RPNS: 2067 | ISSN: 1817-9088
Volumen 24 (2027)
N° 1 (enero - marzo)

Original **Recibido: 19/08/2026 | Aceptado: 19/11/2026**

Suficiencia penal y trazabilidad probatoria del fraude mediante engaño digital en el Perú

Criminal law adequacy and evidentiary traceability of digital deception for data acquisition in Peru

Mary Rebeca Silva Franco. Magíster en Derecho Penal. Profesional independiente. Ica, Perú. [canela02092017@gmail.com]

Resumen

El estudio analizó la suficiencia de los artículos 8 y 9 de la Ley N.° 30096 frente al fraude digital mediante suplantación en el Perú, durante el periodo 2023-2025, y examinó las barreras probatorias que afectan su persecución penal. Se desarrolló una investigación cualitativa, básica, exploratoria y propositiva, con diseño no experimental y transeccional. Se combinaron el análisis normativo y documental con trece entrevistas semiestructuradas a tres magistrados, cuatro fiscales y seis especialistas en litigación penal del Distrito Judicial de Ica, seleccionados mediante un muestreo intencional hasta alcanzar la saturación temática. Los resultados mostraron que el artículo 8 comprende los supuestos de manipulación informática que producen provecho ilícito y perjuicio patrimonial, mientras que el artículo 9 resulta aplicable cuando se acredita la utilización de una identidad ajena y un perjuicio verificable. Se identificaron dificultades para delimitar la preparación, tentativa y consumación, así como cuatro barreras probatorias: preservación incompleta o tardía de mensajes y metadatos, falta de correlación entre registros técnicos y operaciones, ausencia de constancias de actuaciones realizadas a nombre de las personas afectadas y cooperación fragmentada con entidades privadas. Se formuló un procedimiento de preservación, correlación e intercambio estructurado de información, junto con un piloto

institucional de seis meses. Se concluyó que no se justifica crear un delito autónomo, sino fortalecer la aplicación de los tipos vigentes y la trazabilidad probatoria.

Palabras clave: cooperación institucional, delitos informáticos, evidencia digital, fraude digital, suplantación de identidad, trazabilidad

Abstract

This study analyzed the adequacy of Articles 8 and 9 of Peruvian Law No. 30096 in addressing digital fraud through impersonation in Peru during the 2023–2025 period and examined the evidentiary barriers affecting criminal prosecution. A qualitative, basic, exploratory, and propositional study was conducted using a non-experimental, cross-sectional design. Legal and documentary analysis was combined with thirteen semi-structured interviews involving three judges, four prosecutors, and six criminal litigation specialists from the Judicial District of Ica, selected through purposive sampling until thematic saturation was reached. The results showed that Article 8 covers cases involving computer manipulation that produces unlawful gain and financial harm, whereas Article 9 applies when the use of another person's identity and verifiable harm are established. Difficulties were identified in distinguishing preparatory acts, criminal attempt, and completion, as well as four evidentiary barriers: late or incomplete preservation of messages and metadata, insufficient correlation between technical records and transactions, lack of verifiable records of actions performed in victims' names, and fragmented cooperation with private entities. A procedure for evidence preservation, correlation, and structured information exchange was formulated, together with a proposed six-month institutional pilot. It was concluded that creating a separate criminal offence is not justified; strengthening the application of existing offences and evidentiary traceability is preferable.

Keywords: cybercrime, digital evidence, digital fraud, identity impersonation, institutional cooperation traceability

Introducción

La expansión de las actividades económicas y sociales mediante plataformas digitales ha incrementado la exposición de personas y organizaciones a modalidades de fraude basadas en la manipulación de comunicaciones, interfaces y mecanismos de autenticación. Entre estas prácticas, el fraude digital mediante suplantación y captación ilícita de datos (conocido en inglés como: phishing) ocupa un lugar relevante debido a su capacidad para inducir a las víctimas a revelar credenciales, proporcionar información confidencial o ejecutar acciones que facilitan el acceso no autorizado a sus cuentas. Sus consecuencias pueden comprender pérdidas económicas, afectaciones a la identidad y compromisos de seguridad que trascienden el episodio inicial. La literatura reciente reconoce que esta modalidad evoluciona mediante diferentes canales y estrategias de ingeniería social, por lo que su prevención y mitigación requieren integrar componentes tecnológicos y factores asociados al comportamiento humano (Naqvi et al., 2023; Thomopoulos et al., 2024).

La complejidad del phishing no se limita a la obtención inicial de información. La secuencia puede comprender la elaboración de mensajes fraudulentos, la suplantación de páginas o servicios legítimos, la captura de credenciales y su utilización posterior para acceder a cuentas, modificar datos o realizar operaciones en nombre de las víctimas. Esta diversidad dificulta establecer una correspondencia directa entre el mecanismo de engaño, la persona que lo ejecuta y el resultado producido. Althobaiti y Alsufyani (2024) identificaron, mediante una revisión de investigaciones sobre ataques dirigidos a organizaciones, que la producción científica ha prestado especial atención a la detección y concienciación, mientras persisten desafíos relacionados con otras dimensiones de la respuesta frente a estas amenazas. En la misma dirección, Kavya y Sumathi (2025) describieron la evolución de los métodos de detección y las dificultades que plantean las nuevas estrategias utilizadas por los atacantes.

Universidad de Granma. Bayamo MN, Cuba.
Carretera de Manzanillo Km 17 ½ Bayamo. Granma. Cuba.
C.P. 85100. http://olimpia.udg.co.cu

Desde la perspectiva jurídico-penal, la persecución de estas conductas exige diferenciar la existencia de una maniobra fraudulenta, la producción de un resultado lesivo y la atribución de responsabilidad a una persona determinada. La presencia de un mensaje engañoso o de una página suplantada no demuestra, por sí sola, que se haya consumado un fraude informático ni permite identificar automáticamente a quien intervino en su ejecución. En consecuencia, la valoración jurídica debe considerar la secuencia de acontecimientos y los elementos que permiten distinguir los actos preparatorios, la tentativa y la consumación. Esta exigencia adquiere mayor relevancia cuando las campañas se desarrollan de forma masiva o automatizada, pues el volumen de comunicaciones no sustituye la acreditación de los elementos constitutivos de la conducta. Las revisiones sobre ingeniería social y ataques de suplantación confirman la heterogeneidad de sus mecanismos y la necesidad de respuestas que no dependan exclusivamente de herramientas de detección tecnológica (Naqvi et al., 2023; Rathod et al., 2025).

