



Universidad Nacional
Autónoma de México



Facultad de Estudios Superiores
Acatlán

CONFERENCIA · CIUDAD DE MÉXICO

Pruebas electrónicas y código hash

Obtención, preservación con hash, cadena de custodia y promoción de evidencias digitales en los procesos judiciales

Dr. José Luis Tamayo Rodríguez

Especialista en Derecho Digital, Pruebas Electrónicas y Evidencias Digitales

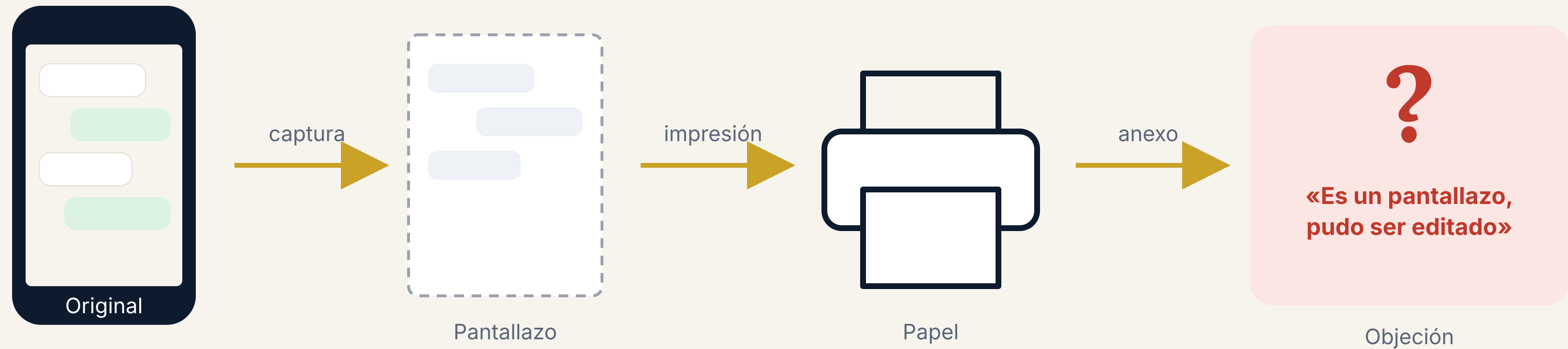
15 de octubre de 2026 · 7:00 p. m. (hora de México) · Ciudad de México



adc80fb9747f8386de77ada075834e08

cd892c163923ac87a83012b81032a35e

¿Cómo promovemos hoy un chat de WhatsApp?



- Sin metadatos ni encabezados
- Sin forma de verificar integridad
- El archivo original se queda en el teléfono...
- ... o se pierde

PREGUNTA

¿Promovemos la prueba... o solo la impresión de su fotografía?

El chat exportado: la conversación completa en .txt

Chat de WhatsApp con Juan Pérez.txt

conversación ficticia

12/10/26, 9:02 a. m. - Los mensajes y las llamadas están cifrados de extremo a extremo...

12/10/26, 9:15 a. m. - Juan Pérez: Buenos días, licenciada

12/10/26, 9:16 a. m. - Juan Pérez: Te debo 10000, te pago el viernes

12/10/26, 9:20 a. m. - María López: De acuerdo, quedo atenta

12/10/26, 9:21 a. m. - María López: IMG-20261012-WA0003.jpg (archivo adjunto)

