
Detalles sobre la publicación, incluyendo instrucciones para autores e información para los usuarios en: https://desafiosjuridicos.uanl.mx/index.php/ds

**Armando Valencia Álvarez** (Instituto de Investigaciones Jurídicas, Universidad Veracruzana)

**Las pruebas digitales o electrónicas y sus desafíos jurídicos actuales.** pp. 56-73 Fecha de publicación en línea: 31 de enero del 2022.

Publicado en *Desafíos Jurídicos La Conjugación del Derecho*. 

Desafíos Jurídicos La Conjugación del Derecho. Revista de temas contemporáneos sobre derecho, y sus conexiones en la vida cotidiana, Volumen 1, No. 1, julio-diciembre de 2021, es una publicación semestral de la Universidad Autónoma de Nuevo León, a través de la Facultad de Derecho y Criminología, editada en la Ciudad Universitaria, N.L, México. Con dirección en Cd. Universitaria, Av. De los Rectores s/n, San Nicolás de los Garza, N.L. C.P. 66451, Página electrónica de la revista: https://desafiosjuridicos.uanl.mx/index.php/ds

Editora en jefe: Dra. Amalia Guillén Gaytán Reserva de Derechos al Uso Exclusivo del Título Volumen 1, No. 1, juliodiciembre de 2021 ISSN: en trámite ante el Instituto Nacional del Derecho de Autor. Responsable de la última actualización de este número: Dra. Karina Soto Canales.

Desafíos Jurídicos La Conjugación del Derecho aborda temas contemporáneos sobre derecho, y sus conexiones en la vida cotidiana, tiene como propósito constituirse en un foro de discusión académica que aborda la compleja, contradictoria y multicausal relación entre el derecho y la vida social. Desafíos Jurídicos se inscribe en el debate académico nacional e internacional en el ámbito de Derecho y su giro especial en las ciencias sociales e invita al análisis de diversas prácticas sociales y formas de organización y acción política desde una perspectiva multidisciplinaria que ponga énfasis en la defensa de los derechos y su aplicación. Los textos publicados incorporan métodos y problemas tratados desde el derecho, la sociología, la ciencia política, la economía, los estudios urbanos, la geografía, los estudios culturales, la antropología, la literatura y el feminismo, entre otros. Las opiniones expresadas
por los autores no reflejan la postura del comité editorial.





**PINTURA DE LA PORTADA:** M.A. Daniel Vázquez Azamar "**En la otra ventanilla**" © 2022

# Las pruebas digitales o electrónicas y sus desafíos jurídicos actuales

## Digital or Electronic Evidence and Your Current Legal Challenges

Fecha de publicación en línea: 31 de enero del 2022

**Por:** Armando Valencia Álvarez[1]

*https://orcid.org/0000-0001-5380-0245
Universidad Veracruzana

**Resumen**. El siguiente artículo nos brinda un panorama general de los errores más comunes en la recolección de las evidencias relativas a las pruebas digitales o electrónicas. Abordado de una forma amena y coloquial despojando en la medida de lo posible los tecnicismo empleados en la jerga de la informática forense; con el objetivo de que el lector pueda ahondar de una forma concisa y práctica los problemas aquí planteados hilvanados con reflexiones jurídicas y técnicas; buscando en todo momento robustecer los conocimientos respecto de los criterios mínimos que se deben atender en el manejo de la evidencia digital o electrónica, para su optima aportación a los procesos jurisdiccionales o extrajudiciales.

**Palabras clave:** Cadena de custodia; evidencia; prueba; fotograma; evidencia digital; enraizado; privilegios de administrador; Firma digital..

**Abstract.** The following article gives us an overview of the most common errors in collecting evidence for digital or electronic evidence. Approached in an entertaining and colloquial way, stripping as far as possible the technicalities used in the jargon of computer forensics; With the objective that the reader can delve in a concise and practical way the problems raised here, stitched together with legal and technical reflections; seeking at all times to strengthen knowledge regarding the minimum criteria that must be met in the management of digital or electronic evidence, for its optimal contribution to jurisdictional or extrajudicial processes.