En el Perú, la Ley N.° 30096, Ley de Delitos Informáticos, contempla figuras relevantes para examinar penalmente las conductas asociadas con el phishing. El artículo 8 regula el fraude informático y, tras la modificación introducida por el Decreto Legislativo N.° 1614, incorpora referencias expresas a la clonación de datos y a la suplantación de interfaces o páginas web. Por su parte, el artículo 9 sanciona la suplantación de identidad mediante tecnologías digitales cuando produce un perjuicio. A estas disposiciones se suman las modificaciones efectuadas por el Decreto Legislativo N.° 1591 y la Ley N.° 32314, esta última relacionada con el empleo de inteligencia artificial en la comisión de delitos. Este marco plantea una cuestión de política criminal que no se reduce a determinar si existe una disposición aplicable, sino que requiere establecer si las figuras vigentes permiten responder de manera coherente a las distintas fases

Universidad de Granma. Bayamo MN, Cuba.
Carretera de Manzanillo Km 17 ½ Bayamo. Granma. Cuba.
C.P. 85100. *http://olimpia.udg.co.cu*

del engaño digital, sin extender sus elementos más allá de los límites establecidos por el principio de legalidad.

Sin embargo, la aplicación de estas disposiciones depende de la disponibilidad de evidencia digital íntegra, auténtica y técnicamente correlacionable. Una captura de pantalla puede mostrar el contenido de un mensaje, pero no necesariamente conserva sus cabeceras, metadatos, redirecciones, registros de acceso o información que permita reconstruir la sesión vinculada con una operación. Del mismo modo, la confirmación de una transacción financiera no acredita, por sí sola, quién controló el entorno de captura o ejecutó la operación. La preservación de los archivos originales, la documentación de su extracción y la continuidad de la cadena de custodia constituyen, por tanto, condiciones relevantes para su posterior valoración. AlKhanafseh y Surakhi (2024) examinaron alternativas tecnológicas para fortalecer la conservación e integridad de la evidencia digital, mientras Zhang y Gong (2024) analizaron las dificultades que presenta la investigación forense electrónica en escenarios de ciberdelincuencia transfronteriza.

A estas dificultades se añade la dependencia de información que permanece bajo control de entidades privadas, principalmente bancos, plataformas digitales y proveedores de servicios de comunicación. La reconstrucción de un incidente puede requerir registros de autenticación, identificadores de sesión, datos de dispositivos, constancias de recuperación de cuentas y documentación de operaciones. No obstante, las diferencias entre formatos de entrega, los tiempos de respuesta y la fragmentación de los requerimientos pueden impedir que esos registros se integren en una secuencia probatoria comprensible. Sachoulidou (2024) examinó la creciente relevancia de la cooperación entre autoridades y proveedores privados para acceder oportunamente a evidencia electrónica, y advirtió las implicaciones jurídicas que supone trasladar determinadas funciones de colaboración investigativa a estos actores. Por ello, la

Universidad de Granma. Bayamo MN, Cuba.
Carretera de Manzanillo Km 17 ½ Bayamo. Granma. Cuba.
C.P. 85100. http://olimpia.udg.co.cu

coordinación institucional debe considerar tanto la utilidad de la información como las garantías que limitan su obtención y tratamiento.

En este contexto, se identifica la necesidad de integrar el análisis de la suficiencia de las disposiciones penales con las condiciones técnicas y operativas que permiten demostrar los hechos investigados. Aunque la literatura ha desarrollado estudios sobre detección, prevención y mitigación del phishing, así como investigaciones sobre conservación de evidencia electrónica y cooperación con proveedores privados, resulta pertinente examinar conjuntamente estas dimensiones desde una realidad jurídico-institucional concreta. En particular, el Distrito Judicial de Ica ofrece un ámbito delimitado para analizar las dificultades de aplicación de los artículos 8 y 9 de la Ley N.° 30096 durante el periodo 2023-2025, considerando la experiencia de operadores jurídicos y especialistas en litigación penal.

Por consiguiente, el objetivo del estudio fue analizar la suficiencia penal y la trazabilidad probatoria de las conductas de engaño digital orientadas a la obtención de datos en el Perú, mediante la integración de las dimensiones jurídico-normativa, probatoria y de cooperación institucional, con referencia al Distrito Judicial de Ica durante 2023-2025. Se examinó el alcance de los artículos 8 y 9 de la Ley N.° 30096, la delimitación entre preparación, tentativa y consumación, las dificultades para vincular el mensaje fraudulento con la infraestructura, la sesión y la operación, así como las condiciones de preservación e intercambio de evidencia digital. El análisis buscó establecer si las principales limitaciones respondían a insuficiencias de tipificación o a dificultades en la aplicación y acreditación de las conductas, con atención a los principios de legalidad, responsabilidad individual y proporcionalidad.

Materiales y métodos

Se desarrolló una investigación cualitativa, de tipo básico, con alcance exploratorio y propositivo, mediante un diseño no experimental y transeccional. El análisis comprendió el

Universidad de Granma. Bayamo MN, Cuba.
Carretera de Manzanillo Km 17 ½ Bayamo. Granma. Cuba.
C.P. 85100. http://olimpia.udg.co.cu

periodo 2023–2025 y se delimitó al Distrito Judicial de Ica, Perú. Se empleó un método comparativo-inductivo para examinar la correspondencia entre las disposiciones penales aplicables al fraude digital mediante suplantación, su interpretación por los operadores jurídicos y las condiciones probatorias necesarias para sustentar su investigación. La integración de los dos componentes documentales permitió abordar, de manera articulada, la suficiencia de los artículos 8 y 9 de la Ley N.° 30096 y las dificultades relacionadas con la preservación, trazabilidad y utilización procesal de la evidencia digital.

