Poder Judicial del Perú
Corte Superior de Justicia de Lima

Cuadernillo N° 6

CATEDRA JUDICIAL

"**Ciberdelincuencia:** ¿Fraude informático, hurto agravado o estafa?"

Autor: Dr. Bonifacio Meneses Gonzáles

SERVIR ES NUESTRA MISIÓN
LA JUSTICIA CON ROSTRO HUMANO
NUESTRO OBJETIVO

OCTUBRE
2026

En la Gestión de la:

Dra. Miluska Cano López
Presidenta de la Corte Superior de Justicia de Lima

Dr. Bonifacio Meneses Gonzáles
Autor
Juez Superior Titular de la Séptima Sala Penal de Apelaciones
Presidente de la Comisión General de Capacitación de la Corte Superior de Justicia de Lima

Dr. Jaime Zevallos Durand
Presidente de la Comisión de Capacitación del Área Penal

El editor no se hace responsable de las opiniones recogidas, comentarios y manifestaciones vertidas por los autores. La presente obra recoge exclusivamente la opinión de su autor como manifestación de su derecho de libertad de expresión.

Tabla de Contenido

Presentación 04

Introducción 05

Caso Práctico N° 1: El falso asesor bancario 06

De la Estafa al Fraude Informático 08

Requisitos del Fraude Informático 10

Jurisprudencia de la Corte Suprema 12

Estándares Internacionales 13

Evidencia Digital: Herramienta de Análisis 14

Tabla de Contenido

Aplicación Integral al Caso del Falso Asesor 16

Checklist para verificar el Fraude Informático 18

Conclusiones 19

Referencias Bibliográficas y Jurisprudenciales 20

PRESENTACIÓN

- En la práctica fiscal y judicial es cada vez más frecuente conocer casos en los que una persona pierde sus ahorros después de recibir un mensaje o una llamada que simula provenir de su banco. Según el Sidpol, las denuncias por delitos informáticos pasaron de 19 101 en 2021 a 44 703 en 2025; y, según la Fiscalía Especializada en Ciberdelincuencia, entre enero y setiembre de 2025 el 68,88 % correspondió a **fraude informático**.

- Estos hechos suelen calificarse de manera dispar: como **estafa**, porque la víctima "entregó" sus claves; como **hurto agravado**, porque se usaron sistemas de transferencia electrónica de fondos; o como **fraude informático**, porque se operó un sistema con datos ajenos. En ocasiones, incluso, se imputan dos de estos delitos en concurso ideal por un mismo desplazamiento patrimonial.

- A ello se suma la situación del titular de la cuenta que recibió el dinero —la llamada **"cuenta mula"**—, a quien a veces se condena por el solo registro bancario y otras veces se absuelve sin examinar los indicios que rodean su conducta.

- La distinción no es académica: determina el tipo penal, la pena, los concursos posibles, la prueba que debe actuarse y la reparación civil. Una calificación incorrecta puede conducir a nulidades, a una doble valoración del mismo hecho o a la impunidad de quien facilita la salida del dinero.

- Además, el marco normativo ha cambiado: desde el **Decreto Legislativo 1614** (2023), el artículo 8 de la Ley 30096 menciona expresamente la **suplantación de interfaces o páginas web** y sanciona a quien colabora intencionalmente facilitando la transferencia de activos; y en 2026 el **Decreto Legislativo 1700** incorporó el delito de tráfico ilícito de datos informáticos.

- El presente cuadernillo propone criterios dogmáticos, jurisprudenciales y probatorios para diferenciar el **fraude informático** de la **estafa** y del **hurto agravado**, y para valorar la evidencia digital con la que se reconstruyen estos casos.

INTRODUCCIÓN

- La teoría del delito exige identificar **cómo se produjo el desplazamiento patrimonial**. En la estafa, la víctima engañada dispone de su patrimonio; en el fraude informático, el perjuicio lo produce un **sistema informático** que procesa datos introducidos o manipulados ilegítimamente por el agente.

- El **fraude informático**, previsto en el artículo 8 de la Ley 30096, protege el **patrimonio** frente a ataques que se valen del procesamiento automatizado de datos. Cuando concurren sus elementos, reconduce la calificación del *phishing*, el *vishing* y el *smishing* que terminan en transferencias no autorizadas.

Idea Central:

- No hay estafa cuando la víctima solo entrega datos: si la transferencia la ejecuta el sistema informático operado por el agente, el hecho es **fraude informático**.

- **¿Qué debe evitarse en la práctica?**
  - Calificar como estafa todo caso en que la víctima entregó sus claves por engaño.
  - Imputar hurto agravado y fraude informático en concurso ideal por el mismo desplazamiento patrimonial.
  - Presumir que el titular de la cuenta receptora conocía el origen ilícito del dinero.
  - Tratar una dirección IP o una captura de pantalla como prueba concluyente de autoría.

Clave teórica:

- Las máquinas no pueden ser engañadas. El error de la estafa exige una persona que dispone; cuando dispone un sistema informático, el engaño previo solo sirvió para obtener los datos, y lo decisivo es su **utilización ilegítima en el sistema** (art. 8, Ley 30096).

