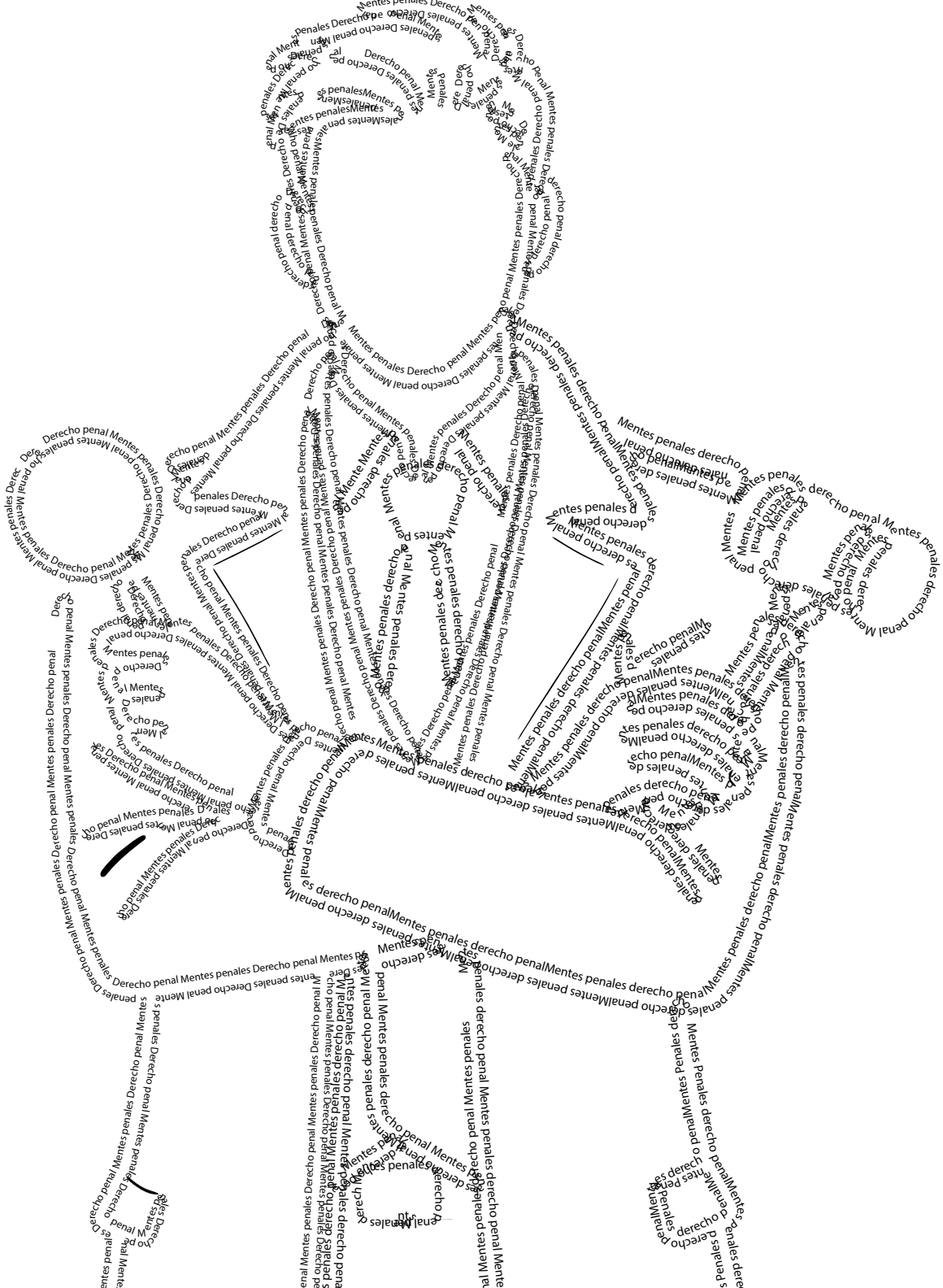
Mentes Penales

Revista de ciencias jurídico-penales

Año 9 | No. 1 | Enero-Marzo 2026



Autora invitada

Juez Lic. Liliana Martínez Sandoval

Juez de oralidad penal adscrita en Guanajuato, Guanajuato.
Licenciada en derecho por la universidad de Guanajuato

La valoración de la evidencia digital en el proceso penal acusatorio y oral

Resumen: Para que la evidencia digital cumpla con el criterio de solidez de la prueba de la fiabilidad, la persona juzgadora debe conocer las condiciones en las que se identificó, recolectó, preservó y analizó.

Palabras clave: Fuentes abiertas. Fuentes cerradas. Cadena de custodia. Valor de integridad hash.

Abstract: For digital evidence to satisfy the reliability requirement of evidentiary soundness, the judge must be informed of the conditions under which the evidence was identified, collected, preserved, and analyzed.

Keywords: Open sources, Closed sources, Chain of custody, Hash value for integrity verification.