La fuente empírica estuvo constituida por trece entrevistas semiestructuradas realizadas a informantes seleccionados mediante muestreo intencional: tres magistrados, cuatro fiscales y seis especialistas en litigación penal con experiencia profesional en el Distrito Judicial de Ica. Los criterios de inclusión comprendieron una experiencia mínima de tres años, desempeño profesional en el ámbito territorial delimitado y participación directa en asuntos relacionados con la materia durante el periodo estudiado. La saturación temática se alcanzó en la entrevista doce y se confirmó en la decimotercera, sin que esta última incorporara categorías sustancialmente nuevas. Las personas participantes fueron identificadas mediante los códigos E1–E13, con el propósito de preservar su identidad y confidencialidad.

El análisis documental comprendió la Ley N.° 30096, sus modificaciones correspondientes al periodo 2023–2025 y documentación técnica relacionada con los mecanismos de fraude digital mediante suplantación, autenticación y evidencia electrónica. Se consideraron especialmente el Decreto Legislativo N.° 1591, el Decreto Legislativo N.° 1614 y la Ley N.° 32314. El corpus empírico se examinó mediante una integración temática de los dos componentes de la investigación, sin incorporar nuevas entrevistas ni considerar las mismas trece declaraciones como muestras independientes. Para ello, se delimitaron las categorías de suficiencia normativa, encaje típico, preparación, tentativa, consumación, automatización,

Universidad de Granma. Bayamo MN, Cuba.
Carretera de Manzanillo Km 17 ½ Bayamo. Granma. Cuba.
C.P. 85100. http://olimpia.udg.co.cu

preservación de evidencia, trazabilidad de operaciones, atribución de responsabilidad y cooperación con actores privados.

El procesamiento de la información siguió una codificación temática orientada por las categorías anteriores. En una primera fase se identificaron los criterios de los informantes sobre la aplicación de los artículos 8 y 9 de la Ley N.° 30096 y las dificultades para distinguir los actos preparatorios de aquellos que podían constituir tentativa o consumación. En una segunda fase se examinaron las limitaciones probatorias relacionadas con la conservación del mensaje fraudulento, sus metadatos, los registros de autenticación, las sesiones digitales, las gestiones realizadas a nombre de los titulares y las operaciones asociadas. Finalmente, se efectuó una comparación entre los hallazgos empíricos y las disposiciones normativas para establecer coincidencias, vacíos operativos y criterios de articulación jurídica y probatoria. Las propuestas de paquete mínimo de evidencia, secuencia de preservación y cooperación interoperable se formularon como resultados propositivos, sin atribuirles una validación experimental o una implementación institucional previa.

La investigación contó con el consentimiento informado de las personas entrevistadas. La información se trató de forma confidencial y se utilizaron códigos alfanuméricos para evitar su identificación. Asimismo, el análisis se mantuvo dentro de los límites de la información documental y testimonial disponible, sin incorporar datos personales ni referencias a expedientes reservados. Por su naturaleza cualitativa y su delimitación territorial, los resultados no se interpretaron como estimaciones de prevalencia ni se plantearon como generalizables estadísticamente al conjunto del sistema judicial peruano.

Desarrollo

Suficiencia normativa de los artículos 8 y 9 de la Ley N.° 30096

Universidad de Granma. Bayamo MN, Cuba.
Carretera de Manzanillo Km 17 ½ Bayamo. Granma. Cuba.
C.P. 85100. http://olimpia.udg.co.cu

El análisis documental y las entrevistas permitieron identificar la aplicación de los artículos 8 y 9 de la Ley N.° 30096 a diferentes supuestos de fraude digital mediante suplantación. En el análisis se reconocieron situaciones relacionadas con la manipulación de datos, sistemas o interfaces digitales, así como con la utilización de identidades ajenas. Los casos examinados comprendieron conductas de obtención de información, realización de operaciones patrimoniales y ejecución de gestiones digitales a nombre de personas afectadas.

En relación con el artículo 8, se identificaron supuestos en los que la manipulación de datos, sistemas o interfaces digitales estuvo asociada con la obtención de un provecho ilícito en perjuicio de terceros. Entre las situaciones examinadas se encontraron transferencias, pagos y compras efectuados después de la captura de credenciales. También se registró la incorporación expresa de la clonación de datos y la suplantación de interfaces o páginas web mediante el Decreto Legislativo N.° 1614.

Respecto del artículo 9, se identificaron situaciones relacionadas con la utilización de una identidad ajena y la producción de un perjuicio. Entre ellas se encontraron altas de productos, modificaciones de información, recuperación de cuentas y emisión de órdenes o comunicaciones a nombre de la persona afectada. En estos supuestos, la documentación examinada comprendió registros de las gestiones realizadas y de los efectos asociados a dichas actuaciones.

Delimitación entre preparación, tentativa y consumación

Las entrevistas identificaron dificultades para establecer criterios uniformes de delimitación temporal de las conductas, especialmente en campañas masivas o automatizadas. Los informantes señalaron situaciones en las que se registraron numerosos mensajes fraudulentos sin que se dispusiera de información suficiente sobre las interacciones posteriores o sobre la existencia de resultados patrimoniales o identitarios.

Universidad de Granma. Bayamo MN, Cuba.
Carretera de Manzanillo Km 17 ½ Bayamo. Granma. Cuba.
C.P. 85100. http://olimpia.udg.co.cu

El análisis permitió organizar la secuencia del comportamiento en tres momentos principales. El primero correspondió a la preparación y difusión del mensaje o interfaz fraudulenta. El segundo comprendió la captura de credenciales o factores de autenticación y las gestiones posteriores relacionadas con el uso de la información obtenida. El tercero correspondió a la utilización de dichos datos para efectuar operaciones patrimoniales o realizar actuaciones a nombre de la persona afectada. La distribución de estos tres momentos, las conductas asociadas y los elementos probatorios identificados se presenta en la Tabla 1.