16/10/26, 6:40 p. m. - Juan Pérez: *Se eliminó este mensaje*

16/10/26, 6:45 p. m. - Juan Pérez: Ya te transferí *<Se editó este mensaje.>*

Fecha

Hora

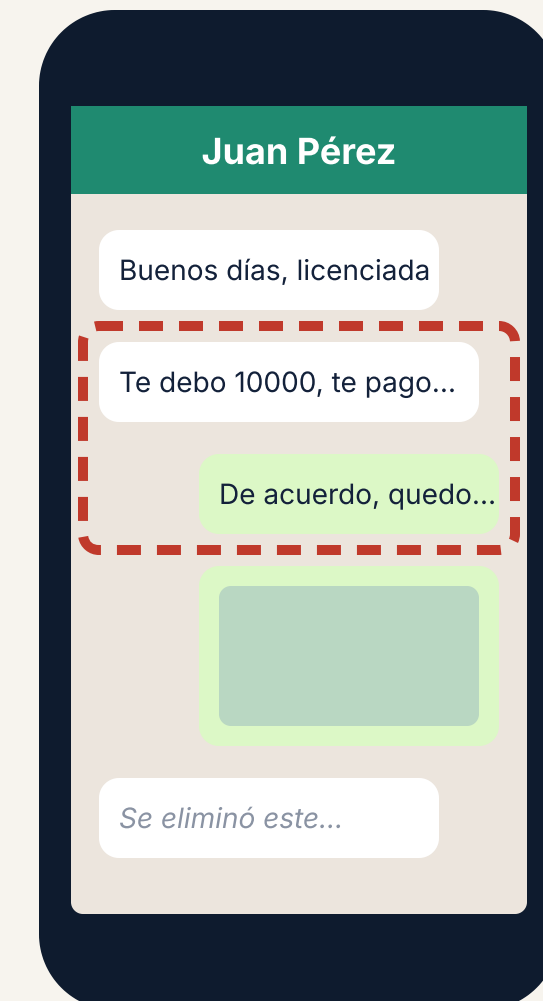
Remitente

Archivo adjunto

Eliminado / editado

Aviso del sistema

Y el archivo en sí: **nombre, tamaño, fechas del sistema**, el **.zip con la multimedia** y, sobre todo, un **hash SHA-256 calculable**.



EL PANTALLAZO

Solo un fragmento, sin fecha completa, sin archivo adjunto y sin hash.

Correo impreso **vs.** correo descargado (.eml)

Metadatos: «datos sobre los datos». Información que describe el origen, la autoría, la fecha, la ruta y las características técnicas de un archivo o mensaje, sin ser su contenido.

CORREO DE GMAIL IMPRESO

Pago pendiente

De: Juan Pérez <juan.perez@gmail.com>

Para: María López <maria.lopez@ejemplo.mx>

Fecha: 12 oct 2026, 9:15

Solo algunos metadatos: remitente, destinatario, fecha y asunto.

CORREO DESCARGADO · «MOSTRAR ORIGINAL» → .EML

```
Return-Path: <juan.perez@gmail.com>
Received: from mail-sor-f41.google.com ([203.0.113.41])
  by mx.google.com; Mon, 12 Oct 2026 08:15:23 -0700
Received: by 2002:a05:6512:xx with SMTP
Authentication-Results: mx.google.com;
  dkim=pass header.i=@gmail.com; spf=pass; dmarc=pass
DKIM-Signature: v=1; a=rsa-sha256; d=gmail.com; bh=Q2x...; b=hT9...
Message-ID: <CAF3x9kR2...@mail.gmail.com>
Date: Mon, 12 Oct 2026 09:15:22 -0600
From / To / Subject: ...
MIME-Version: 1.0 · Content-Type: multipart/alternative
```

Ruta del correo (servidores)

Autenticación SPF · DKIM · DMARC

Identificador único y hora con zona

IDEA CLAVE

Todos esos son metadatos: el impreso solo conserva algunos; el .eml los conserva todos.

El nacimiento de la prueba electrónica: del papel al comercio electrónico

A finales del siglo XX, el comercio internacional documenta acuerdos por correo e intercambio electrónico de datos. Surge la necesidad de reconocerlos como prueba, **aunque no exista papel**.



FINALIDAD

Adaptar el derecho a las operaciones sin papel.

De la Ley Modelo al Código de Comercio mexicano

2000 DOF 29-05-2000

Se incorpora el comercio electrónico

- Nace el Título Segundo, «Del Comercio Electrónico»: **arts. 89 a 94**
- **Art. 89:** define el mensaje de datos
- Además: art. 49 (conservación), 80 (contratos), 1205 (prueba) y **1298-A** (fiabilidad del método)

2003 DOF 29-08-2003

Llegan los artículos «bis» y la firma electrónica

- 89** Glosario y principios: neutralidad tecnológica, equivalencia funcional
- 89 bis** No se niegan efectos jurídicos por constar en mensaje de datos
- 93 bis** **Forma original:** garantía confiable de integridad
- 90 bis · 91 bis** Atribución y momento de envío
- 96-114** Firma electrónica avanzada (art. 97) y certificadores

ART. 89 · MENSAJE DE DATOS

«La información generada, enviada, recibida o archivada por medios electrónicos, ópticos o cualquier otra tecnología».

Es el género. Sus especies: correo electrónico, WhatsApp, SMS, redes sociales, audios, fotos, videos y PDF.