ÚLTIMA HORA
Mallete robado justo antes de ceremonia
A pocos días del evento anual, el histórico mallete que inaugura la apertura de sesiones permanece desaparecido.
14 : 05 : 52
Cuenta regresiva para la ceremonia anual de inauguración judicial

Introducción

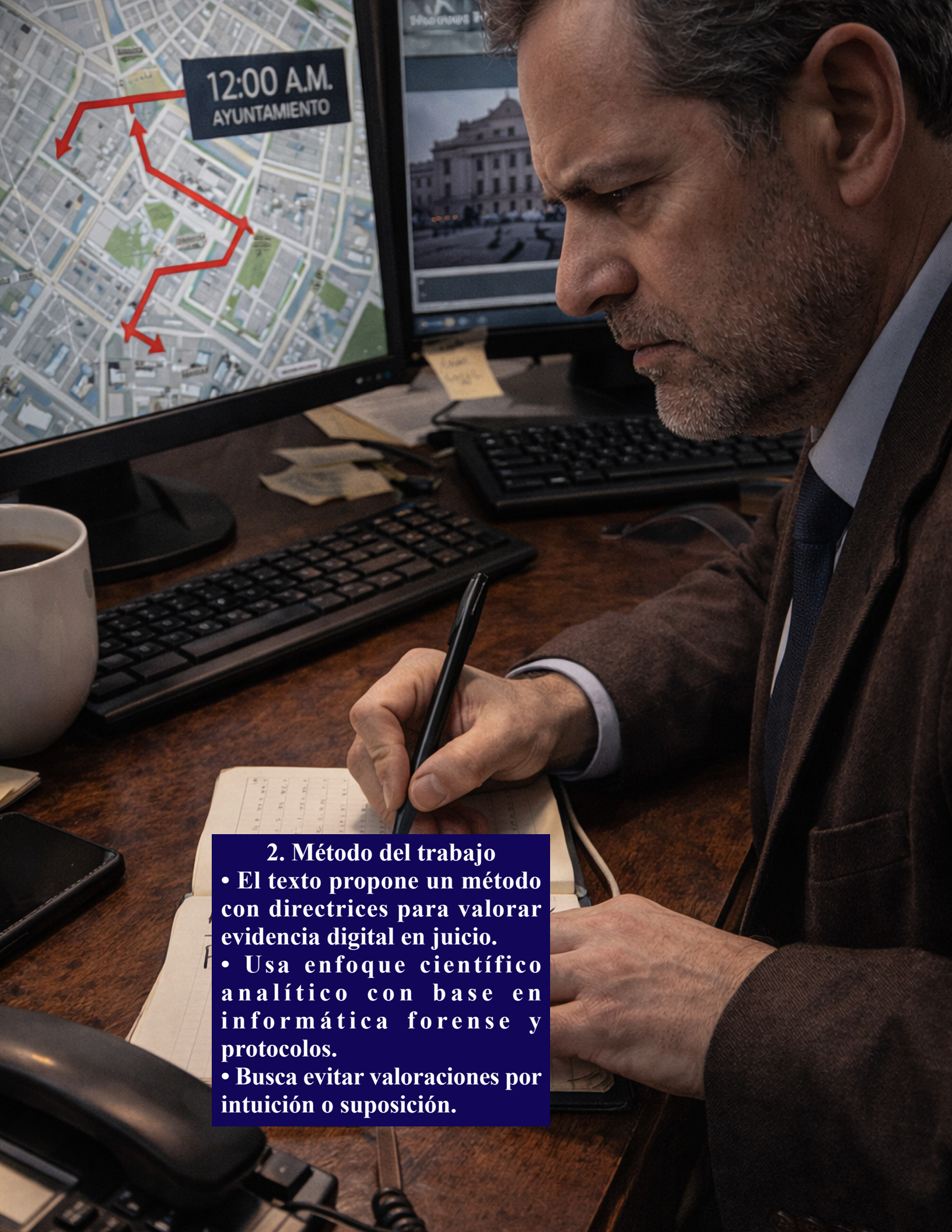
A través de este trabajo se pretende proponer un método y directrices para valorar la evidencia digital incorporada como prueba en la audiencia de juicio oral.

Para valorar esta clase de evidencia se debe conocer con precisión su identificación, recolección, preservación, análisis y presentación, con la finalidad de que los hechos que se logren reconstruir a través de estos, generen convicción firme en la persona juzgadora más allá de toda duda razonable.

En el presente trabajo se aplicó el método científico-analítico, pues a través de las diferentes fuentes consultadas sobre informática forense, protocolos para la identificación, recolección, preservación, análisis y presentación de la evidencia digital, se establece un método para que la persona juzgadora pueda valorar la evidencia digital incorporada a juicio, y a su vez, esta genere una convicción firme.

