dispone de garantías de contradicción y presunción de inocencia; y terceros ajenos al proceso mantienen derechos respecto de sus datos. Los deberes de seguridad exigibles al prestador del servicio se examinan a partir de normas concretas y de su relación con la operación. No resulta adecuado resolver todos estos ámbitos mediante una sola etiqueta de fraude electrónico.

## DISCUSIÓN

La tesis de Gómez Ramos (2025) constituye un antecedente para delimitar las dificultades atribuidas a las transferencias virtuales y la estafa. No obstante, las entrevistas de ese trabajo no se reproducen ni se someten aquí a una nueva revisión empírica. La contribución del artículo es documental: distinguir los elementos de la estafa del artículo 186, la apropiación fraudulenta del artículo 190 y los requisitos de tratamiento de contenido digital de los artículos 456 y 500 del COIP (Asamblea Nacional del Ecuador, 2014a). El contraste permite formular criterios de lectura jurídica, no conclusiones sobre el funcionamiento efectivo de tribunales o bancos.

Existe una tensión entre la celeridad de los medios de pago y el tiempo que requiere una investigación con garantías. Un movimiento puede completarse antes de que la persona advierta el engaño, mientras que identificar al responsable requiere preservar registros y obtener información mediante las vías autorizadas. Esta tensión no se resuelve atribuyendo responsabilidad objetiva al banco, al titular receptor o al usuario. Debe traducirse en reglas de colaboración, notificación y documentación que permitan investigar sin anular la estabilidad del sistema.

La discusión dogmática exige evitar dos extremos. El primero consiste en exigir siempre una manipulación técnica para reconocer el engaño patrimonial cometido por internet; ello dejaría fuera las transferencias ordenadas por la víctima bajo una representación falsa. El segundo consiste en calificar toda transferencia no reconocida como estafa, incluso si el titular no intervino en la disposición y los hechos se originan en una alteración informática. Ambos errores afectan la subsunción jurídica y pueden determinar líneas de prueba inadecuadas.

En materia de carga de la prueba, la evidencia técnica no ofrece certezas ilimitadas. Un registro puede acreditar acceso desde una cuenta, no necesariamente la identidad humana de quien actuó. La inferencia jurídica depende de la conexión con testimonios contrastados, registros complementarios y circunstancias anteriores y posteriores. Cuando se carece de esos vínculos, la investigación debe reconocerlo. Esta cautela no favorece a una parte sobre otra: protege la calidad de la decisión y reduce el riesgo de conclusiones basadas en la apariencia de precisión de un sistema informático.

Volumen: 4, Número: 4, Año: 2026 páginas 496-511
E-ISSN: 3103-1536
Bajo licencia: CC BY-SA 4.0

El alcance documental constituye una limitación expresa. No se examinaron sentencias ejecutoriadas mediante un protocolo exhaustivo ni se verificaron expedientes de transferencias específicas. Tampoco se utilizaron las entrevistas de la tesis base como entrevistas nuevas. Por tanto, el trabajo aporta una matriz de interpretación y criterios para orientar la recopilación de evidencia, no una medición de la frecuencia delictiva ni una evaluación empírica de efectividad de las entidades financieras. Futuras investigaciones podrían contrastar estos criterios con resoluciones y expedientes anonimizados.

## CONCLUSIONES

La transferencia bancaria electrónica es un medio de ejecución patrimonial, no una categoría penal autosuficiente. Para examinar la estafa se debe acreditar, en relación causal, el engaño, el error, la disposición patrimonial, el perjuicio y el elemento subjetivo correspondiente. La utilización de aplicaciones o plataformas no elimina esas exigencias ni convierte automáticamente un incumplimiento en un delito.

La distinción entre el artículo 186 y las conductas de apropiación fraudulenta mediante medios electrónicos requiere identificar si el desplazamiento surgió de una decisión de la víctima viciada por engaño o de una intervención no consentida sobre el sistema. La diferencia se refleja en el objeto de la investigación, en la construcción de la hipótesis y en los medios que deben recabarse.

El marco regulatorio de pagos, protección de usuarios y datos personales cumple una función complementaria. Sus disposiciones ayudan a precisar la infraestructura, las obligaciones operativas y las vías de reclamación; no permiten, por sí solas, presumir culpabilidad individual ni asegurar la reversión automática de una operación. La asignación de responsabilidades exige identificar deberes jurídicos y relaciones causales concretas.

La prueba digital demanda una reconstrucción conjunta de comunicaciones, registros de autenticación, trazas financieras y datos de atribución individual. La cadena de custodia, el examen pericial y la contradicción son indispensables para valorar su integridad y alcance. El comprobante de una transferencia no sustituye la demostración de engaño ni identifica necesariamente al autor.

Las posibles mejoras en conservación de registros, coordinación institucional y atención de reclamos se presentan como líneas de examen posterior, no como efectos comprobados por este estudio. Antes de plantear reformas penales o protocolos obligatorios se requiere contrastar el marco normativo con expedientes, decisiones judiciales y prácticas documentadas. El alcance del presente artículo se limita a determinar criterios de calificación y exigencias probatorias a partir de las fuentes analizadas.

Volumen: 4, Número: 4, Año: 2026 páginas 496-511
E-ISSN: 3103-1536
Bajo licencia: CC BY-SA 4.0

## REFERENCIAS BIBLIOGRÁFICAS

Asamblea Constituyente. (2008). Constitución de la República del Ecuador. Registro Oficial No. 449. https://www.asambleanacional.gob.ec/es/contenido/constitucion-de-la-republica-del-ecuador

Asamblea Nacional del Ecuador. (2014a). Código Orgánico Integral Penal. Registro Oficial Suplemento No. 180. https://www.presidencia.gob.ec/wp-content/uploads/2024/05/CODIGO_ORGANICO_INTEGRAL_PENAL_COIP_2024.pdf

Asamblea Nacional del Ecuador. (2014b). Código Orgánico Monetario y Financiero. Registro Oficial Suplemento No. 332.

Asamblea Nacional del Ecuador. (2021). Ley Orgánica de Protección de Datos Personales. Registro Oficial Quinto Suplemento No. 459. https://www.registroficial.gob.ec/267223-2/

Asamblea Nacional del Ecuador. (2022a). Ley Orgánica para el Desarrollo, Regulación y Control de los Servicios Financieros Tecnológicos. Registro Oficial Suplemento No. 215.

Asamblea Nacional del Ecuador. (2022b). Ley Orgánica para Defender los Derechos de los Clientes del Sistema Financiero Nacional y Evitar Cobros Indebidos y Servicios No Solicitados. Registro Oficial.

Gómez Ramos, J. R. (2025). Las transferencias bancarias virtuales y el delito de estafa en Ecuador [Trabajo de titulación, Universidad Técnica de Ambato]. Repositorio Institucional UTA. https://repositorio.uta.edu.ec/server/api/core/bitstreams/94aa9b27-c994-490d-92af-2156bf2cc3e7/content