El mensaje de datos tiene **reconocimiento jurídico**

Código de Comercio

- | | |
|--------------------|---|
| 89 bis | No se niegan efectos jurídicos por ser electrónico; puede ser prueba. |
| <hr/> | |
| 90 · 90 bis | Atribución del mensaje a su emisor. |
| <hr/> | |
| 93 | Satisface las exigencias de escrito y firma. |
| <hr/> | |
| 1298-A | Se valora primordialmente la fiabilidad del método . |

CNPCF · 2023

- | | |
|------------|--|
| 308 | Mismo trato a documentales físicas y electrónicas. |
| <hr/> | |
| 348 | Prueba en medios electrónicos, ópticos, digitales, en una cadena de bloques o cualquier tecnología. |
| <hr/> | |
| 349 | Fiabilidad, atribución y accesibilidad para consulta posterior. |

OJO Reconocimiento jurídico no significa eficacia probatoria automática.

Documento impreso **vs.** documento electrónico



Impreso

- Es prueba documental
- Representa solo el contenido visible
- Omite encabezados y metadatos
- No permite verificar integridad

Contenido

Encabezados

Metadatos

Hash SHA-256

Electrónico nativo

- También es prueba documental
- Conserva origen, transmisión y contexto
- Permite cálculo de hash
- Admite examen técnico

IDEA CLAVE

La impresión puede probar; el archivo original permite verificar.

La forma original: **integridad y verificación**

ART. 93 BIS, FR. I · CÓDIGO DE COMERCIO

«...garantía confiable de que se ha conservado la integridad de la información, a partir del momento en que se generó por primera vez en su forma definitiva...»

Integridad · completa e inalterada

Accesibilidad · puede mostrarse

Confiabilidad · según el caso

Art. 49 · Código de Comercio

- El comerciante debe **conservar por al menos diez años** los originales de los documentos —incluidos los **mensajes de datos**— que generen derechos y obligaciones.
- Para conservar o presentar el original de un mensaje de datos, la información debe mantenerse **íntegra e inalterada** desde que se generó en su forma definitiva y ser **accesible** para consulta posterior.
- Remite a la **NOM-151-SCFI-2016** para los requisitos de conservación.

Art. 350 · CNPCF

- Cuando la ley exige la **forma original**, se cumple si la información se mantuvo **íntegra e inalterada** desde que se generó por primera vez en su forma definitiva...
- ... y es **accesible** para su ulterior consulta.
- La información en una **cadena de bloques pública hace prueba plena**, salvo circunstancias fehacientes de que fue vulnerada, manipulada o no es confiable.

¿Por qué el original tiene **valor probatorio superior**?

Los criterios legales de valoración **solo pueden examinarse sobre el archivo nativo.**

CRITERIO LEGAL	IMPRESIÓN	ARCHIVO NATIVO
Fiabilidad del método · 1298-A CCom / 349 CNPCF	✗	✓
Atribución al emisor · 90 bis CCom / 349 CNPCF	✗	✓
Integridad desde su forma definitiva · 93 bis CCom / 350 CNPCF	✗	✓
Accesibilidad para consulta posterior · 349-350 CNPCF	Solo como copia	✓

IDEA CLAVE

Promover el original es colocar al juez en condiciones de aplicar la ley; promover la impresión es pedirle un acto de fe.

El código hash: la huella digital del archivo



- Resumen matemático de longitud fija
- Identifica el archivo de forma prácticamente única
- **No cifra ni oculta:** sirve para comparar

UN REGISTRO DE HASH COMPLETO INDICA

- ① Archivo identificado
- ② Algoritmo
- ③ Valor hash completo
- ④ Fecha, hora y responsable

Cómo funciona: **cuatro propiedades** útiles en juicio



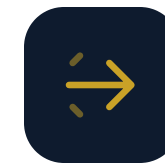
Determinista

El mismo archivo produce siempre el mismo valor.



Efecto avalancha

Una coma o un cero cambian el hash por completo.



Unidireccional

Del hash no se puede reconstruir el archivo.



Sin colisiones

Prácticamente imposible: dos archivos, un mismo hash.

256
bits

=

64
caracteres
hexadecimales

SHA-256
el estándar
recomendado

MD5 y SHA-1

Aún frecuentes en pericias, pero con vulnerabilidades conocidas: preferir SHA-256.