**Keywords:** Chain of custody; evidence; proof; root; hash; jailbreak; Frames; administrative Privileges..

1 Universidad Veracruzana; Doctorado en Derecho por el Instituto de Investigaciones Jurídicas de la Universidad Veracruzana, Perito certificado por DURIVA y UNICOLOMBIA; TICS e Informática Forense; arvaal@hotmail.com

## INTRODUCCIÓN

A pesar de los múltiples avances tecnológicos de la actualidad, la recolección, manejo y resguardo de evidencia relativa a las pruebas electrónicas o digitales sigue siendo una problemática latente en los diversos procesos jurisdiccionales, de modo tal, que la posibilidad de que evidencia de esta naturaleza trascienda a prueba, se ve reducida al mínimo. De ahí la inquietud de dar a conocer los aspectos básicos que los litigantes así como operadores del Derecho en general (Fiscales, Jueces, Magistrados, etc.) deben conocer respecto de la recolección, manejo y resguardo de este tipo de evidencia.

Lo anterior con dos finalidades, una que desde el punto en que se litigue u opere, se logre ofrecer la evidencia lo mejor posible para que esta sea calificada como prueba y se le otorgue el valor de convicción; en un segundo momento para permitirnos vislumbrar qué tan lejos puede llegar nuestra evidencia, y de ser el caso, optar por alguna forma anticipada del procedimiento, al conocer la debilidad de nuestra evidencia o prueba.

En este contexto, el presente artículo parte de la ilustración práctica de los aspectos mínimos a tomar en cuenta al momento de manejar las pruebas electrónicas o digitales, en los medios de almacenamiento más comunes en el mercado; posteriormente se realiza un análisis a diversas tesis emitidas por la Suprema Corte de Justicia de la Nación, respecto del valor a las pruebas electrónicas o digitales.

## LAS PRUEBAS ELECTRÓNICAS O DIGITALES.

Las pruebas[1] físicas son aquellas que podemos tocar, oler, degustar, oír y observar, sin embargo, son estas dos últimas características las que de forma recurrente están presentes tanto en las pruebas físicas como en las electrónicas o digitales; cabe agregar que, actualmente se encuentra en desarrollo tecnología para poder transmitir mediante la red formas del cuerpo replicadas[2], lo que en un futuro no muy distante hará posible el tacto de manera remota.

En la actualidad a pesar de los múltiples avances tecnológicos en todos los campos de la vida cotidiana, continua latente la problemática en la recolección y manejo de la evidencia, así, en elementos como la sangre, semen, ca-

1 "Quadri ya ha sostenido que la prueba es un medio de verificación de las proposiciones que los litigantes formulan en juicio o, en el caso en que la ley lo autoriza (ej. arts. 163, inc. 6°, p.2 Cód. Proc. Civ. y Com.; arts. 200 y 201, Cód. Proc. Civ. Córdoba), de acreditación de los hechos conducentes para solución del litigio; mientras tanto, si pasamos a su análisis en el marco de un proceso concreto, prueba será---vista desde el enfoque del resultado---todo motivo o razón aportados al proceso para llevar al juez el convencimiento o la certeza sobre los hechos. Probar será, entonces, la acción de aportar tales razones y motivos, en orden a dejar verificada alguna de las proposiciones formuladas en juicio; y la actividad probatoria será aquella encaminada a probar (por cierto, con un resultado contingente, pues podrá ---o no---lograr su objetivo)" Quadri, G,H, La prueba en el proceso civil comercial, Abeledo-Perrot, Buenos Aires, 2011 T.1, p.1109

2 Disponible en: https://www.antena3.com/noticias/economia/sensacion-tocar-objetos-personas-distancia_20150501571df6d66584a8abb5822ff1.html

bello y huellas dactilares, que por sí mismos, son sensibles a los agentes externos como el medio ambiente, son fáciles de contaminar o perder por el mal manejo que se le proporciona o inclusive por la acción del ser humano tratando de borrar sus actos valiéndose de químicos u otros agentes. Sin embargo, la problemática es aún más grande cuando hablamos de la recolección, manejo y preservación de evidencias digitales o informáticas, cuya manipulación pasa inadvertida para personas no especializadas en la materia.

Así como las pruebas físicas necesitan ciertos elementos para su recolección, manejo y conservación, las pruebas electrónicas o digitales dependiendo del medio en que se encuentren (Memoria USB[3], Computadoras, DVD[4], DVR[5], Disco duro, Teléfonos celulares, etc.) también necesitan determinados cuidados para su recolección, manejo y conservación. A continuación, se expone un cuadro en donde se detallan los cuidados mínimos a tomar en cuenta al momento de manejar las pruebas electrónicas o digitales, en los medios de almacenamiento más comunes en el mercado, como lo son las Memoria USB, Disco duro externo, DVD, CD, Computadoras, Teléfonos celulares y DVR.