Tabla 1. Correspondencia entre las fases de la conducta y su relevancia jurídico-probatoria.

Fase identificada	Hecho susceptible de acreditación	Relevancia jurídico-penal	Evidencia necesaria
Preparación	Diseño y difusión del mensaje o interfaz fraudulenta	Acto preparatorio, como regla general	Mensaje íntegro, cabeceras, dominio y cronología
Captura	Obtención de credenciales y acceso al entorno de captura	Posible inicio de ejecución, según la conducta y finalidad acreditadas	Metadatos, registros de acceso y eventos de autenticación
Gestión fallida	Intento de autenticación, recuperación, alta o transferencia no completada	Elemento para examinar la tentativa	Identificador de sesión, dispositivo, hora y resultado del evento
Uso patrimonial	Transferencia, pago, compra o disposición económica mediante manipulación informática	Posible configuración del fraude informático previsto en el artículo 8	Registro de operación, destino, monto, sesión y perjuicio
Uso identitario	Alta, modificación, recuperación u orden realizada a nombre de la víctima con perjuicio	Posible configuración de la suplantación de identidad prevista en el artículo 9	Constancia del trámite, canal, validaciones, sello de tiempo y efecto

Fuente: Elaboración propia (2026)

Los criterios recogidos en las entrevistas permitieron identificar tres elementos relacionados con la documentación de las conductas en campañas masivas o automatizadas: la preservación íntegra del mensaje fraudulento y sus metadatos; la existencia de una traza técnica

Universidad de Granma. Bayamo MN, Cuba.
Carretera de Manzanillo Km 17 ½ Bayamo. Granma. Cuba.
C.P. 85100. http://olimpia.udg.co.cu

hacia un entorno de captura operativo; y la documentación de gestiones posteriores, como intentos de autenticación, altas de dispositivos, solicitudes de códigos o transferencias no completadas. Estos elementos fueron identificados como aspectos relevantes para el registro y la reconstrucción de la secuencia de los hechos.

Barreras para la preservación y trazabilidad de la evidencia digital

La integración de las entrevistas permitió reconocer cuatro barreras principales que afectaron la disponibilidad y utilidad procesal de la evidencia digital. Estas se relacionaron con la preservación tardía o incompleta del material inicial, la dificultad para vincular la sesión con la operación y la persona ejecutora, la ausencia de constancias verificables de actuaciones realizadas a nombre del titular y la fragmentación de la cooperación con entidades privadas. La distribución de estas barreras, sus principales manifestaciones y sus consecuencias para la disponibilidad y utilidad procesal de la evidencia digital se presentan en la Tabla 2.

Tabla 2. Barreras probatorias y sus efectos en la disponibilidad y utilidad procesal de la evidencia digital

Barrera	Manifestación identificada	Consecuencia para la investigación
Preservación tardía o incompleta	Capturas aisladas, enlaces inactivos y ausencia de cabeceras	Dificultad para establecer autenticidad, origen y secuencia
Falta de correlación técnica	Ausencia o incompatibilidad de identificadores de sesión, dispositivo y operación	Debilitamiento del vínculo entre ejecución y resultado
Gestión identitaria no documentada	Falta de constancias sobre actuaciones realizadas a nombre del titular	Limitación para acreditar la suplantación y sus efectos
Cooperación fragmentada	Respuestas tardías, parciales y formatos heterogéneos	Demoras, reprocesamiento y dificultad para integrar la información

Fuente: Elaboración propia (2026).

La integración de las entrevistas permitió identificar cuatro barreras relacionadas con la disponibilidad y documentación de la evidencia digital: preservación tardía o incompleta del material inicial, dificultades para relacionar los registros técnicos con las operaciones y las

Universidad de Granma. Bayamo MN, Cuba.
Carretera de Manzanillo Km 17 ½ Bayamo. Granma. Cuba.
C.P. 85100. http://olimpia.udg.co.cu

personas involucradas, ausencia de constancias documentales de actuaciones realizadas a nombre de la persona afectada y fragmentación de la cooperación con entidades privadas. Estas categorías se organizaron según las manifestaciones descritas por los informantes.

La primera barrera correspondió a la conservación del mensaje fraudulento y sus metadatos. Los informantes E1, E4, E7, E8, E9, E12 y E13 señalaron situaciones en las que el material se recibió después de que el contenido había cambiado o desaparecido. Entre las manifestaciones identificadas estuvieron las capturas de pantalla sin archivo original, los mensajes reenviados sin cabeceras, los enlaces inactivos y los horarios expresados en zonas temporales diferentes.

La segunda barrera se relacionó con la vinculación de los registros del entorno de captura, la sesión digital, la operación y la persona presuntamente ejecutora. Los informantes E3, E5, E10 y E11 identificaron dificultades para establecer correspondencia entre los registros técnicos disponibles y la persona que habría ejecutado la conducta. Entre los elementos cuya disponibilidad se consideró relevante estuvieron los identificadores de sesión, la información del dispositivo y los registros de acceso administrativo.

La tercera barrera comprendió la ausencia de constancias verificables de actuaciones realizadas a nombre de la persona afectada. Los informantes E1, E3 y E11 mencionaron las altas, modificaciones, recuperaciones de cuentas y órdenes efectuadas mediante canales digitales. Asimismo, señalaron la necesidad de disponer de información sobre el procedimiento realizado, las validaciones utilizadas, el responsable del registro y el efecto producido.

La cuarta barrera correspondió a la cooperación fragmentada con bancos y plataformas digitales. Las entrevistas describieron demoras, respuestas parciales y diferencias en los formatos de entrega de información. Entre las manifestaciones identificadas se encontraron

documentos narrativos sin campos estructurados, hojas de datos sin diccionarios de variables y comunicaciones distribuidas en varios correos electrónicos.