Ejemplo: **un solo carácter** lo cambia todo

«Te debo 10000»

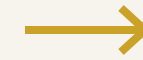
ORIGINAL



adc80fb9 747f8386 de77ada0 75834e08 cd892c16 3923ac87 a83012b8 1032a35e

«Te debo 1000»

SE BORRÓ UN CERO



bf0296d8 b01c1c43 b10bcfc6 c98831c5 52928213 37776398 6780409c 9bfe8146

«Te debo 10000.»

SE AGREGÓ UN PUNTO



2626914a 35a8922f 4dd44383 83633e6f 28500348 05d6f587 a572ac46 a9292e42

SHA-256 calculado sobre el texto exacto (UTF-8, sin salto de línea).

LECTURA

Si el hash coincide, el archivo no cambió desde el momento de su obtención. Si cambia un carácter, cambia todo.

¿Qué garantiza el hash... y qué no?

Sí garantiza

- ✓ **Integridad:** no cambió desde su obtención
- ✓ **Identidad:** es el mismo archivo preservado
- ✓ **Verificación** por juez, contraparte o perito
- ✓ **Trazabilidad** en la cadena de custodia

NO garantiza

- ✗ **Autoría:** quién escribió o envió
- ✗ **Veracidad** del contenido
- ✗ **Licitud** de la obtención
- ✗ Que no fuera falso **antes** del cálculo

ADVERTENCIA

Un archivo falso o fabricado con IA también puede conservarse íntegro.

Las normas **ISO/IEC**: el estándar internacional

Estándares elaborados por la **ISO** (Organización Internacional de Normalización) y la **IEC** (Comisión Electrotécnica Internacional). México participa en su desarrollo.

NO SON LEYES, PERO...

constituyen el **estándar de diligencia técnica** para evaluar la integridad y confiabilidad de la evidencia digital.

PRINCIPIO DE MISMIDAD

Lo que se presenta en juicio es exactamente lo que se recolectó: sin alteración de forma, contenido, metadatos ni contexto técnico.

ISO/IEC 27037:2012

ISO/IEC 27042:2015



Estas normas exigen el hash para:

- ✓ Documentar el estado original
- ✓ Comparar copias y duplicados
- ✓ Asegurar la imagen forense
- ✓ Garantizar la trazabilidad

La ISO/IEC 27042:2015: hash **antes y después** de toda intervención pericial; análisis sobre imagen forense.

El anclaje del hash en las normas mexicanas

ISO/IEC 27037 · 27042



México recoge esas prácticas en cinco instrumentos:

Norma Mexicana · voluntaria

NMX-I-289-NYCE-2016

Análisis forense digital. Su **Anexo 11**, incorporado a la Guía Nacional de Cadena de Custodia: bloqueo de escritura, imagen forense, **cálculo y registro del hash**.

NOM · obligatoria

NOM-151-SCFI-2016

Conservación de mensajes de datos: **hash certificado por un PSC**, firma electrónica avanzada y **sello digital de tiempo**.

CJF · DOF 17-06-2016

Lineamientos del CJF

Obtención y tratamiento de evidencias digitales en el PJJ: imagen forense, duplicadores con bloqueo de escritura, **hash en adquisición y análisis**.

CJF · DOF 17-06-2016

Protocolo del CJF

Copia bit a bit, **cálculo y verificación del hash** de la imagen forense, embalaje y cadena de custodia en formatos normalizados.

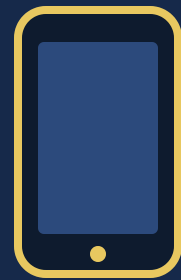
PGR · 2018

Guía Técnica de Cadena de Custodia de Evidencia Digital

SHA-256 antes y después de la imagen forense; copias maestra y de trabajo.

El hash es la **columna vertebral** de la cadena de custodia digital.

Dos objetos, **doble cadena de custodia**



EVIDENCIA ELECTRÓNICA

El dispositivo

Celular, tablet, laptop, USB, disco

CADENA DE CUSTODIA FÍSICA

Identificación (marca, modelo, IMEI)

Fotografía

Embalaje y sellado

Etiquetado

Traslado y resguardo

01001101
{chat.txt}
IMG_0003
10110010
metadata

EVIDENCIA DIGITAL

La información

Chats, fotos, audios, correos, metadatos

CADENA DE CUSTODIA DIGITAL

Exportación o imagen forense

Hash SHA-256

Copias maestra y de trabajo

Acta técnica

Verificación del hash

Referente comparado: el **Protocolo Anexo al Manual Único de Cadena de Custodia** (Venezuela, 2022) regula de forma diferenciada la adquisición de la evidencia electrónica y el examen de la evidencia digital.