3 "USB" responde a las siglas *Universal Serial Bus* y hace referencia a un protocolo de conexión que permite enlazar diversos periféricos a un dispositivo electrónico (frecuentemente, un ordenador) para el intercambio de datos, el desarrollo de operaciones y, en algunos casos, la carga de la batería del dispositivo o dispositivos conectados. Es, por tanto, básicamente, un puerto que funciona de toma de conexión entre diferentes aparatos. Disponible en: https://softwarelab.org/es/usb/

4 Por sus siglas en inglés *Digital Versatile disc.* (Disco versátil digital) Disco que posee gran capacidad de almacenamiento. Lira, Arteaga, *Cibercriminalidad fundamentos de investigación en México,* 3ed., 2018, p.553.

5 DVR o Digital Video Recorder: Se conecta a cámaras analógicas que le envían una señal de video que digitaliza. Es lo más económico y se pueden encontrar cámaras de calidad (960H y 1000 líneas de resolución) por precios muy buenos. Han evolucionado tanto que se pueden conectar a alarmas, con protocolo RTSP e incluso gran calidad en streaming, entre otros. Se usa un cable RG59 para instalar, aunque se puede usar "UTP" con transceptores de vídeo. Disponible en:https://www.camarasdevigilanciabarcelona.com/noticias/sabes-cual-es-la-diferencia-entre-dvr-nvr-y-ndvr/index.html

| Medio de almacenamiento | Recolección, Transporte | Preservación | Copia de dispositivo |
|---|---|---|---|
| **Indicaciones generales mínimas no límitativas, cambian de acuerdo al caso** | | | |
| **Memoria USB/ Disco duro externo** | Para la recolección:<br>• Tomar fotografías del dispositivo;<br>• Mencionar sus características;<br>• Realizar un croquis del lugar del hallazgo.<br>Para el resguardo y transporte:<br>• Bolsa antiestática o papel aluminio;<br>• Caja anti golpes para el Disco duro externo ó mínimo bien acojinada de cartón.<br>• Evitar golpes. | • Tener en un lugar sin humedad;<br>• No exponerlos a los cambios bruscos de temperatura;<br>• No almacenarlos o manipularlos cerca de campos electromagnéticos;<br>• Evitar golpes. | • Usar bloqueador de escritura;<br>• Copia con programas forenses especializados;<br>• Realizar el hash o huella digital del USB o disco. |

| | | | |
|---|---|---|---|
| **DVD/CD** | Para la recolección:<br>• Tomar fotografías del dispositivo en el lugar donde se encontró;<br>• Sí el medio DVD o CD tiene número de serie hacerlo constar.<br>Para el resguardo y transporte:<br>• Cajas plásticas adecuadas para resguardar el medio o en su defecto bolsas de papel especiales para guardar DVD o CD;<br>• Sellado y lacrado en el lugar del hallazgo, de preferencia realizar ahí mismo el copiado. | • Tener en un lugar sin humedad;<br>• No exponerlos a los cambios bruscos de temperatura;<br>• No exponerse al sol directo;<br>• Evitar ralladuras;<br>• No exponer a solventes agresivos que afecten el medio de almacenamiento. | • Copia con programas forenses especializados;<br>• Realizar el hash[6] o huella digital del contenido del DVD o CD. |
| **Computadoras (Escritorio/ Laptop)** | Para la recolección:<br>• Tomar fotografías del dispositivo en el lugar donde se encontró;<br>• Mencionar sus características una vía: 1) Extrayendo el disco duro para analizar; o 2) llevándose toda la computadora asegurándose de cubrir todos los agujeros de conexión incluso aquellos que permiten el desensamble del ordenador reguardado;<br>Para el resguardo y transporte:<br>• Bolsa antiestática o papel aluminio;<br>• Caja anti golpes para el Disco duro externo ó mínimo bien acojinada de cartón.<br>• Evitar golpes. | • Tener en un lugar sin humedad;<br>• No exponerlos a los cambios bruscos de temperatura;<br>• No almacenarlos o manipularlos cerca de campos electromagnéticos; | • Usar bloqueador de escritura;<br>• Copia con programas forenses especializados;<br>• Realizar el hash o huella digital del USB o disco. |