1. Tesis del texto

- **La evidencia digital solo es sólida si es fiable y el juez conoce cómo fue obtenida.**
- **Se exige claridad sobre identificación, recolección, preservación y análisis.**
- **La meta es convicción firme más allá de duda razonable.**



2. Método del trabajo

- El texto propone un método con directrices para valorar evidencia digital en juicio.
- Usa enfoque científico analítico con base en informática forense y protocolos.
- Busca evitar valoraciones por intuición o suposición.

I. La valoración de la prueba en el proceso penal acusatorio y oral en el sistema jurídico mexicano

El proceso penal acusatorio y oral, cuyos principios están desarrollados a detalle en al artículo 20, apartado A, de la constitución política de los Estados Unidos Mexicanos, contempla un sistema libre de valoración de la prueba, a través del cual, la persona juzgadora, al momento de analizar la prueba incorporada con las formalidades legales, debe exponer las razones lógicas de las máximas de la experiencia y de los conocimientos científicos que le llevan a considerar que los hechos fueron probados.

El ejercicio de valoración que realiza la persona juzgadora está constituido por el deber de motivar los hechos probados, previsto en el artículo 16 de la constitución política de los Estados Unidos Mexicanos, que delimita la actuación de la persona juzgadora al establecer el deber de exponer las razones por las cuales, un hecho o hechos, que forman parte de la tesis acusatoria, fueron o no probados.[1]

El análisis racional de la prueba debe realizarse bajo las directrices del principio de presunción de inocencia de la persona acusada, la cual constituye una regla de trato, de prueba y de juicio.

La presunción de inocencia es una regla de trato, porque la persona acusada no puede ser expuesta ante la opinión pública como persona culpable de la comisión de un delito hasta que se emita sentencia firme que declare su culpabilidad; esto tiene una razón de ser, ya que la exposición del rostro de la persona acusada en los medios de comunicación puede influir de manera negativa en el reconocimiento que realicen los testigos, impactando en la fiabilidad de un testimonio respecto a la identidad del autor o partícipe de un hecho delictivo.

La presunción de inocencia es una regla de prueba, en virtud de que corresponde a la parte acusadora probar la culpabilidad de la persona acusada a través de las pruebas lícitas que hayan sido incorporadas a la audiencia de juicio, de acuerdo con las formalidades legales.

1 Cfr. Ibáñez, Perfecto Andrés: Los hechos en la sentencia penal. Fontamara. Primera reimpresión. México, D.F. 2007. p. 43.

Luego entonces, la presunción de inocencia es una regla de juicio, ya que la persona juzgadora solo podrá tener por probado el hecho o los hechos de la acusación, cuando la prueba recibida en juicio genere convicción firme de culpabilidad y se superen las hipótesis alternativas o la duda razonable.

Lo anterior implica no solamente un análisis racional de la prueba, sino que dicho ejercicio racional debe ser acorde al estándar de prueba alto exigido por el artículo 20, apartado A, de la constitución política de los Estados Unidos Mexicanos.

El estándar probatorio exigido en la etapa de juicio oral es alto, a efectos de que se pueda enervar la presunción de inocencia de la persona acusada, lo cual impone a la parte acusadora el deber constitucional de llevar al proceso penal medios de prueba que cumplan con criterios de solidez, fiabilidad, suficiencia, variación y relevancia.

El criterio de fiabilidad de la prueba depende de cómo llegamos a conocer los hechos, e implica que la información se haya obtenido sin violación a derechos humanos, que estos hayan sido producto de conclusiones científicas o resultado de alguna inferencia lógica.

El criterio de suficiencia se actualiza cuando se cuenta con un número suficiente de hechos confirmados por otros medios de prueba, o con un solo medio de prueba con alta fiabilidad.

El criterio de variación se actualiza cuando se eliminan las hipótesis alternativas y se logra superar la duda razonable.

El criterio de relevancia se refiere a la pertinencia de la información, esto es, que los hechos se refieran de manera directa a la hipótesis acusatoria.[2]

Si la información incorporada en el juicio cumple con los anteriores criterios, es posible asumir que un hecho o hechos fueron probados, superando toda duda razonable.

2 Cfr. González Lagier Daniel: Quaestio facti. Ensayos sobre la prueba, causalidad y acción. Editorial Fontamara. México D.F. 2013. pp 51, 57-58, donde se expresa que la solidezes la propiedad de generar la convicción del Juez, y los criterios de solidez de los hechos probatorios son: a) fiabilidad y precisión, b) suficiencia, c) son variados y d) pertinencia o relevancia.

II. Concepto de evidencia digital y las fuentes que la contienen

En la práctica judicial, es común que las partes presenten medios de prueba de naturaleza digital.

Por lo tanto, es necesario definir qué se debe entender por evidencia digital, la cual es cualquier dato, registro o archivo que pueda ser generado, transmitido o almacenado por equipos de tecnología informática, los cuales están constituidos por campos magnéticos y pulsos electrónicos que pueden ser recolectados y analizados con herramientas o técnicas especiales.[3]

3. Presunción de inocencia
• Regla de trato no exhibir como culpable antes de sentencia firme.
• Regla de prueba la acusación debe probar con prueba lícita.
• Regla de juicio condena solo si se supera la duda razonable.