Requerimientos mínimos para la reconstrucción de los hechos

El análisis conjunto de las barreras identificadas permitió organizar seis componentes de información relacionados con la documentación del fraude digital mediante suplantación: mensaje, infraestructura, autenticación, gestión identitaria, operación y comunicaciones de voz o mensajería. Cada componente comprendió determinados registros y campos documentales, cuya distribución se presenta en la Tabla 3.

La información correspondiente al mensaje comprendió el archivo original o una exportación íntegra, con identificación del remitente, destinatario, cabeceras, enlace y fecha de recepción. El componente de infraestructura incluyó el dominio, los registros del Sistema de Nombres de Dominio (DNS), el Localizador Uniforme de Recursos (URL), el alojamiento, los certificados y los registros de acceso disponibles. En cuanto a la autenticación, se identificaron los intentos de acceso, factores utilizados, resultados, direcciones del Protocolo de Internet (IP), dispositivos, identificadores de sesión y marcas temporales.

La gestión identitaria comprendió los registros de altas, modificaciones, recuperaciones u órdenes realizadas a nombre del titular, con identificación del canal, las validaciones, el responsable y el efecto producido. La información sobre operaciones incluyó el tipo de transacción, monto, destino, identificador, estado y sesión asociada. Finalmente, en los casos que involucraron comunicaciones de voz o mensajería, se identificaron los archivos originales, participantes, metadatos, duración y transcripciones complementarias.

Tabla 3. Componentes de evidencia digital, campos mínimos y finalidad probatoria

Componente	Información requerida	Finalidad probatoria
Mensaje	Archivo íntegro, remitente, destinatario, cabeceras,	Acreditar el mecanismo de engaño y su origen

Universidad de Granma. Bayamo MN, Cuba.
Carretera de Manzanillo Km 17 ½ Bayamo. Granma. Cuba.
C.P. 85100. http://olimpia.udg.co.cu

	enlace y fecha UTC (Tiempo Universal Coordinado)	
Infraestructura	Dominio, DNS, URL, alojamiento, certificados y registros de acceso	Relacionar el mensaje con el entorno digital utilizado
Autenticación	Intentos, factores, resultados, IP, dispositivo, sesión y hora UTC	Reconstruir los accesos y eventos de autenticación
Gestión identitaria	Altas, cambios, recuperaciones, órdenes, canal, validaciones y responsable	Acreditar actuaciones realizadas a nombre del titular
Operación	Tipo, monto, destino, identificador, estado y sesión asociada	Identificar el resultado patrimonial y su secuencia
Voz o mensajería	Archivo original, participantes, metadatos, duración y transcripción	Conservar el contexto y los elementos de comunicación

Fuente: Elaboración propia (2026).

Secuencia de preservación y cooperación con actores privados

El análisis de las entrevistas y de la documentación examinada permitió identificar aspectos relacionados con la preservación de los registros digitales, la correspondencia entre sesiones y operaciones, y el intercambio de información entre los distintos custodios. A partir de estos elementos, se formuló una secuencia de actuación compuesta por seis etapas: preservación inicial del mensaje fraudulento; normalización de la cronología mediante el uso del Tiempo Universal Coordinado (UTC), conservando también la hora local declarada; asignación de un identificador único por incidente; emisión de requerimientos diferenciados según el custodio de la información; correlación de los registros del mensaje, acceso, sesión, gestión identitaria y operación; y verificación de integridad mediante valores de comprobación criptográfica o firma digital, cuando correspondiera.

La secuencia propuesta comprendió también la construcción de una línea temporal con tres categorías de información: evidencia del hecho, evidencia del resultado y evidencia de autoría. En esta organización se distinguieron los registros relativos a la difusión de la campaña

Universidad de Granma. Bayamo MN, Cuba.
Carretera de Manzanillo Km 17 ½ Bayamo. Granma. Cuba.
C.P. 85100. http://olimpia.udg.co.cu

fraudulenta, los correspondientes a las operaciones o actuaciones realizadas y aquellos vinculados con la identificación de quien habría ejecutado la conducta o controlado la sesión digital.

En cuanto a la cooperación con bancos y plataformas digitales, se formularon criterios para el intercambio de información entre las instituciones participantes. Estos comprendieron el establecimiento de canales electrónicos institucionales con acuse de recepción, identificación de responsables y plazos diferenciados según la urgencia del requerimiento. Asimismo, se propuso utilizar formatos estructurados, como valores separados por comas (CSV) o notación de objetos de JavaScript (JSON), acompañados de un diccionario de campos y una constancia legible. Para los casos en que la información solicitada no estuviera disponible, se contempló registrar el campo ausente y especificar si ello obedecía a su inexistencia, falta de conservación o restricción de acceso.

Finalmente, se formuló una distribución funcional de responsabilidades entre los actores participantes en la investigación. La víctima o persona receptora tendría a su cargo la conservación del mensaje y su contexto; la Policía Nacional, la documentación de la extracción y preservación técnica; el Ministerio Público, la dirección de los requerimientos y la articulación de las hipótesis de correlación; los bancos y las plataformas digitales, la preservación y entrega de los registros bajo su custodia; y los peritos, la descripción de la integridad, correspondencia y limitaciones de los elementos examinados.

Propuesta de evaluación operativa

Como resultado del análisis propositivo, se estructuró un modelo de evaluación institucional mediante un piloto de seis meses en el Distrito Judicial de Ica. El primer mes comprendería la elaboración del formulario de requerimiento y la designación de puntos de contacto institucionales; los cuatro meses siguientes se destinarían a la aplicación de los

Universidad de Granma. Bayamo MN, Cuba.
Carretera de Manzanillo Km 17 ½ Bayamo. Granma. Cuba.
C.P. 85100. http://olimpia.udg.co.cu

procedimientos en nuevos casos; y el sexto mes correspondería a la evaluación de la experiencia y al ajuste de los campos, plazos y responsabilidades establecidos.