CASO PRÁCTICO: EL FALSO ASESOR BANCARIO

Carmen, de 68 años, es jubilada y titular de una cuenta de ahorros en la que recibe su pensión. El 9 de marzo de 2026, a las 15:20 h, recibe un SMS que simula provenir de su banco: "Detectamos un consumo no reconocido. Para bloquearlo, valide sus datos aquí", seguido de un enlace.

El enlace la lleva a una página idéntica a la del banco, donde registra el número de su tarjeta, su DNI y su clave de internet. A las 15:31 h la llama un hombre que dice ser asesor de seguridad del banco; conoce sus datos y le pide, para "anular la operación fraudulenta", el código de seis dígitos que le llegará por SMS. Carmen se lo dicta.

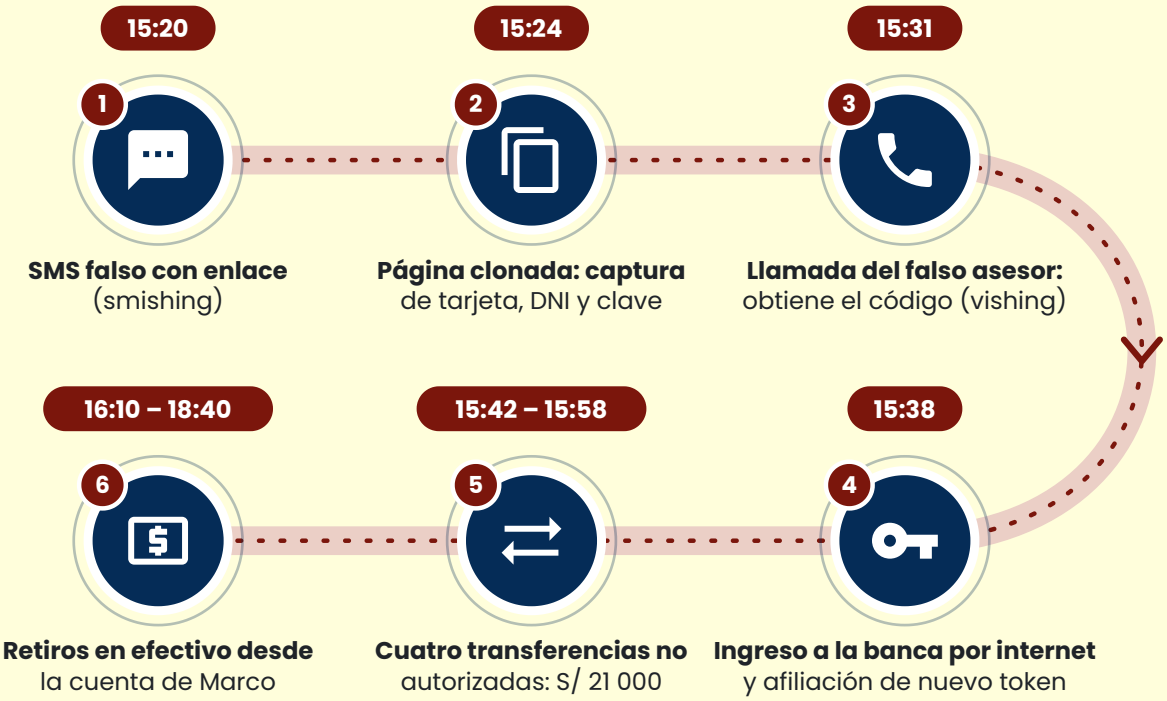
Con esos datos, desde un equipo y una IP ajenos a Carmen, se ingresa a su banca por internet, se afilia un nuevo dispositivo como token digital, se amplía el límite diario y, entre las 15:42 y las 15:58 h, se hacen tres transferencias por S/ 18 300 a la cuenta de Marco y una de S/ 2 700 a una billetera digital. Carmen no ordenó ninguna de esas operaciones.

Marco, de 23 años, había "alquilado" su cuenta por S/ 300 a un contacto de un grupo de mensajería que ofrecía "trabajo desde casa". Esa tarde retiró el dinero en efectivo en seis operaciones, entregó S/ 18 000 a un motorizado y se quedó con su "pago". En las dos semanas previas, su cuenta recibió transferencias de otras tres personas, también retiradas en pocas horas, y en su celular se halló el mensaje "retira rápido antes de que bloqueen". Los registros de acceso condujeron a Julio, en cuyo celular se hallaron la plantilla de la página clonada y la afiliación del token.

Persona	Situación (perjuicio / imputación)
01 **Carmen** *Agraviada*	Perjuicio patrimonial de S/ 21 000: tres transferencias (S/ 18 300) a la cuenta de Marco y una (S/ 2 700) a una billetera digital, entre las 15:42 y las 15:58 h. No autorizó ninguna.
02 **Julio** *Acusado*	Se le atribuye el SMS con la página clonada, la llamada para obtener el código y la operación de la banca por internet. Los registros de acceso y la afiliación del token lo vinculan con su celular incautado.
03 **Marco** *Acusado*	Titular de la cuenta receptora. Retiró S/ 18 300 el mismo día, entregó S/ 18 000 a un tercero y conservó S/ 300. Alega que desconocía el origen del dinero.