Las fuentes que generen las evidencias digitales pueden ser de dos tipos: a) fuentes abiertas y b) fuentes cerradas.[4]

Las fuentes abiertas son aquellos datos, registros o archivos generados con tecnología informática que pueden ser identificados en internet y que están al alcance de todo público; basta que cualquier persona visite una página web para que puedan ser observados por las personas a cargo de una investigación, sin restricción alguna.

Las fuentes cerradas son aquellos datos, registros o archivos generados con tecnología informática que pueden estar almacenados en equipos de cómputo o equipos de telefonía celular, y que no están al alcance de todo público al ser información privada o reservada de una persona; y para poder tener acceso a esta, es necesario que la persona

3 Cfr. Ministerio Público Fiscal y Ministerio de Seguridad de la República Argentina: Protocolo para la identificación, recolección, preservación, procesamiento y presentación de evidencia digital. Recurso digital disponible en https://www.fiscales.gob.ar/wp-content/uploads/2023/04/MINSEG-MPFN-Protocolo-evidencia-digital-2.pdf consultado el 6 de marzo de 2026.

4 Cfr. Oficina del Alto Comisionado de las Naciones Unidas y Centro de Derechos Humanos de la Facultad de Derecho de la Universidad de California, Berkeley: Protocolo de Berkeley sobre las investigaciones en fuentes abiertas digitales. Recurso digital disponible en https://www.ohchr.org/sites/default/files/2024-01/Berkeley-Protocol-Spanish_0.pdf consultado el 6 de marzo de 2026.

titular la aporte de manera voluntaria en la investigación, o que las personas a cargo de la investigación obtengan autorización judicial para intervenir las comunicaciones privadas o para la extracción de la información relevante, relacionada con el hecho o hechos objeto de una investigación.

5. Solidez probatoria

• Para vencer la presunción de inocencia se exige un estándar probatorio alto.

• El texto usa criterios de solidez fiabilidad, suficiencia, variación y relevancia.

• El objetivo es evitar conclusiones endebles en la sentencia.

III. La identificación, recolección, preservación, análisis y presentación de la evidencia digital en fuentes abiertas

En la etapa de investigación de un hecho probablemente delictivo, es común que las personas a cargo de una investigación acudan a fuentes abiertas para obtener información relacionada con un hecho. Dicho proceso de investigación debe cumplir con las fases o etapas siguientes:

1.- La indagación en línea, a través de la búsqueda o monitoreo de información, para el descubrimiento de información relevante.

2.- La evaluación preliminar, que se aplica en la información obtenida para evitar una recolección excesiva y cumplir con los principios de minimización de datos y de investigación específica, para lo cual se deben tomar en cuenta los factores siguientes:

A.- La pertinencia, es decir, que esté relacionado con el hecho materia de la investigación.

B.- La fiabilidad, es decir, que se debe evaluar la información contextual incluida en el archivo. Es necesario comprobar los metadatos integrados, la información vinculada y la fecha original del material.

C.- Las personas que investigan en fuentes abiertas deben evaluar si es probable que un elemento digital sea eliminado de internet o que deje de ser público, pues de ser así, se debe recolectar la información más fiable del elemento.

D.- La preservación segura de los datos.

3.- Recolección, que es el acto por el que se adquiere la información en línea, ya sea a través de captura de pantalla, conversión a PDF, descarga forense u otra forma de captura. Es recomendable que se capture la información en el momento de su recolección, lo cual resulta útil para establecer la autenticidad de un elemento digital, realizándose dicha recolección en el formato original, y si hubiera alguna alteración, transformación o conversión causada por el proceso de recolección, esta deberá documentarse. La captura de los siguientes elementos genera una base sólida de recolección:

A.- Dirección web de destino: debe dejarse constancia de la dirección web del contenido recogido.
B.- Código fuente: El código HTML de la página web, el cual contribuirá a autenticar el material recogido.
C.- Captura de página completa, indicando fecha y hora.
D.- Archivos multimedia integrados.
E.- Metadatos integrados, como identificador del usuario que subió el contenido, identificador del mensaje, la imagen o el video, la fecha y hora en que se subió el contenido, la etiqueta geográfica (geotag) y la etiqueta hashtag.

6. Evidencia digital
• Se entiende como datos o registros generados, transmitidos o almacenados digitalmente.
• Su soporte exige técnicas especiales para recolectar y analizar.
• Puede alterarse con facilidad si no se protege desde el inicio.

F.- Datos contextuales como comentarios de un mensaje, imagen o video, información sobre la subida a internet o información de la persona que lo subió a internet.
G.- Datos de recolección: nombre de la persona que lo hizo, la dirección IP de la máquina utilizada para recoger la información, la identidad virtual utilizada, y el sello de fecha y hora.
H.- Valor de direccionamiento hash, que es una forma única de identificación digital que confirma, mediante el uso de criptografía, si el contenido es auténtico o ha sido modificado. En el momento de la recolección se debe añadir el valor de direccionamiento.