La propuesta incluiría cuatro dimensiones de evaluación: oportunidad, integridad, utilidad y trazabilidad. La oportunidad se mediría mediante el tiempo transcurrido entre la emisión del requerimiento y la recepción de la respuesta. La integridad se determinaría a partir de la proporción de campos obligatorios entregados respecto del total solicitado. La utilidad se examinaría mediante la proporción de respuestas incorporadas a la investigación sin requerimientos complementarios. Finalmente, la trazabilidad se evaluaría según la posibilidad de relacionar el mensaje, la sesión digital y la operación mediante identificadores verificables. El piloto no fue ejecutado y el modelo no contó con validación empírica durante el periodo de estudio. Por tanto, la propuesta quedó formulada como un procedimiento de evaluación futura de los mecanismos de preservación de evidencia digital y cooperación institucional.

Los resultados permiten establecer que la suficiencia de los artículos 8 y 9 de la Ley N.° 30096 debe analizarse en función de las conductas y los resultados que pueden acreditarse durante la investigación. El artículo 8 comprende los supuestos en los que la manipulación de datos, sistemas o interfaces digitales se relaciona con la obtención de un provecho ilícito en perjuicio de terceros, mientras que el artículo 9 requiere demostrar la utilización de una identidad ajena y el perjuicio correspondiente. Esta diferenciación adquiere importancia porque una misma secuencia de fraude digital mediante suplantación puede incluir actuaciones con consecuencias patrimoniales y otras relacionadas con la identidad de la persona afectada. Por tanto, la calificación jurídica debe atender a los elementos objetivos de cada conducta y a su correspondencia con el resultado acreditado, sin asumir que todas las fases de una campaña constituyen necesariamente un mismo supuesto de consumación. En este sentido, los hallazgos

Universidad de Granma. Bayamo MN, Cuba.
Carretera de Manzanillo Km 17 ½ Bayamo. Granma. Cuba.
C.P. 85100. http://olimpia.udg.co.cu

respaldan una aplicación diferenciada de las figuras penales existentes, antes que la creación de una categoría delictiva autónoma.

La delimitación entre preparación, tentativa y consumación constituye uno de los principales problemas identificados, especialmente cuando la difusión de mensajes fraudulentos se realiza de manera masiva o automatizada. La existencia de numerosos mensajes no demuestra por sí misma que se haya iniciado la ejecución de una conducta penalmente relevante ni que se haya producido un perjuicio patrimonial o identitario. Steinmetz et al. (2025), mediante entrevistas a personal vinculado con investigaciones de ciberdelincuencia, identificaron dificultades relacionadas con el anonimato, el volumen de información, la jurisdicción y la obtención de datos de proveedores de servicios electrónicos. Estos aspectos coinciden con las dificultades señaladas por los informantes del Distrito Judicial de Ica, particularmente respecto de la conexión entre el entorno de captura, las sesiones digitales y las operaciones posteriores. La delimitación temporal de la conducta requiere, por tanto, identificar actuaciones verificables que permitan diferenciar la difusión inicial del mensaje, el inicio de la ejecución y la producción del resultado, sin convertir la cantidad de mensajes enviados en un indicador automático de responsabilidad penal.

Las dificultades relacionadas con la preservación del mensaje inicial y sus metadatos también deben examinarse desde los requisitos de autenticidad e integridad de la evidencia. D’Anna et al. (2023) destacaron que la cadena de custodia permite documentar las circunstancias de recolección, conservación, transferencia y análisis de los elementos examinados. Aunque su revisión aborda la práctica forense en un sentido amplio, sus planteamientos resultan pertinentes para la evidencia digital, cuya facilidad de reproducción, modificación y transmisión exige documentar cada intervención. En concordancia con los resultados, una captura de pantalla aislada no necesariamente permite reconstruir el origen del

Universidad de Granma. Bayamo MN, Cuba.
Carretera de Manzanillo Km 17 ½ Bayamo. Granma. Cuba.
C.P. 85100. http://olimpia.udg.co.cu

mensaje, sus características técnicas o su secuencia temporal. De ahí que la preservación deba considerar el archivo original o una exportación íntegra, los metadatos disponibles, la identificación de la fuente y el registro de las actuaciones realizadas desde la primera recepción. La utilización de valores de comprobación criptográfica puede contribuir al control de integridad, pero no sustituye la documentación de la procedencia ni demuestra, por sí sola, la identidad de quien produjo o transmitió el contenido.

La propuesta de organizar la información en seis componentes: mensaje, infraestructura, autenticación, gestión identitaria, operación y comunicaciones responde a la necesidad de reconstruir la secuencia técnica del incidente. Klasén et al. (2024) examinaron la función de la informática forense en la investigación de hechos delictivos y destacaron la importancia de integrar los rastros digitales en los procedimientos de análisis. Desde esta perspectiva, la información procedente de diferentes dispositivos, plataformas y sistemas debe interpretarse en relación con el evento que documenta y con los demás registros disponibles. En el estudio realizado, esta relación se expresó en la necesidad de conectar el mensaje fraudulento con el entorno de captura, los intentos de autenticación, la sesión digital, las gestiones realizadas a nombre del titular y las operaciones posteriores. Sin embargo, la coincidencia temporal o técnica entre dos registros no demuestra necesariamente que ambos hayan sido generados o controlados por una misma persona. La interpretación pericial debe precisar qué acredita cada elemento, cuáles son sus limitaciones y qué correspondencias pueden establecerse sin recurrir a inferencias no sustentadas.