IDEA CLAVE

Custodiar el teléfono no basta: también hay que custodiar, con hash, la información que contiene.

Obtención: la licitud es el primer filtro



ARTÍCULO 16 · CONSTITUCIÓN POLÍTICA DE LOS ESTADOS UNIDOS MEXICANOS

«**Las comunicaciones privadas son inviolables.** La ley sancionará penalmente cualquier acto que atente contra la libertad y privacidad de las mismas, **excepto cuando sean aportadas de forma voluntaria por alguno de los particulares que participen en ellas.** El juez valorará el alcance de éstas, siempre y cuando contengan información relacionada con la comisión de un delito. En ningún caso se admitirán comunicaciones que violen el deber de confidencialidad que establezca la ley.»

«Exclusivamente la autoridad judicial federal [...] podrá autorizar la intervención de cualquier comunicación privada. [...] no podrá otorgar estas autorizaciones cuando se trate de materias de carácter electoral, fiscal, mercantil, civil, laboral o administrativo [...]»

VÍAS LÍCITAS DE OBTENCIÓN



Participante

Quien intervino en la comunicación la aporta.



Información pública

Perfiles y publicaciones abiertas.



Autorización judicial

Para intervenir o extraer datos ajenos.

IDEA CLAVE

La prueba ilícita no se salva con un buen hash.

La preconstitución de la prueba electrónica

Asegurar la prueba **antes del proceso**, antes de que la evidencia volátil desaparezca: el mensaje se borra, la cuenta se cancela, el servidor sobrescribe.

NO ES
peritar

ES
conservar

Perú · Resolución N.º 341-2025-MP-FN: el instructivo GUFEC/INS-04 ordena a los propios **fiscales** exportar el chat de WhatsApp y consignar su hash en acta.

GUÍA DE ACTUACIÓN FASTA-UCHAMP (ARGENTINA, 2024)

① **Adquisición** · desde la fuente original



② **Preservación** · hash + acta



③ **Presentación** · al expediente

Principio: la cadena de custodia es un atributo **del procedimiento**, no del sujeto que lo realiza.

CNPP, art. 227: «La cadena de custodia es el sistema de control y registro que se aplica al indicio, evidencia, objeto, instrumento o producto del hecho delictivo, desde su localización, descubrimiento o aportación [...] hasta que la autoridad competente ordene su conclusión». Registra identidad, estado original, condiciones de recolección, preservación, empaque y traslado, y a todas las personas que tuvieron contacto con la evidencia.

“

Los letrados podrán recabar información de bases de datos públicas sobre la identidad digital de una determinada persona, certificar prueba electrónica mediante terceros de confianza, estudiar encabezados de correos electrónicos, **exportar chats de WhatsApp**, analizar el código fuente de páginas webs, entre otras tareas relativas a la investigación.

Gastón E. Bielli y Carlos J. Ordóñez, *La prueba electrónica*, La Ley, Buenos Aires, cap. 4, § 4.4. Tesis sostenida desde la 1.ª ed. (2019).

Una analogía: preconstituir una prueba física

El abogado necesita probar una nota publicada en un periódico de hace 30 años.



PRUEBA FÍSICA · EL PERIÓDICO

1

Localizar el ejemplar en la **Hemeroteca Nacional**: fecha, edición y página

2

Obtener la **reproducción** de la página por la vía institucional

3

Dar **fe pública**: fe de hechos notarial del ejemplar consultado

4

Conservar y presentar; el original queda **disponible para cotejo**

PRUEBA ELECTRÓNICA · EL CHAT

Identificar el **teléfono** y el chat donde está la evidencia

Exportar el chat en formato nativo

Hash SHA-256 + acta técnica + fecha cierta

Resguardar, promover; el teléfono queda **disponible para cotejo**

IDEA CLAVE

Lo que siempre hicimos con el papel, hoy lo hacemos con el hash.

Protocolo: preconstituir un chat de WhatsApp

1 📱

Identificar el teléfono

Marca, modelo, número, IMEI y titular. Fotografiarlo.

2 👁

Documentar el chat

Contacto, número y contexto en pantalla.

3 ✉

Exportar el chat

⋮ → Más → Exportar chat → **Incluir archivos**. Enviar a **Gmail** (preferible) o a **Google Drive** si es muy pesado.