4.- Preservación, la cual es indispensable para que el material digital sea utilizable a corto y a largo plazo. Las propiedades de un elemento digital que deben preservarse a largo plazo son:
A.- Autenticidad: es la capacidad de demostrar que un material digital sigue siendo el mismo que cuando se recogió.
B.- Disponibilidad: el hecho de seguir existiendo y ser recuperable.
C.- Identidad: el material debe ser identificable y distinguirse de otros, por ejemplo, al aplicarle un identificador.

D.- Persistencia: se refiere a su integridad y viabilidad, esto es, las secuencias de bits deben estar intactas, ser procesables y recuperables.

E.- Representabilidad: se refiere a la interacción entre el elemento digital y el hardware y software adecuados.

F.- Comprensibilidad: se refiere a la cualidad de ser interpretado y comprendido por los usuarios.

Los problemas específicos que se pueden presentar durante el proceso de preservación son los siguientes:

7. Fuentes abiertas y fuentes cerradas

• Fuentes abiertas son contenidos públicos disponibles en internet.

• Fuentes cerradas son datos privados en dispositivos o cuentas no públicas.

• La diferencia importa por el acceso permitido y por las exigencias legales.

A.- La cadena de custodia: se refiere a la documentación cronológica de la secuencia de custodios de un material. Una vez recogido un elemento digital, la cadena de custodia debe mantenerse, implementando un sistema de preservación digital adecuado.

B.- Copia probatoria: es un material digital recogido en la investigación en su forma original que no debe alterarse o modificarse.

C.- Copias de trabajo: se deben crear una o varias copias del material digital con el objeto de analizarlo y almacenarlo por separado.

D.- Almacenamiento: ayuda a garantizar la persistencia de los elementos digitales. La información digital puede almacenarse en línea o por ejemplo en un disco duro local o soporte local extraíble, en una unidad en red que forme parte de una red de área local, un servidor remoto o un sistema de almacenamiento en la nube.

5.- Verificación: es el proceso por el cual se establece la exactitud o validez de la información que ha sido recogida en línea. A través de un análisis técnico de un elemento digital se puede comprobar su integridad a través de un examen forense digital, el cual se integra de los componentes siguientes:

A.- Metadatos: son datos que describen y dan información sobre otros datos. Pueden ser creados por el usuario que generó dicho elemento, por otros usuarios, por un proveedor de servicios de comunicación o por cualquier dispositivo en que se crean, transfieren, reciben o ven datos.

B.- Datos de formato de archivo de imágenes intercambiables: es un tipo de metadatos que especifica los formatos de las imágenes, el sonido y las etiquetas auxiliares que utilizan las cámaras digitales, los escáneres y otros sistemas que manejan archivos audiovisuales grabados por cámaras digitales.

C.- El código fuente: es el código de programación que existe en cualquier página web o software.

8. Fases en fuentes abiertas

- **Indagación en línea para localizar información relevante.**
- **Evaluación preliminar para filtrar lo pertinente y valorar riesgos de desaparición o cambio.**
- **Recolección y preservación con documentación del proceso de captura.**

También se puede verificar la exactitud de una información digital a través de un análisis de contenido, a través del cual se evalúa la autenticidad y veracidad de un video, imagen o documento por medio de identificadores únicos, por ejemplo: edificios, flora, fauna, personas, símbolos o insignias, por medio de información objetivamente verificable y a través de la geolocalización, osea, a través de la ubicación de un objeto, una actividad o el lugar desde el que se generó un material digital, esto permite conocer la ubicación desde la que tomó un video o una fotografía.

Los resultados de una investigación en fuentes abiertas pueden presentarse de forma oral, visual o escrita.[5]

5 Cfr. Oficina del Alto Comisionado de las Naciones Unidas y Centro de Derechos Humanos de la Facultad de Derecho de la Universidad de California, Berkeley: Protocolo de Berkeley sobre las investigaciones en fuentes abiertas digitales. Recurso digital disponible en https://www.ohchr.org/sites/default/files/2024-01/Berkeley-Protocol-Spanish_0.pdf consultado el 6 de marzo de 2026.

IV. Identificación, recolección, preservación, análisis y presentación de información digital en fuentes cerradas

Recordemos que la información digital que no está disponible al público en línea, se considera que es reservada, y para que esta pueda ser identificada, recolectada, preservada, analizada y presentada en una investigación, es necesario que la persona titular de esa información la aporte voluntariamente a la investigación, y en caso de que esto no suceda, el servidor público a cargo de la investigación debe obtener la autorización del órgano jurisdiccional competente para tener acceso a esas comunicaciones, tal como lo establece el artículo 16 de la constitución política de los Estados Unidos Mexicanos.