La secuencia de actuación propuesta también debe valorarse desde la confiabilidad de los procedimientos utilizados para obtener y examinar la información. Stoykova y Franke (2023) plantearon un marco de evaluación de la confiabilidad de la informática forense que diferencia tres niveles: tecnología, método y aplicación. Esta distinción permite reconocer que

Universidad de Granma. Bayamo MN, Cuba.
Carretera de Manzanillo Km 17 ½ Bayamo. Granma. Cuba.
C.P. 85100. http://olimpia.udg.co.cu

la utilización de una herramienta técnica no garantiza automáticamente la fiabilidad de sus resultados; también deben examinarse el procedimiento aplicado y las condiciones concretas de su utilización. La propuesta formulada en esta investigación, que comprende la preservación inicial, la normalización temporal, la asignación de un identificador por incidente, los requerimientos diferenciados, la correlación de registros y la verificación de integridad, guarda correspondencia con esa exigencia de control metodológico. Asimismo, Patil et al. (2024) analizaron la aplicación de tecnologías de registro distribuido en la cadena de custodia y destacaron la importancia de mantener la integridad y verificabilidad de la evidencia durante su transferencia entre los participantes. Ambos trabajos respaldan la necesidad de documentar los procedimientos, aunque no permiten afirmar que la incorporación de una tecnología específica sea suficiente para garantizar la validez jurídica de cualquier registro digital.

La cooperación fragmentada entre instituciones públicas, entidades financieras y plataformas digitales constituye otro aspecto relevante de los resultados. Las demoras, respuestas parciales y diferencias en los formatos de entrega pueden dificultar la integración de los registros que se encuentran bajo custodia de distintos actores. Tosza (2024), al examinar los desafíos jurídicos derivados del acceso a evidencia electrónica después de la adopción del paquete normativo europeo sobre prueba electrónica, abordó los problemas de aplicación y las cuestiones pendientes en la cooperación para obtener información digital. Aunque su análisis corresponde a otro ordenamiento jurídico, permite reconocer que la disponibilidad de evidencia no depende exclusivamente de las capacidades de los órganos investigadores, sino también de los procedimientos de acceso y colaboración con quienes conservan los datos. En el ámbito peruano, los criterios propuestos de canales institucionales identificables, acuses de recepción, plazos diferenciados y formatos estructurados deben entenderse como mecanismos de organización de las solicitudes y entregas, no como una ampliación de las facultades legales de

Universidad de Granma. Bayamo MN, Cuba.
Carretera de Manzanillo Km 17 ½ Bayamo. Granma. Cuba.
C.P. 85100. http://olimpia.udg.co.cu

acceso. Su aplicación debe respetar las competencias de cada institución y los límites establecidos para la obtención y tratamiento de información personal.

La separación entre evidencia del hecho, evidencia del resultado y evidencia de autoría representa una condición importante para evitar que la existencia de registros digitales se interprete como demostración automática de responsabilidad individual. Bérubé et al. (2025), mediante el análisis de un caso judicial, identificaron dificultades operativas, técnicas y de gestión de información que pueden afectar la interpretación de los rastros digitales durante una investigación y un proceso penal. Sus resultados también señalaron riesgos asociados con la selección parcial de información y la construcción de explicaciones que no consideran elementos contradictorios. Esta observación coincide con la necesidad identificada en el presente estudio de distinguir la documentación de una campaña fraudulenta de los registros que acreditan una operación y de aquellos que permiten relacionarla con una persona determinada. En consecuencia, la reconstrucción cronológica debe incluir tanto las correspondencias como las discrepancias y los vacíos de información. La atribución de responsabilidad requiere elementos individualizadores y una valoración conjunta de la evidencia, sin que la existencia de una operación económica permita presumir quién controló la sesión desde la cual se ejecutó.

Finalmente, el piloto institucional de seis meses en el Distrito Judicial de Ica constituye una propuesta de evaluación futura y no una intervención cuyos resultados puedan darse por demostrados. Las dimensiones de oportunidad, integridad, utilidad y trazabilidad permitirían examinar el funcionamiento de los procedimientos formulados, mediante indicadores relacionados con los tiempos de respuesta, la entrega de campos solicitados, la incorporación de información a las investigaciones y la posibilidad de relacionar los distintos registros.

La pertinencia de esta evaluación se relaciona con las dificultades operativas descritas por la literatura sobre investigación digital y confiabilidad forense; sin embargo, su eficacia

Universidad de Granma. Bayamo MN, Cuba.
Carretera de Manzanillo Km 17 ½ Bayamo. Granma. Cuba.
C.P. 85100. http://olimpia.udg.co.cu

deberá determinarse mediante una aplicación posterior con participación de las instituciones involucradas. Asimismo, el carácter cualitativo del estudio y su delimitación al Distrito Judicial de Ica no permiten estimar la frecuencia nacional de las barreras identificadas. Por ello, los resultados deben interpretarse como una aproximación contextual a los problemas de aplicación normativa y documentación probatoria, cuya contrastación en otros distritos judiciales contribuiría a establecer el alcance de los criterios propuestos.

Conclusiones

Se concluye, que los artículos 8 y 9 de la Ley N.° 30096 ofrecen cobertura penal para los supuestos centrales de fraude digital mediante suplantación, siempre que se acrediten los elementos correspondientes a cada figura: provecho ilícito y perjuicio patrimonial derivados de la manipulación informática, en el primer caso, y utilización de una identidad ajena con perjuicio verificable, en el segundo; por tanto, los hallazgos no justifican la creación de un delito autónomo. La principal dificultad se concentra en delimitar los actos preparatorios, la tentativa y la consumación, especialmente en campañas masivas o automatizadas, donde resulta necesario relacionar el mensaje fraudulento, el entorno de captura y las gestiones orientadas al resultado.

Asimismo, se identificaron cuatro barreras probatorias: preservación tardía o incompleta del mensaje y sus metadatos, dificultades para vincular los registros técnicos con las sesiones y operaciones, ausencia de constancias verificables de actuaciones realizadas a nombre de las personas afectadas y fragmentación de la cooperación con bancos y plataformas digitales. Frente a estas limitaciones, la documentación de la evidencia requiere integrar información sobre el mensaje, la infraestructura digital, la autenticación, la gestión identitaria, las operaciones y las comunicaciones, mediante registros íntegros, cronologías normalizadas, identificadores correlacionables y una cadena de custodia documentada.