6 “Hash”. Una función criptográfica “hash”- usualmente conocida como “hash”- es un algoritmo matemático que transforma cualquier bloque arbitrario de datos en una nueva serie de caracteres con una longitud fija. Disponible en: https://latam.kaspersky.com/blog/que-es-un-hash-y-como-funciona/2806/

| | | | |
|---|---|---|---|
| **Teléfonos celulares: vieja generación/ Inteligentes** | Para la recolección:<br>• Tomar fotografías del dispositivo;<br>• Mencionar sus características;<br>• Realizar un croquis del lugar del hallazgo.<br>Para el resguardo y transporte:<br>• Bolsa Faraday o en su defecto envolverlo en varias capas de aluminio, para evitar conexiones externas o ponerlo en modo avión;<br>• Sí posible también conseguir la clave de acceso al teléfono celular o móvil; sí se advierte que tiene redes sociales o correo abierto, alguna aplicación que corra el riesgo de perderse con el apagado, llevarlo encendido al laboratorio forense pero aislado mediante una bolsa de faraday o un bote de aluminio como de pintura para que no deje penetrar señales externas conectado a una batería que le suministre energía para llegar al laboratorio o lugar de resguardo. | • Tener en un lugar sin humedad;<br>• No exponerlos a los cambios bruscos de temperatura;<br>• Con bloqueadores de señal para evitar que señales externas proporcionen la orden de borrado del aparato celular o móvil. | • Usar bloqueador de escritura para clonado de memorias externas del teléfono o móvil;<br>• Copia con programas forenses especializados;<br>• Realizar el hash o huella digital de la memoria interna del teléfono de ser posible. |

| | | | |
|---|---|---|---|
| **DVR** | Para la recolección:<br>• Tomar fotografías del dispositivo;<br>• Mencionar sus características;<br>• Realizar un croquis del lugar del hallazgo.<br>• En dado caso de no poder extraer todo el sistema del DVR se extrae la trama del video que interesa en el lugar del hecho, para su exhibición posterior, debido a que estos aparatos tienen su propio sistema de encriptación (único) y aunque se extraiga el disco duro no se podrá leer fuera de su consola original;<br>• Sí se retira del sistema DVR es necesario cubrir todos los agujeros de conexión incluso aquellos que permiten el desensamble del DVR;<br>• Copia de trama en disco duro externo para la transportación de evidencia obtenida;<br>• Bolsa Antiestática o papel aluminio;<br>• Caja anti golpes para el disco duro ó mínimo bien acojinada de cartón;<br>• Copia de trama en DVD o CD cajas plásticas adecuadas para resguardar el medio o en su defecto bolsas de papel especiales para guardar DVD o CD;<br>• Sellado y lacrado en el lugar del hallazgo de preferencia realizar ahí mismo el copiado, evitar golpes;<br>• Usar bloqueador de escritura para resguardar la información obtenida. | • Tener en un lugar sin humedad;<br>• No exponerlos a los cambios bruscos de temperatura;<br>• Disco duro no estar cerca de campos electromagnéticos;<br>• DVD no exponerse al sol directo, evitar ralladuras, no exponer a solventes agresivos que afecten el medio de almacenamiento. | • Copia con programas forenses especializados;<br>• Realizar el hash o huella digital del disco.<br>Copia con programas forenses especializados.<br>• Realizar el hash o huella digital del disco; *DVD* o *CD* o *Memoria USB*<br>• * Usar el mismo programa de la consola para después exportar la evidencia con programas forenses.<br>• * Realizar el hash o huella digital de la evidencia.<br>• * Usar bloqueador de escritura |

*Tabla elaboración propia.*

Como puede observarse las técnicas de recolección, traslado, manejo y preservación de evidencia electrónica o digital son bastante complejas y requiere conocimientos precisos en técnicas de informática, las cuales de forma común los Ingenieros en Sistemas o Informáticos o personas egresadas de carreras afines no vieron o cursaron en sus troncos de enseñanza, debido a que estas técnicas son relativamente novedosas.

Esto es en lo tocante tan solo a la recolección, manejo y preservación de evidencia electrónica o digital, porque en el análisis en

sí para determinar si una evidencia es falsa o no puede requerir de los conocimientos de diversas áreas tales como la foniatría[7], fotografía o fotografía digital, contaduría, antropometría[8], estilometría[9], por mencionar algunas; volcándose así en un estudio transdisciplinar.

De este modo, el estudio (pericial de informática forense[10]) puede ser tan complejo como se decida por parte de los investigadores (Fiscalías, Ministerios públicos, Jueces y otras autoridades) o inclusive por las partes, abriendo un abanico amplio de múltiples combinaciones con el objeto de llegar al conocimiento de verdad material de los hechos que se indaguen. La ventaja de recurrir a estas técnicas novedosas con los recaudos técnicos necesarios para preservar la evidencia, es que generan pruebas objetivas de los hechos, con la certeza de su no manipulación, que a su vez brindan al juzgador o las partes una perspectiva más amplia del evento.