Pregunta Jurídica:

¿El vaciamiento de la cuenta de Carmen, realizado con las claves que ella misma entregó por engaño, constituye **estafa**, **hurto agravado** por medios telemáticos o **fraude informático**? ¿Responde penalmente Marco, titular de la cuenta que recibió y retiró el dinero?



La importancia de reconstruir la secuencia digital de los hechos:

Los estados de cuenta describen un resultado: el dinero salió. La calificación exige reconstruir **cómo** salió: quién operó el sistema, con qué datos, desde qué dispositivo y quién dispuso del patrimonio.

- Carmen entregó datos, pero no ordenó ni autorizó ninguna transferencia.
- Las credenciales se capturaron en una página que suplantaba la interfaz del banco.
- El código de verificación se obtuvo mediante una llamada engañosa.
- Un tercero introdujo esos datos, afilió un nuevo token y amplió los límites de operación.
- El sistema bancario ejecutó las transferencias; el dinero se retiró en efectivo en pocas horas.
- La cuenta de Marco registraba el mismo patrón con otras tres víctimas.

DE LA ESTAFA AL FRAUDE INFORMÁTICO

Los delitos contra el patrimonio se diferencian por **la forma en que se produce el desplazamiento patrimonial**. En la **estafa** (arts. 196 y 196-A CP), el agente induce o mantiene en error a una persona, que dispone de su patrimonio en su propio perjuicio. En el **hurto** (arts. 185 y 186 CP), el agente se apodera del bien sin la voluntad de la víctima.

El **fraude informático** responde a una tercera estructura. Cuando el perjuicio se produce porque un sistema procesa datos introducidos, alterados o manipulados ilegítimamente, el engaño previo a la víctima es solo el medio para obtener esos datos: el núcleo típico está en su utilización indebida en el sistema.

Fraude informático:

Es la obtención de un provecho ilícito en perjuicio de tercero mediante la manipulación de datos informáticos o del funcionamiento de un sistema. Protege el **patrimonio** frente a ataques que se valen del procesamiento automatizado de datos.

Suplantación de interfaces o páginas web

Desde el D. Leg. 1614 (21/12/2023), el tipo menciona expresamente esta modalidad: sitios, aplicaciones o pantallas que imitan a los de una entidad para capturar datos o inducir operaciones. La página clonada no es un simple antecedente del fraude: es uno de los medios comisivos que la ley describe.

Artículo 8 de la Ley 30096 (texto vigente)

"El que deliberada e ilegítimamente procura para sí o para otro un provecho ilícito en perjuicio de tercero mediante el diseño, introducción, alteración, borrado, supresión, clonación de datos informáticos, suplantación de interfaces o páginas web o cualquier interferencia o manipulación en el funcionamiento de un sistema informático, será reprimido con una pena privativa de libertad no menor de cuatro ni mayor de ocho años y con sesenta a ciento veinte días-multa".

- **Forma agravada:** de cinco a diez años cuando se afecte el patrimonio del Estado destinado a fines asistenciales o a programas de apoyo social.
- **Colaborador:** "La misma pena se aplica al que intencionalmente colabora con la comisión de alguno de los supuestos de los párrafos precedentes, facilitando la transferencia de activos".

Clave de Análisis:

Pregunte primero **quién ejecutó la disposición patrimonial**. Si fue la víctima engañada, el caso se orienta a la estafa; si fue el sistema informático operado por el agente con datos ajenos o manipulados, se trata de fraude informático, que desplaza por especialidad al hurto agravado por medios telemáticos.

Tres estructuras típicas, una pregunta decisiva

Concurso aparente con el hurto agravado

El artículo 186, segundo párrafo, inciso 4, del Código Penal agrava el hurto cometido "mediante la utilización de sistemas de transferencia electrónica de fondos, de la telemática en general o la violación del empleo de claves secretas" (4 a 8 años). Ese supuesto y el fraude informático describen el mismo desplazamiento patrimonial por medios informáticos: hay **concurso aparente de leyes**, no concurso ideal. Prevalece el artículo 8 de la Ley 30096, norma especial y posterior que describe con precisión el medio comisivo; aplicar ambos tipos supondría valorar dos veces el mismo hecho.

¿Cuándo es estafa?

Si la víctima, engañada, realiza ella misma la transferencia —por ejemplo, "paga" un falso premio, una falsa deuda o una supuesta inversión desde su aplicación—, existe una disposición patrimonial humana y el caso se analiza como **estafa** (arts. 196 y 196-A CP; el inciso 5 del art. 196-A agrava la estafa realizada para sustraer o acceder a datos de tarjetas de ahorro o de crédito).

Conductas conexas que deben examinarse

- Adquisición, posesión y tráfico ilícito de datos informáticos o credenciales: art. 12-A de la Ley 30096 (D. Leg. 1700, 2026).
- Activación ilegal de líneas de servicios móviles: art. 9-A de la Ley 30096 (Ley 32451, 2025).
- Suplantación de identidad mediante tecnologías de la información: art. 9 de la Ley 30096.