Universidad de Granma. Bayamo MN, Cuba.
Carretera de Manzanillo Km 17 ½ Bayamo. Granma. Cuba.
C.P. 85100. http://olimpia.udg.co.cu

La secuencia de actuación y los criterios de cooperación institucional formulados constituyen una propuesta para mejorar la preservación, el intercambio y la correlación de dicha información, con responsabilidades delimitadas y formatos estructurados. Finalmente, el piloto de seis meses propuesto para el Distrito Judicial de Ica permitiría evaluar la oportunidad, integridad, utilidad y trazabilidad del procedimiento; no obstante, al no haberse ejecutado durante el estudio, su eficacia permanece pendiente de validación empírica.

Referencias bibliográficas

AlKhanafseh, M., & Surakhi, O. (2024). Evidence preservation in digital forensics: an approach using blockchain and LSTM-based steganography. *Electronics*, *13*(18), 3729. https://doi.org/10.3390/electronics13183729

Althobaiti, K., & Alsufyani, N. (2024). A review of organization-oriented phishing research. *PeerJ. Computer science*, *10*, e2487. https://doi.org/10.7717/peerj-cs.2487

Bérubé, M., Beaulieu, L. A., Allard, S., & Denault, V. (2025). From digital trace to evidence: Challenges and insights from a trial case study. *Science & Justice*, *65*(5), 101306. https://doi.org/10.1016/j.scijus.2025.101306 https://www.sciencedirect.com/science/article/pii/S1355030625000905

Congreso de la República del Perú. (2013, 21 de octubre). *Ley N.° 30096, Ley de Delitos Informáticos*. Diario Oficial El Peruano. https://www.gob.pe/institucion/congreso-de-la-republica/normas-legales/239569-30096

Congreso de la República del Perú. (2023, 5 de julio). *Ley N.° 32314*. Diario Oficial El Peruano. https://www.gob.pe/institucion/congreso-de-la-republica/normas-legales/4565760-31814

D'Anna, T., Puntarello, M., Cannella, G., Scalzo, G., Buscemi, R., Zerbo, S., & Argo, A. (2023). The chain of custody in the era of modern forensics: From the classic procedures for

Universidad de Granma. Bayamo MN, Cuba.
Carretera de Manzanillo Km 17 ½ Bayamo. Granma. Cuba.
C.P. 85100. http://olimpia.udg.co.cu

gathering evidence to the new challenges related to digital data. *Healthcare*, *11*(5), 634. https://doi.org/10.3390/healthcare11050634

Kavya, S., & Sumathi, D. (2025). Staying ahead of phishers: A review of recent advances and emerging methodologies in phishing detection. *Artificial Intelligence Review*, *58*, 50. https://doi.org/10.1007/s10462-024-11055-z

Klasén, L., Fock, N., & Forchheimer, R. (2024). The invisible evidence: Digital forensics as key to solving crimes in the digital age. *Forensic Science International*, *362*, 112133. https://doi.org/10.1016/j.forsciint.2024.112133

Naqvi, B., Perova, K., Farooq, A., Makhdoom, I., Oyedeji, S., & Porras, J. (2023). Mitigation strategies against the phishing attacks: A systematic literature review. *Computers & Security*, *132*, 103387. https://doi.org/10.1016/j.cose.2023.103387

Patil, H., Kohli, R. K., Puri, S., & Puri, P. (2024). Potential applicability of blockchain technology in the maintenance of chain of custody in forensic casework. *Egyptian Journal of Forensic Sciences*, *14*, 12. https://doi.org/10.1186/s41935-023-00383-w

Poder Ejecutivo del Perú. (2023). *Decreto Legislativo N.° 1591*. Diario Oficial El Peruano. https://img.lpderecho.pe/wp-content/uploads/2023/12/Decreto-Legislativo-1591-LPDerecho.pdf

Poder Ejecutivo del Perú. (2023, 21 de diciembre). *Decreto Legislativo N.° 1614*. Diario Oficial El Peruano. https://busquedas.elperuano.pe/dispositivo/NL/2246611-13

Rathod, T., Jadav, N. K., Tanwar, S., Alabdulatif, A., Garg, D., & Singh, A. (2025). A comprehensive survey on social engineering attacks, countermeasures, case study, and research challenges. *Information Processing & Management*, *62*(1), 103928. https://doi.org/10.1016/j.ipm.2024.103928

Sachoulidou, A. (2024). Cross-border access to electronic evidence in criminal matters: The new EU legislation and the consolidation of a paradigm shift in the area of 'judicial' cooperation. *New Journal of European Criminal Law*, *15*(3), 256–274. https://doi.org/10.1177/20322844241258649

Steinmetz, K. F., Schaefer, B. P., Brewer, C. G., & Kurtz, D. L. (2025). The role of computer technologies in structuring evidence gathering in cybercrime investigations: A qualitative analysis. *Criminal Justice Review*, *50*(1), 67–84. https://doi.org/10.1177/07340168231161091

Stoykova, R., & Franke, K. (2023). Reliability validation enabling framework (RVEF) for digital forensics in criminal investigations. *Forensic Science International: Digital Investigation*, *45*, 301554. https://doi.org/10.1016/j.fsidi.2023.301554

Thomopoulos, G. A., Lyras, D. P., & Fidas, C. A. (2024). A systematic review and research challenges on phishing cyberattacks from an electroencephalography and gaze-based perspective. *Personal and Ubiquitous Computing*, *28*, 449–470. https://doi.org/10.1007/s00779-024-01794-9

Tosza, S. (2024). Electronic evidence after E-evidence package's adoption: Challenges for application and unresolved problems. *Studia Iuridica Lublinensia*, *33*(5), 237–260. https://doi.org/10.17951/sil.2024.33.5.237-260

Zhang, H., & Gong, X. (2024). The research on an electronic evidence forensic system for cross-border cybercrime. *The International Journal of Evidence & Proof*, *28*(1), 21–44. https://doi.org/10.1177/13657127231187059

Universidad de Granma. Bayamo MN, Cuba.
Carretera de Manzanillo Km 17 ½ Bayamo. Granma. Cuba.
C.P. 85100. http://olimpia.udg.co.cu