9. Contenido mínimo de una recolección sólida

- **Conservar la ubicación de origen del contenido y su contexto de publicación.**
- **Incorporar información técnica disponible y elementos que permitan verificación posterior.**
- **Registrar datos de quien recolecta y el momento de la recolección.**

En caso de que lo anterior se cumpla, las personas encargadas de la investigación informática deberán realizar:

1.- Identificación: al conocer los detalles del caso, el analista decide qué equipos tecnológicos formarán parte de una investigación, qué instancias de la nube serán requeridas, qué servidores serán solicitados, o si se van a llevar o no un router para analizarlo. Esta parte es delicada, ya que será el analista el que indicará qué se analiza y qué puede ser excluido.

2.- Recolección de evidencia: Durante este proceso de obtención de la información es recomendable llevar un formato para llenar los aspectos más importantes de la investigación; además, se deben tomar imágenes fotográficas del lugar y de los equipos de cómputo, tomar los generales de la persona que pone a la vista el equipo de cómputo, la hora en que se tuvo a la vista el equipo de cómputo, así como la hora en que el personal mostró dicho equipo

informático. Las herramientas para la recolección de evidencia informática son los discos duros y memorias USB limpias o formateadas.

3.- La preservación es el punto toral de una investigación cuyo resultado se presentará ante una autoridad, siendo la cadena de custodia la que permite darle trazabilidad a cada uno de los elementos digitales. En el campo de la informática, la cadena de custodia registra desde que un archivo fue extraído de un equipo de cómputo, pasando por validar la integridad del mismo, dando una certeza científica que permite comprobar que el archivo continúa íntegro tal y como fue extraído desde su inicio. Esa cadena de custodia en la rama informática es el valor de integridad hash.

El valor de integridad hash funge como un número de serie que está asociado a un elemento digital, pudiendo ser un archivo en formato word, excel, power point, una imagen fotográfica, un video, audio, pdf, o un archivo html.

4.- Análisis para conocer qué herramientas se deben usar y cómo se deben emplear.

5.- Presentación de resultados a través de un dictamen pericial, en donde se darán a conocer las conclusiones que obtuvieron del análisis forense de los elementos digitales obtenidos en una investigación.[6]

Hoy en día es común que en las investigaciones de naturaleza penal, las partes que intervienen en una comunicación privada aporten capturas de pantalla de mensajes escritos, o incluso de impresiones de esos mensajes, pero cabe destacar que esta información no es fiable en virtud de la falta de garantías de que la información sea auténtica; pues en esos supuestos es el perito en informática forense quien debe recolectar dicha información del dispositivo que la contiene, con la anuencia del titular de dicha comunicación o con autorización del órgano jurisdiccional competente, a través del método siguiente:

6 Cfr. Laguna Romero, Alejandro Jocsan Fundamentos de la Informática Forense. Río Subterráneo Editores. México. 2022. Recurso digital disponible en https://play.google.com/store/books/details?id=MN2pEQAAQBAJ&pli=1 consultado el 6 de marzo de 2026.

1.- Aislar el dispositivo móvil e impedir su conexión a la red móvil de telefonía o wifi para evitar su alteración o borrado remoto.
2.- Documentar el proceso realizado, en virtud de que los dispositivos móviles registran todas las interacciones realizadas, y por lo tanto, al momento de practicarse en el laboratorio la obtención de datos, el equipo especializado reportará los mismos.
3.- El primer interviniente, al observar si el dispositivo se encuentra encendido, no debe apagarlo, procurando realizar los procedimientos recomendados para garantizar la preservación y la correcta identificación de los elementos detallados a continuación:

10. Preservación y cadena de custodia

• Preservar significa mantener autenticidad, disponibilidad, identidad y persistencia del material.

• La cadena de custodia documenta quién tuvo control del material y qué se hizo con él.

• Se distingue entre copia probatoria que no se altera y copias de trabajo para análisis.

A.- Realizar la extracción de la tarjeta SIM para prevenir el acceso o modificación remota a través de la red de telefonía celular (3G, 4G y 5G).
B.- Registrar la numeración y logo en el exterior de la tarjeta SIM.
C.- Registrar el slot, o espacio físico donde se coloca la tarjeta SIM.
D.- Adherir la tarjeta SIM con cinta transparente a la carcasa del equipo.
E.- De ser posible identificar, el IME del dispositivo telefónico.
F.- Activar el modo avión del dispositivo.
G.- Desactivar la opción de wifi.
H.- Identificar y registrar la marca del dispositivo.
I.- Identificar y registrar modelo técnico.
J.- Identificar el número de serie. En caso de no observarse, por ningún motivo se deberá manipular el equipo con la intención de obtener el número de serie.
K.- De existir tarjeta o memoria, consignar el tipo, capacidad o inscripción observada.