4 📄

Descargar el .zip

En la computadora, sin abrirlo ni editarlo.

5 #

Hash del .zip

Calcular su SHA-256 de inmediato.

6 📄

Hash de cada archivo

Abrir la carpeta exportada y calcular el hash del .txt y de cada .jpg, .opus, .mp4, .pdf...

7 📁

Carpeta contenedora

Reunir archivos y hashes, comprimirla y grabarla en **CD** o **DVD**.

8 🌐

Nube + código QR

Subirla a Google Drive, obtener el enlace y generar el **código QR**.

9 ✎

Acta técnica

Todo lo anterior consta en ella: fechas, horas, pasos, hashes, enlace y responsable.

10 🔒

Conservar el teléfono

Para promover la pericia en caso de impugnación fundada de la contraparte.

IDEA CLAVE

Quien preserva no perita: conserva con un procedimiento verificable.

El acta técnica es la cadena de custodia

El acta técnica de preconstitución equivale a la cadena de custodia del **art. 227 CNPP**: el sistema de control y registro de la evidencia desde su localización, descubrimiento o aportación hasta su conclusión.



Cada eslabón queda registrado en el acta: quién, cuándo, dónde, con qué herramienta y con qué valor hash.

NO ES SOLO PARA LA MATERIA PENAL

Aplica en **toda materia** —civil, mercantil, familiar, laboral, administrativa— en que se **preconstituya** la prueba.

¿Y EL PERITO?

El peritaje será necesario **en caso de impugnación fundada** de la contraparte: el perito contrasta el hash declarado con el actual.

Cómo promover la prueba **preconstituida**

QUÉ ACOMPAÑAR AL ESCRITO



Archivos nativos

.zip · .txt · .mp4
.opus · .jpg · .pdf
.docx · .eml

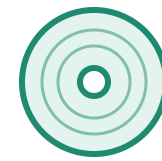
LA PRUEBA



Acta técnica

Pasos, hashes SHA-256,
enlace y responsable

LA GARANTÍA



CD o DVD

Con la carpeta contenedora
comprimida

EL SOPORTE



Código QR

Enlace a la carpeta en
Google Drive

EL ACCESO



Impresión

Solo como apoyo de
lectura

EL APOYO

SI HAY IMPUGNACIÓN FUNDADA

 Pericial: contraste del hash

 Cotejo con el teléfono

 Inspección judicial

IDEA CLAVE

La impresión acompaña; el archivo nativo prueba; el hash lo garantiza.

Chats: **licitud y cadena de custodia**



Estándar mínimo en materia penal

1

Obtención lícita

2

Cadena de custodia

Segundo Tribunal Colegiado en Materia Penal del Primer Circuito

Tesis aislada I.2o.P.49 P (10a.) · Registro 2013524

[Consultar criterio ↗](#)



Aportación por un interlocutor

En el procedimiento administrativo sancionador, el participante puede **levantar el secreto** de la conversación: la prueba es lícita.

Décimo Tribunal Colegiado en Materia Administrativa del Primer Circuito

Tesis aislada I.10o.A.53 A (11a.) · Registro 2029973

[Consultar criterio ↗](#)

IDEA CLAVE

Obtener lícitamente y demostrar que el contenido se preservó.

Teléfonos: **asegurar no equivale a extraer**



Teléfono del detenido

La extracción **sin autorización judicial** es ilícita, aunque la carpeta ya esté judicializada.

1er. T.C. en Materias Penal y Administrativa del Décimo Séptimo Circuito

XVII.1o.P.A.86 P (10a.) · Reg. 2019633

[Consultar criterio ↗](#)



Aparatos hallados en un cateo

La orden de cateo **no basta** para extraer comunicaciones privadas de los dispositivos.

1er. T.C. del Vigésimo Séptimo Circuito · CFPP abrogado

XXVII.1o.5 P (10a.) · Reg. 2016187

[Consultar criterio ↗](#)



Datos de las telefónicas

Expectativa legítima de privacidad sobre las «**sábanas de llamadas**»; se cuestiona el art. 303 CNPP.

Primera Sala de la SCJN

1a. VIII/2024 (11a.) · Reg. 2028872

[Consultar criterio ↗](#)

IDEA CLAVE

El dispositivo y sus comunicaciones tienen protecciones distintas.