REQUISITOS DEL FRAUDE INFORMÁTICO

1. Medio comisivo informático

El tipo describe medios alternativos: diseño, introducción, alteración, borrado, supresión o clonación de datos informáticos; suplantación de interfaces o páginas web; o cualquier interferencia o manipulación en el funcionamiento de un sistema. La introducción de datos auténticos —claves, códigos OTP— por quien no está autorizado a usarlos es una **introducción ilegítima**: el sistema procesa como válida una orden que su titular no dio.

Aplicación al Caso:

Julio utilizó una página que suplantaba la interfaz del banco para capturar las credenciales; luego introdujo en el sistema los datos y el código de Carmen, afilió un nuevo token y amplió los límites de operación. Concurren la suplantación de interfaces, la introducción ilegítima de datos y la manipulación del funcionamiento del sistema.

2. Perjuicio patrimonial de tercero

Es un delito de resultado: exige una disminución patrimonial económicamente evaluable, que puede recaer en el titular de la cuenta o en la entidad financiera. Se consuma con el desplazamiento del saldo; no es necesario que el agente llegue a retirar el dinero.

Regla:

El perjuicio se mide en la cuenta de origen, no en lo que el agente logró cobrar: la transferencia no autorizada consuma el delito, aunque luego parte del dinero sea bloqueado o recuperado.

Aplicación al Caso:

Carmen sufrió un perjuicio de S/ 21 000. El delito se consumó con las transferencias (15:42 a 15:58 h); los retiros posteriores pertenecen a la fase de agotamiento.

3. Provecho ilícito y dolo: "deliberada e ilegítimamente"

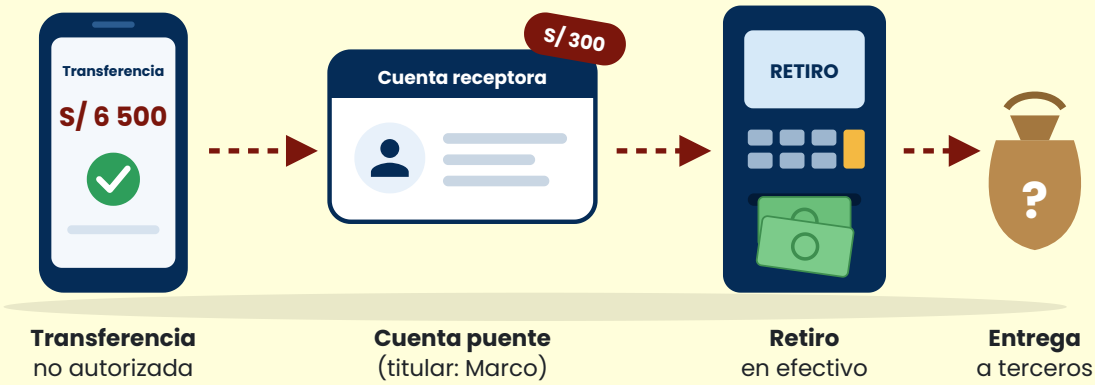
El agente debe actuar con conocimiento y voluntad de usar o manipular el sistema sin autorización del titular, y con la finalidad de procurar para sí o para otro un provecho económico indebido. No se exige que el provecho se obtenga: basta que se persiga.

Aplicación al Caso:

La secuencia planificada —SMS masivo, página clonada, llamada simulada, afiliación del token y transferencias inmediatas a una cuenta puente— revela dolo directo y finalidad lucrativa en la conducta de Julio.

4. Colaboración intencional: la "cuenta mula"

El tercer párrafo del artículo 8 sanciona con la misma pena a quien **intencionalmente** colabora con el fraude **facilitando la transferencia de activos**; típicamente, el titular de la cuenta puente. Ese término excluye la imputación por el solo hecho de ser titular: debe probarse que sabía que su aporte servía al fraude.



Regla:

La titularidad de la cuenta es un punto de partida, no una prueba de culpabilidad. El conocimiento se acredita con **indicios plurales, concordantes y convergentes** (R. N. 1912-2005/Piura, precedente vinculante): pago por "alquilar" la cuenta, ingresos de terceros desconocidos, retiros inmediatos en efectivo, entrega del dinero a terceros e instrucciones para evitar bloqueos.

Aplicación al Caso:

Marco cobró S/ 300 por poner su cuenta a disposición, recibió transferencias de cuatro víctimas en dos semanas, retiró el dinero en pocas horas, lo entregó a un tercero y recibió la instrucción de "retirar rápido antes de que bloqueen". Los indicios convergen en su **colaboración intencional**.

JURISPRUDENCIA DE LA CORTE SUPREMA

R. N. 780-2022, Lima Este (15/08/2023)

Un trabajador bancario usó indebidamente claves secretas de otros funcionarios para ingresar al sistema de la entidad y realizar transferencias. Condenado por delito informático y hurto agravado en concurso ideal, la Sala Penal Transitoria estableció que los hechos se subsumen solo en el **fraude informático** del artículo 8 de la Ley 30096, ley posterior y más favorable, y descartó el concurso ideal.