L.- Registrar el estado de conservación a simple vista del dispositivo, incluyendo detalles.
M.- Colocar el dispositivo en una bolsa de Fadaray.
N.- Se procurará mantener el dispositivo encendido, manteniendo la carga del mismo conectándolo a una batería portátil utilizando el método de aislamiento electromagnético, para su remisión al laboratorio evitando que se apague.
Ñ.- El examen deberá realizarse por personal especialista, usando las funciones propias del dispositivo. Las interacciones quedarán registradas en el dispositivo, teniendo además que documentarse.[7]

10. Fuentes cerradas y extracción forense

• La obtención de datos privados puede requerir consentimiento del titular o autorización judicial.
• La recolección debe ser documentada con cuidado del dispositivo y del procedimiento.
• El análisis debe realizarlo personal especializado con método y herramientas adecuadas.

7 Cfr. Ministerio Público Fiscal y Ministerio de Seguridad de la República Argentina: Protocolo para la identificación, recolección, preservación, procesamiento y presentación de evidencia digital. Recurso digital disponible en https://www.fiscales.gob.ar/wp-content/uploads/2023/04/MINSEG-MPFN-Protocolo-evidencia-digital-2.pdf consultado el 6 de marzo de 2026.

V. Criterios de solidez que debe reunir la evidencia digital incorporada al juicio oral, para generar convicción firme, en la persona juzgadora

La persona juzgadora, al momento de realizar el ejercicio racional de la valoración de la evidencia digital que se incorpora a un juicio, debe verificar la fiabilidad o credibilidad de dicha evidencia.

El primer elemento que debe analizarse es conocer la fuente de origen de la información para poder establecer si proviene de una fuente abierta o de una fuente cerrada.

En caso de que esta tenga su origen en una fuente abierta, no sería necesario que la o las personas a cargo de una investigación hayan obtenido autorización de la autoridad judicial competente para la intervención de la comunicación, porque la misma fue obtenida en internet, y por ende, está disponible al público.

En el supuesto de que esta tenga su origen en equipos de cómputo o teléfonos celulares que hayan sido asegurados en el marco de una investigación, debe analizarse que la obtención de esa información privada o reservada no se haya realizado con violación a la privacidad del domicilio, a la privacidad de las comunicaciones o a la libertad de la persona acusada.

En el caso de fuentes cerradas, se deben analizar las condiciones o circunstancias bajo las cuales se realizó el secuestro o aseguramiento de un equipo de cómputo, de un dispositivo móvil o de cualquier otro dispositivo que contenga almacenada información digital. Si dichos aparatos se localizaron en un lugar cerrado, debieron contar con la autorización judicial para ingresar al domicilio, o estar en alguno de los supuestos de excepción previstos por el artículo 290 del código nacional de procedimientos penales, para que el aseguramiento sea válido.

En caso de que el aseguramiento de un dispositivo que contenga información digital almacenada se haya realizado en lugar abierto, al momento de la detención de la persona acusada, debe analizarse que la detención se haya realizado de acuerdo a los parámetros

establecidos por el artículo 16 de la constitución política de los Estados Unidos Mexicanos en los supuestos de flagrancia o urgencia, también regulados en los preceptos 146 y 150 del código nacional de procedimientos penales, de ser dicha detención apegada a derecho, el aseguramiento del dispositivo también será válido.

Una vez que se verificó la legalidad del aseguramiento, se debe verificar la autenticidad de los elementos digitales obtenidos en la investigación, para lo cual se debe analizar que los medios de almacenamiento que contienen dicha información cuenten con cadena de custodia en donde se lleve un registro o control respecto al tipo de dispositivo, señalando características como la marca visible, color, modelo visible, número de serie, lugar del aseguramiento, fecha y hora del aseguramiento, la identidad de la persona o de las personas a quien o a quienes se les aseguró dicho objeto de almacenamiento, así como los datos de la persona o personas que ejecutaron el aseguramiento, de manera tal que si se cumplió con lo anterior, se puede llegar a conocer la fuente de origen de esa información, y eventualmente, a quien pertenece.

La persona juzgadora, después de verificar la fuente de origen de la evidencia digital, debe analizar la regularidad de los demás registros o eslabones de la cadena de custodia de la evidencia material, a efecto de conocer la identidad de las personas que tuvieron contacto con dicha evidencia en su traslado y resguardo, así como el nombre de las personas especialistas en informática que examinaron la evidencia digital. De confirmarse la regularidad en los registros de la cadena de custodia, se puede llegar a sostener que la información digital fue recolectada del dispositivo asegurado.

La persona juzgadora, para verificar que los elementos digitales que fueron presentados en juicio son auténticos y que no tuvieron modificación alguna, debe analizar que las personas que ejecutaron el aseguramiento del dispositivo o medio de almacenamiento lo hayan realizado conforme a los manuales de cadena de custodia emitidos por las instituciones de seguridad pública y de procuración de justicia; de cumplirse con lo anterior, se tendría un indicio de autenticidad de los archivos digitales presentados en juicio.