Información pública y víctima menor de edad



Perfil público de Facebook

Obtener la impresión fotográfica del perfil **público** del imputado no es prueba ilícita.

Quinto Tribunal Colegiado en Materia Penal del Primer Circuito

Tesis aislada I.5o.P.42 P (10a.) · Registro 2010454

[Consultar criterio ↗](#)



Teléfono de la víctima menor

Si quien ejerce la patria potestad aporta el teléfono, equivale a que el propio menor **revele** la comunicación: la prueba es lícita.

Tercer Tribunal Colegiado del Décimo Quinto Circuito

Tesis aislada XV.3o.8 P (10a.) · Registro 2015198

[Consultar criterio ↗](#)

IDEA CLAVE

Verificar el carácter público y analizar quién revela la comunicación.

Correos electrónicos: **valoración e identidad**



Documentos en sentido amplio

Su formato electrónico no justifica descartarlos; se valoran conforme a las reglas de los mensajes de datos.

Cuarto Tribunal Colegiado en Materia Civil del Primer Circuito

Tesis aislada I.4o.C.19 C (10a.) · Registro 2002142

[Consultar criterio ↗](#)



¿Quién envió y quién recibió?

Analizar la generación y transmisión: claves, sistemas automatizados, acuerdos previos y métodos de identificación.

Segundo Tribunal Colegiado en Materia Civil del Tercer Circuito

Tesis aislada III.2o.C.46 K (10a.) · Registro 2021967

[Consultar criterio ↗](#)

IDEA CLAVE

Reconocer el correo como prueba no demuestra automáticamente su autoría.

Documento electrónico: cuándo hace prueba plena

Requiere perfeccionamiento

Eficacia probatoria plena

más verificable →

Sin firma ni sello

En el juicio laboral, la documental de sistemas de registro electrónico **no goza de valor pleno** y debe perfeccionarse.

Segundo Tribunal Colegiado en Materia de Trabajo del Séptimo Circuito

Jurisprudencia (11a.) · Registro 2023914

[Consultar criterio ↗](#)

Con cadena original, sello o firma

Eficacia **plena**: la carga de desvirtuarla pasa **a quien lo objeta**.

1er. T.C. en Materias Penal y Administrativa del Vigésimo Primer Circuito
· art. 210-A CFPC (hoy 348-350 CNPCF)

Tesis aislada XXI.1o.P.A.11 K (10a.) · Registro 2015428

[Consultar criterio ↗](#)

Principios que rigen **la validez de la evidencia digital**



Licitud

Obtenida sin violar derechos fundamentales (art. 16 CPEUM).



Mismidad

Lo que se presenta es exactamente lo que se obtuvo.



Integridad

Completa e inalterada desde su forma definitiva: el hash lo demuestra.



Autenticidad

Proviene de quien se afirma: atribución al emisor.



Trazabilidad

Cada paso documentado en la cadena de custodia.



Equivalencia funcional

El mensaje de datos vale como el escrito, la firma y el original.



Contradicción

La contraparte puede verificar el hash e impugnar.

**Lícita + nativa + hash +
cadena de custodia =
prueba sólida**

Cinco ideas **para el litigante**

- 1** El mensaje de datos es prueba desde 2000; **el pantallazo es solo su fotografía impresa.**
- 2** El valor probatorio está en la **forma original**, no en la impresión.
- 3** El hash demuestra **integridad**, no autoría.
- 4** Sin licitud ni cadena de custodia, **no hay hash que salve la prueba.**
- 5** Promueva el **archivo nativo**; la impresión, solo como apoyo.

DEMOSTRACIÓN EN VIVO

CustodIA® WhatsApp



Del chat exportado al archivo preservado



Cálculo del hash SHA-256 en pantalla



Acta técnica y escrito de promoción

Demostración con una conversación ficticia.

De la teoría a la práctica.



LIVE

Lo invito al Live de presentación de CustodIA®

Martes 20 de octubre de 2026 · 6:00 p. m. (hora de México)

En Instagram: [@joseluistamayorodriguez](#)

Corpus Iuris: IA jurídica mexicana

Plataforma de búsqueda y consulta jurídica con IA, especializada en el **derecho mexicano**.