R. N. 1087-2025, Lima (16/03/2026)

El acusado proporcionó su DNI para recibir los fondos sustraídos de la cuenta de la agraviada y cobró el dinero en una agencia bancaria. Acusado por hurto agravado mediante sistemas de transferencia electrónica de fondos, la Sala Penal Transitoria reformó la calificación a **fraude informático** (art. 8, Ley 30096), por ser la norma más favorable.

Casación 3330-2022, El Santa (14/02/2024)

Un ejecutivo bancario usó DNI falsos para introducir en el sistema del banco datos de supuestos clientes y obtener tarjetas de crédito. La Sala Penal Permanente precisó que el fraude informático criminaliza la alteración de datos o la manipulación del sistema y, como el documento falso se usó precisamente para manipularlo, apreció unidad de acción: **concurso ideal** con falsedad material impropia.

R. N. 175-2023, Lima (10/11/2023)

Absolvió a quien obtuvo el duplicado de un chip que luego terceros usaron para transferir fondos por banca por internet: no se probó que supiera que su actuación contribuiría al fraude, y condenarlo por su sola intervención implicaba "incurrir en una responsabilidad objetiva", proscrita en el sistema penal.

Criterio Común:

La Corte Suprema reconduce al fraude informático los desplazamientos patrimoniales ejecutados con claves o datos ajenos en sistemas informáticos; admite el concurso ideal solo si concurre una lesión autónoma (como la falsedad), y exige probar el conocimiento de quien aporta el chip, el DNI o la cuenta.

ESTÁNDARES INTERNACIONALES

Convenio de Budapest sobre la Ciberdelincuencia: artículo 8

En vigor para el Perú desde el 1 de diciembre de 2019 (Resolución Legislativa 30913 y Decreto Supremo 010-2019-RE). Obliga a sancionar los actos deliberados e ilegítimos que causen un perjuicio patrimonial mediante la introducción, alteración, borrado o supresión de datos, o la interferencia en un sistema, con la intención de obtener un beneficio económico. Su Informe explicativo precisa que se busca sancionar "toda manipulación indebida realizada en el transcurso del procesamiento de datos con la intención de efectuar una transferencia ilegal de bienes". El artículo 8 de la Ley 30096 sigue este modelo.

Convenio de Budapest: herramientas procesales

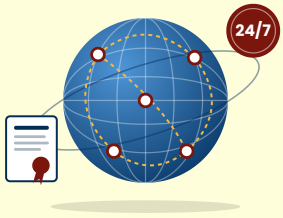
Prevé la conservación rápida de datos (arts. 16 y 17), la orden de presentación (art. 18), el registro y la confiscación de datos (art. 19), la obtención en tiempo real (arts. 20 y 21) y la Red 24/7 (art. 35): herramientas para preservar a tiempo una prueba volátil y, muchas veces, transfronteriza.

Convención de las Naciones Unidas contra la Ciberdelincuencia

Adoptada por la Asamblea General (Resolución 79/243, de 24 de diciembre de 2024) y abierta a la firma en Hanói en octubre de 2025, fue suscrita por el Perú y aún no entra en vigor. Su artículo 13 comprende, junto con la manipulación de datos y la interferencia en sistemas, el **engaño producido mediante un sistema de TIC** que lleva a una persona a actuar; y su artículo 17 exige sancionar el blanqueo del producto de estos delitos.

Corte IDH: Escher y otros vs. Brasil (2009)

La protección de la vida privada (art. 11 de la Convención Americana) alcanza a las comunicaciones. Su interceptación exige base legal, orden judicial motivada, fin legítimo, necesidad y proporcionalidad; la prueba obtenida sin esas garantías compromete su validez (art. VIII del Título Preliminar del CPP).



Consecuencia Práctica

La calificación debe ajustarse a la estructura internacional del fraude informático —perjuicio patrimonial por manipulación o uso indebido de datos— y la prueba digital debe preservarse y obtenerse por las vías legales, incluida la cooperación internacional, con respeto del secreto de las comunicaciones y del secreto bancario.

EVIDENCIA DIGITAL: HERRAMIENTA DE ANÁLISIS

La evidencia digital no determina por sí sola quién tiene razón. Su función es permitir reconstruir, con fiabilidad, qué ocurrió en el sistema —qué datos se introdujeron, desde qué dispositivo, en qué momento y con qué resultado— y, sobre todo, **a quién puede atribuirse** esa actuación. Es volátil, alterable y suele estar en poder de terceros (bancos, operadoras, plataformas), por lo que su valoración exige verificar su integridad, su origen y su licitud.