Después de confirmarse la regularidad del aseguramiento de la evidencia digital, se debe verificar que la persona o personas que realizaron la identificación, recolección, preservación y análisis de los elementos digitales sean especialistas en informática forense o que tengan la capacitación y experiencia suficiente como para permitir conocer el método que emplearon en dichas actividades de investigación, las herramientas informáticas idóneas que utilizaron para realizar copias forenses de esos archivos, y a su vez, que garanticen la preservación de esos archivos en su estado original, a través del algoritmo o valor de integridad hash, siendo este criterio matemático el que permite conocer con certeza si los metadatos que contiene un archivo digital fueron o no modificados.

De cumplirse con los parámetros anteriores, se puede asumir que la evidencia digital proveniente de las fuentes cerradas es sólida, y por lo tanto, fiable.

En el caso de la evidencia digital proveniente de fuentes abiertas no será necesario que se acuda ante una autoridad judicial para obtener algún tipo de autorización, porque se trata de información pública; pero ante estos supuestos, debe ser una persona especialista en informática forense quien realice la identificación del archivo en línea, del cual se deberá dejar un registro de la localización de esa información a través de las herramientas informáticas idóneas que permitan conocer la página o la plataforma en que fue hallado el archivo.

La recolección y preservación del archivo procedente de fuentes abiertas debe precisarse con la cadena de custodia a través de la utilización de medios de almacenamiento idóneos, así como a través del análisis forense informático para que se pueda conocer la autenticidad de la información, incluyéndolo con el valor de integridad hash.

De cumplirse con lo anterior, se podrá asumir que la evidencia digital es sólida y por lo tanto, confiable.


CAM01 SALA SUR
00:18:45
CAM02 SALA S
VIGILANCIA

Conclusiones

La evidencia digital incorporada en juicio oral, para que cumpla con los criterios de solidez y de fiabilidad, debe ser sometida a un estricto escrutinio por la persona juzgadora a efecto de descartar que esta se haya obtenido por medio de la violación de algún derecho, y para conocer la autenticidad de dicha evidencia digital.

Lo anterior hace necesario que en las investigaciones donde se obtenga o se cuente con evidencia digital, dicha información debe ser identificada, recolectada, preservada y procesada por personas especialistas en informática forense que permitan conocer cuando un elemento digital es auténtico u original, o cuando este ha sido alterado o editado.

Las investigaciones que cuenten con evidencia digital no solo deben esclarecer la originalidad de esa información a través de los especialistas en informática forense, sino que también deben esclarecer la identidad del autor de esos archivos, la identidad del dispositivo de origen y el lugar en donde fueron emitidos o transmitidos a través de la geolocalización.

Por lo tanto, si la evidencia digital cumple con lo anterior, se cumplió con el criterio de solidez y fiabilidad de la prueba.

11. Valoración judicial final

• Primero se revisa la legalidad de obtención y el tipo de fuente de la evidencia.

• Luego se evalúa autenticidad e integridad con cadena de custodia y verificación técnica.

• Al final se decide el peso probatorio según fiabilidad, suficiencia, variación y relevancia.

Bibliografía

González Lagier Daniel: Quaestio facti. Ensayos sobre la prueba, causalidad y acción. Editorial Fontamara. México D.F. 2013. pp 51, 57-58, donde se expresa que la solidezes la propiedad de generar la convicción del Juez, y los criterios de solidez de los hechos probatorios son: a) fiabilidad y precisión, b) suficiencia, c) son variados y d) pertinencia o relevancia.

Ibáñez, Perfecto Andrés: Los hechos en la sentencia penal. Fontamara. Primera reimpresión. México, D.F. 2007. p. 43.

Laguna Romero, Alejandro Jocsan: Fundamentos de la Informática Forense. Río Subterráneo Editores. México. 2022. Recurso digital disponible en https://play.google.com/store/books/details?id=MN2pEQAAQBAJ&pli=1 consultado el 6 de marzo de 2026.

Ministerio Público Fiscal y Ministerio de Seguridad de la República Argentina: Protocolo para la identificación, recolección, preservación, procesamiento y presentación de evidencia digital. Recurso digital disponible en https://www.fiscales.gob.ar/wp-content/uploads/2023/04/MINSEG-MPFN-Protocolo-evidencia-digital-2.pdf consultado el 6 de marzo de 2026.

Oficina del Alto Comisionado de las Naciones Unidas y Centro de Derechos Humanos de la Facultad de Derecho de la Universidad de California, Berkeley: Protocolo de Berkeley sobre las investigaciones en fuentes abiertas digitales. Recurso digital disponible en https://www.ohchr.org/sites/default/files/2024-01/Berkeley-Protocol-Spanish_0.pdf consultado el 6 de marzo de 2026.


12.00 AM
Ayuntamiento
Audaz Robo del Mallete

Cómo citar esta obra:

Martínez Sandoval, Liliana: La valoración de la evidencia digital en el proceso penal acusatorio y oral, en Mentes Penales. Año 9 | No. 1 | Enero-Marzo 2026. Gilberto Martiñón Cano (Director). Rafael Rosado Cabrera (Coordinador). Editorial Poder Judicial del estado de Guanajuato. Guanajuato, México. 2026. p (pp.)...