6,710

leyes federales y estatales

311,701

tesis de la SCJN

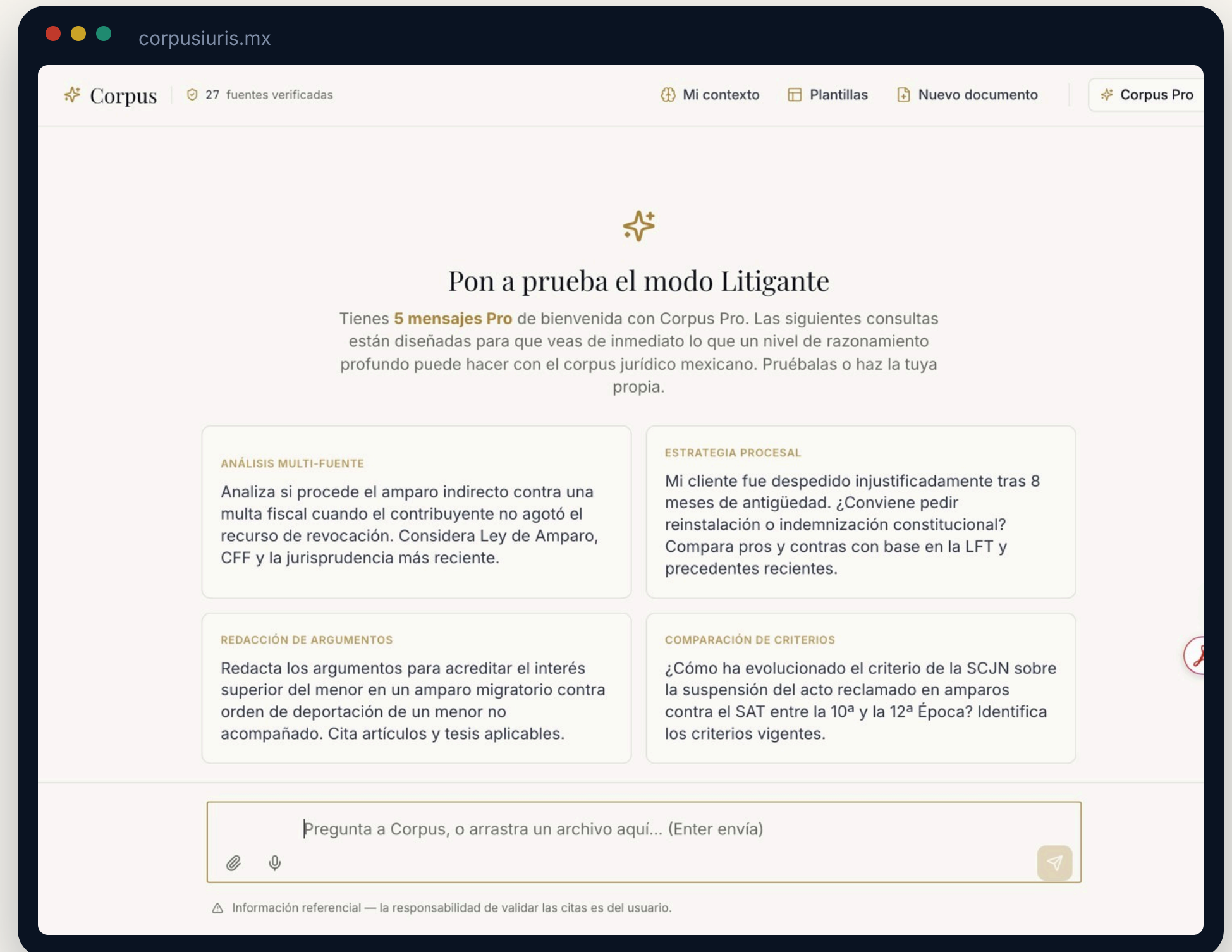
11,708

precedentes

Cifras publicadas por el sitio, octubre de 2026.

- Respuestas con cita y enlace al DOF, al Semanario Judicial o a la gaceta estatal
- Modo **Litigante**: análisis multifuente, estrategia y redacción de argumentos
- Casos, plantillas y nuevos documentos

Ojo: «Información referencial — la responsabilidad de validar las citas es del usuario».



Gracias

*El expediente ya no es solo de papel: es de datos, metadatos y algoritmos. Adaptar el litigio a la era digital y de la inteligencia artificial no es una opción tecnológica; es un **deber profesional** con nuestros clientes y con la justicia.*

Dr. José Luis Tamayo Rodríguez



digital@joseluitamayorodriguez.com



+52 442 363 0656



@joseluitamayorodriguez



facebook.com/joseluitamayor