Concepto	Pregunta de verificación
01 **Integridad**	¿Se acreditó que el archivo o registro no fue modificado desde su obtención (copia forense, valor *hash*, acta de extracción)?
02 **Autenticidad y origen**	¿Se sabe quién generó el registro (banco, operadora, plataforma) y cómo llegó al proceso (orden judicial, requerimiento fiscal, entrega voluntaria)?
03 **Cadena de custodia**	¿Está documentado cada traslado o manipulación del soporte o del archivo, con responsables, fechas y condiciones de conservación?
04 **Coherencia técnica**	¿Los registros de acceso, direcciones IP, IMEI y horas son coherentes entre sí (misma zona horaria y secuencia lógica)?
05 **Atribución**	¿Qué prueba independiente vincula el dispositivo, la línea o la IP con la persona acusada?
06 **Licitud**	¿Se respetaron el secreto de las comunicaciones y el secreto bancario (arts. 2.10 y 2.5 de la Constitución; arts. 230 y 235 del CPP)?

¿Qué razonamientos pueden distorsionar el caso?

- **“Carmen entregó sus claves; entonces es estafa (o ella es responsable)”.**
  Entregar datos no es disponer del patrimonio: la transferencia la ordenó el agente a través del sistema. La eventual imprudencia de la víctima no excluye la tipicidad; la ingeniería social está diseñada, precisamente, para explotar la confianza.
- **“La IP identifica al autor”.**
  La IP identifica una conexión y, a lo sumo, a un abonado en un momento dado. La atribución exige corroboración: dispositivo incautado, IMEI, patrón de uso, pagos o testigos.

- **"Una captura de pantalla prueba el hecho (o no vale nada)".**
  Ni se sacraliza ni se descarta: su valor depende de su autenticación y corroboración. La Corte Suprema admitió capturas de WhatsApp cuando el acusado reconoció su número y no promovió su pericia (R. N. 600-2022, Lima).

- **"El dinero llegó a su cuenta; por tanto, es responsable".**
  Es responsabilidad objetiva, proscrita por el artículo VII del Título Preliminar del Código Penal. Debe probarse el conocimiento y la intención del titular (R. N. 175-2023, Lima).

- **"Sin pericia informática no hay prueba del fraude".**
  La pericia es muy útil, pero rige la libertad probatoria (art. 157 del CPP): registros bancarios, informes técnicos de la entidad, testimonios e indicios pueden acreditar los hechos.

Estos razonamientos sustituyen la reconstrucción técnica del hecho por conclusiones automáticas. El análisis debe centrarse en la secuencia de accesos y operaciones, en la fiabilidad de cada registro y en la prueba que vincula la actuación digital con una persona concreta.

Precisión:

La evidencia digital no es una prueba superior ni inferior a las demás: se valora conforme a las reglas de la lógica, la ciencia y las máximas de la experiencia (art. 158 del CPP).

Este enfoque no crea presunciones contra el acusado ni exime a la acusación de probar la autoría; exige, en cambio, controlar las condiciones técnicas que hacen fiable cada dato.

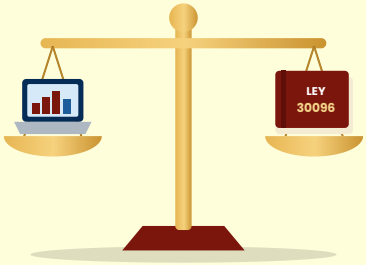
APLICACIÓN INTEGRAL AL CASO DEL FALSO ASESOR

Elemento	Valoración
01 **Medio comisivo informático**	Concurre. Julio usó una página que suplantaba la interfaz del banco para capturar las credenciales; luego introdujo los datos y el código de Carmen, afilió un nuevo token y amplió los límites.
02 **Perjuicio patrimonial**	Concurre. Salieron S/ 21 000 de la cuenta de Carmen en cuatro transferencias no autorizadas (15:42 a 15:58 h). El delito se consumó con las transferencias.
03 **Provecho ilícito y dolo**	Concurre. La secuencia planificada (SMS, página clonada, llamada simulada, afiliación del token y transferencias inmediatas a una cuenta puente) revela dolo directo y finalidad lucrativa.
04 **Disposición patrimonial**	No la realizó Carmen: entregó datos, pero las transferencias las ejecutó el sistema operado por Julio. Se descarta la estafa; el hurto agravado por medios telemáticos queda desplazado.
05 **Colaboración intencional (Marco)**	Concurre. Indicios plurales y convergentes: cobro por "alquilar" la cuenta, ingresos de otras tres víctimas, retiros en efectivo en pocas horas, entrega a un tercero y la instrucción de "retirar rápido".
06 **Evidencia digital**	Registros de acceso (IP y dispositivo), afiliación del token, *logs* de las transferencias y extracción forense del celular de Julio, con *hash* y cadena de custodia; la atribución se corrobora con el equipo incautado.

Conclusión del caso:

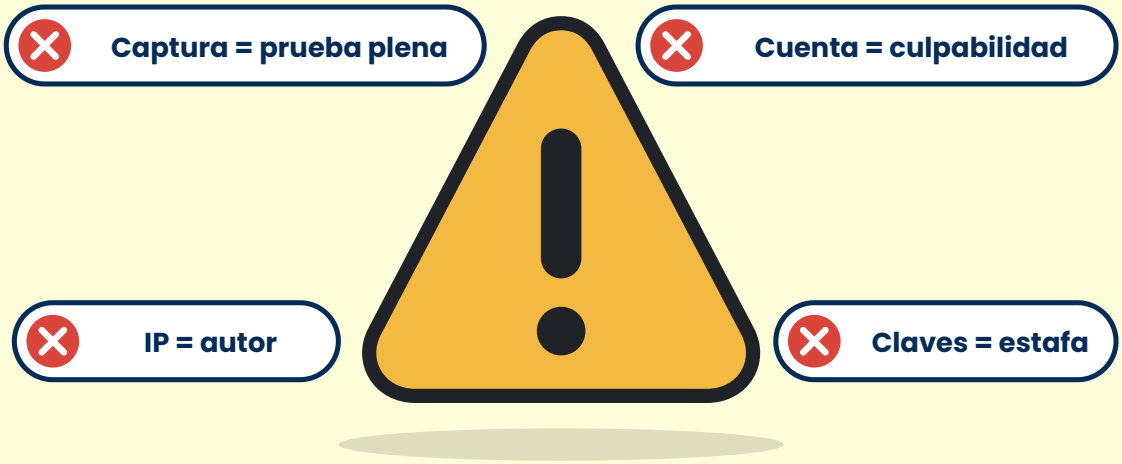
Julio responde como **autor de fraude informático** (art. 8, primer párrafo, de la Ley 30096, modificado por el D. Leg. 1614): obtuvo un provecho ilícito en perjuicio de Carmen mediante la suplantación de la interfaz del banco y la introducción ilegítima de sus datos en el sistema.

Marco responde conforme al **tercer párrafo** del mismo artículo, pues colaboró intencionalmente facilitando la transferencia de los activos. La reparación civil debe cubrir los S/ 21 000, sin perjuicio de los reclamos de la agraviada frente a la entidad financiera.



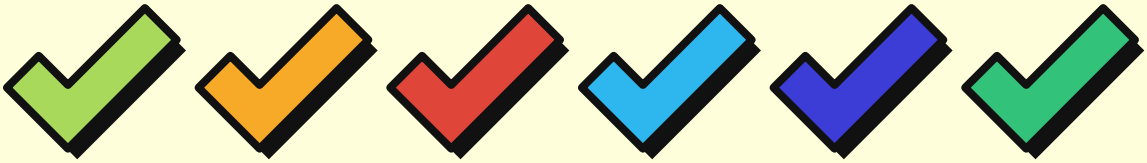
Errores que deben evitarse:

- Calificar como estafa todo caso en que la víctima entregó sus claves, sin determinar quién ejecutó la disposición patrimonial.
- Imputar en concurso ideal el hurto agravado (art. 186, segundo párrafo, inc. 4 CP) y el fraude informático por el mismo desplazamiento patrimonial.
- Condenar al titular de la cuenta receptora por el solo registro bancario, sin prueba de su colaboración intencional.
- Aplicar la agravante del art. 11.3 de la Ley 30096 (fin de obtener un beneficio económico) al fraude informático, que ya exige un provecho ilícito.
- Identificar automáticamente al titular de una IP, de una línea o de un dispositivo con el autor del hecho.
- Valorar capturas, reportes o registros sin verificar su origen, su integridad y su cadena de custodia.



Regla Final:

La transferencia define el delito: si la ordena la víctima engañada, es estafa; si la ejecuta el sistema operado por el agente, es fraude informático. Y quien presta su cuenta responde solo si se prueba que **colaboró intencionalmente**.



CHECKLIST PARA VERIFICAR EL FRAUDE INFORMÁTICO

- ¿Se identificó el medio comisivo informático concreto: introducción, alteración o supresión de datos, suplantación de interfaces o páginas web, o manipulación del sistema?
- ¿Se determinó quién ejecutó la disposición patrimonial: la víctima engañada o el sistema operado por el agente?
- ¿Está acreditado el perjuicio patrimonial, con montos, cuentas de origen y destino, y hora de cada operación?
- ¿Se probó que el acceso o la operación fue ilegítimo, sin autorización del titular, y el dolo de obtener un provecho ilícito?
- ¿Se descartó el concurso ideal con el hurto agravado del artículo 186, segundo párrafo, inciso 4, del Código Penal?
- ¿Se evaluó si concurren delitos que lesionan un bien jurídico distinto (falsedad documental, tráfico ilícito de datos del art. 12-A)?
- Respecto del titular de la cuenta receptora, ¿existen indicios plurales, concordantes y convergentes de su colaboración intencional?
- ¿La evidencia digital tiene integridad verificable, cadena de custodia documentada y origen lícito?
- ¿La atribución del acceso (IP, dispositivo o línea) está corroborada con prueba independiente?
- ¿Se aplicaron correctamente las agravantes del art. 11 de la Ley 30096 y se fijó una reparación civil que cubra el perjuicio?

CONCLUSIONES

- El fraude informático no es una estafa "por computadora": su núcleo no es el error de una persona, sino la manipulación o el uso ilegítimo de datos y sistemas que producen el desplazamiento patrimonial. Por ello, el *phishing* que termina en transferencias ejecutadas por terceros se subsume en el artículo 8 de la Ley 30096, que desplaza al hurto agravado por medios telemáticos.

- La tipicidad exige acreditar el medio comisivo informático, el perjuicio patrimonial, el provecho ilícito y la actuación deliberada e ilegítima. Desde el D. Leg. 1614, la suplantación de interfaces o páginas web y la colaboración intencional que facilita la transferencia de activos están previstas expresamente; esta última exige probar el conocimiento del colaborador.

- La evidencia digital es la columna vertebral de estos procesos: su integridad, su cadena de custodia y su licitud deben controlarse, y la atribución de autoría requiere corroboración. La Corte Suprema reconduce estos hechos al fraude informático y proscribe la responsabilidad objetiva del colaborador.

REFERENCIAS BIBLIOGRÁFICAS Y JURISPRUDENCIALES

- ASAMBLEA GENERAL DE LAS NACIONES UNIDAS. Resolución 79/243, *Convención de las Naciones Unidas contra la Ciberdelincuencia*. 24 de diciembre de 2024.
- CASEY, Eoghan. *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet*. 3.ª ed. Waltham: Academic Press, 2011.
- CHUMPITAZ, Óscar. "Ciberdelincuencia aumentó 134 % en los últimos 5 años en Perú". *La República*, 3 de mayo de 2026 (datos del Sidpol y de la Fiscalía Especializada en Ciberdelincuencia).
- CONSEJO DE EUROPA. *Convenio sobre la Ciberdelincuencia* (STE n.º 185) e Informe explicativo. Budapest, 23 de noviembre de 2001.
- CORTE INTERAMERICANA DE DERECHOS HUMANOS. Caso *Escher y otros vs. Brasil*. Sentencia de 6 de julio de 2009. Serie C, n.º 200.
- CORTE SUPREMA DE JUSTICIA DE LA REPÚBLICA. Casación n.º 3330-2022/El Santa. Sala Penal Permanente, 14 de febrero de 2024.
- CORTE SUPREMA DE JUSTICIA DE LA REPÚBLICA. Recurso de Nulidad n.º 175-2023/Lima. Sala Penal Transitoria, 10 de noviembre de 2023.
- CORTE SUPREMA DE JUSTICIA DE LA REPÚBLICA. Recurso de Nulidad n.º 600-2022/Lima. Sala Penal Transitoria.
- CORTE SUPREMA DE JUSTICIA DE LA REPÚBLICA. Recurso de Nulidad n.º 780-2022/Lima Este. Sala Penal Transitoria, 15 de agosto de 2023.
- CORTE SUPREMA DE JUSTICIA DE LA REPÚBLICA. Recurso de Nulidad n.º 1087-2025/Lima. Sala Penal Transitoria, 16 de marzo de 2026.
- CORTE SUPREMA DE JUSTICIA DE LA REPÚBLICA. Recurso de Nulidad n.º 1912-2005/Piura (prueba indiciaria), precedente vinculante conforme al Acuerdo Plenario n.º 1-2006/ESV-22.
- GALÁN MUÑOZ, Alfonso. *El fraude y la estafa mediante sistemas informáticos*. Valencia: Tirant lo Blanch, 2005.
- ISO/IEC 27037:2012. *Guidelines for identification, collection, acquisition and preservation of digital evidence*. Ginebra: ISO, 2012.
- MAYER LUX, Laura y OLIVER CALDERÓN, Guillermo. "El delito de fraude informático: concepto y delimitación". *Revista Chilena de Derecho y Tecnología*, vol. 9, n.º 1, 2020.
- MENESES GONZÁLES, Bonifacio y MENESES OCHOA, Jean Paul. *La cibercriminalidad. Consideración criminológica, político-criminal, dogmática, procesal y cooperación internacional*. 2.ª ed. Salamanca: UPSA Ediciones (Universidad Pontificia de Salamanca), 2026.
- MIRÓ LLINARES, Fernando. *El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio*. Madrid: Marcial Pons, 2012.
- PERÚ. Ley n.º 30096, Ley de Delitos Informáticos, modificada por la Ley n.º 30171, la Ley n.º 32451 y los Decretos Legislativos n.º 1614 (2023), 1700 (2026) y 1741 (2026).
- PERÚ. Código Penal (arts. 185, 186, 196 y 196-A) y Código Procesal Penal (arts. VIII del Título Preliminar, 157, 158, 230 y 235).
- REYNA ALFARO, Luis Miguel. *Los delitos informáticos. Aspectos criminológicos, dogmáticos y de política criminal*. Lima: Jurista Editores, 2002.
- VILLAVICENCIO TERREROS, Felipe. "Delitos informáticos". *Ius et Veritas*, n.º 49, 2014.

CORTE SUPERIOR DE JUSTICIA DE LIMA

https://www.instagram.com/csjdelima/
https://www.tiktok.com/@cortedelima
https://www.facebook.com/cortedelima
https://www.youtube.com/@CSJdeLIMA
https://x.com/CSJdeLima