Sin embargo, para llegar a obtener los resultados deseados y satisfactorios respecto de la evidencia electrónica o digital, esto es, por ejemplo en materia penal, que la evidencia logre convertirse en prueba al trascender en las diferentes etapas del procedimiento (investigación ministerial, investigación complementaria o judicializada, depuración en etapa intermedia o acusación y desahogo en juicio), requiere que los abogados o litigantes, así también las autoridades de investigación, cuenten con determinados conocimientos o en su defecto que estén asesorados por quienes si los tienen (peritos), a efecto de recolectar u ofrecer la evidencia electrónica o digital de la manera adecuada. Asimismo, contar con los conocimientos adecuados en esta materia, les permitirá vislumbrar hasta qué punto podrá llegar la evidencia, y de ser el caso, buscar un arreglo extrajudicial.

Para Jeremías *Betham* el objeto de las leyes es producir el más alto grado de felicidad máxima al mayor número de personas; en cuanto a los objetivos del procedimiento, se busca que las decisiones sean rectas, celeridad en el proceso y que este sea económico;

7 f. Med. Parte de la medicina dedicada a las enfermedades de los órganos de la fonación. Disponible en: https://dle.rae.es/foniatría

8 "La antropometría es la ciencia de la medición de las dimensiones y algunas características físicas del cuerpo humano. Permite medir longitudes, anchos, grosores, circunferencias, volúmenes, centros de gravedad y masas de diversas partes del cuerpo, las cuales tienen diversas aplicaciones." Disponible en: https://capanutri.com.mx/blog/antropometria-en-nutricion/

9 La estilometría analiza ciertos rasgos del estilo del autor y los utiliza para comparar dos o más textos. El punto de base de la estilometría es que el estilo es algo que nace en el subconsciente, y por esta razón, cada quien tiene su estilo propio. Por otro lado, la estilometría es una forma de analizar textos a diferentes niveles. Algunas de sus aplicaciones es determinar la autoría de una obra, la autenticidad, clasificación de textos, medición de frecuencia de palabras, identificación de lenguas. Disponible en: http://humanidadesdigitales.net/blog/2012/10/27/que-es-la-estilometria-y-para-que-sirve/

10 Se entiende por informática forense al conjunto multidisciplinario de teorías, técnicas y métodos de análisis que brindan soporte conceptual y procedimientos de investigación de la prueba indiciaria informática. Darahuge, María, Elena y Arellano, González, Luis E., Manual de informática forense (prueba indiciaria informática forense)bases metodológicas: científicas, sistemática, criminalística, tecnológica-pericial y Marco Legal, Buenos Aires, enrrepar, 2011, p.9

así como la eliminación de obstáculos superfluos[11].

Empero las máximas descritas anteriormente si bien son un ideal de lo que debería ser la ley y el procedimiento, en la actualidad distan mucho de alcanzar dicho objetivo, así pareciera que el fin último de los procedimientos no es la justicia sino la legalidad, al encontrarnos en plena revolución digital aún inmersos en procedimientos exhaustivamente formalistas; ante este panorama, es sumamente beneficioso previo a ejercitar cualquier acción de carácter legal, realizar un ejercicio de los alcances jurídicos que podría llegar a tener nuestra prueba electrónica o digital, más aun tratándose de pruebas que se recolectan de manera local pero que sus efectos involucran a otros países, en los cuales la cooperación internacional será inevitable, bien sea a través de los tratados y acuerdos de colaboración previamente signados, o mediante exhortos o cartas rogatorias; de esta forma, vislumbrar los alcances de la prueba permitirá elegir la opción que nos resulte más beneficiosa, aún tratándose de acuerdos extrajudiciales, ante la falta de certeza de poder recabar una prueba o involucrarnos en un procedimiento sumamente largo como consecuencia de recabar evidencia de otros países en donde las barreras de distancia e idioma son determinantes.

La experiencia del suscrito como Perito en Informática Forense me ha permitido observar las diversas complicaciones en la recolección de evidencia electrónica o digital, porque conllevan en determinadas circunstancias violaciones a los derechos humanos, en especifico al debido proceso, a veces no dolosa pero aun así perjudicial, por el desconocimiento de los aspectos más mínimos y elementales en materia de informática forense de los operadores del derecho, así, es común dañar la evidencia (hacerla inservible para la práctica de la pericial) o realizar un mal llenado de la cadena de custodia, lo que en un sistema tan formalista como el Penal hace intrascendente dicha prueba. Claros ejemplo de lo anterior es, una inadecuada recolección técnica al ocupar firmas digitales en desuso por las prácticas internacionales, asimismo, la nula posibilidad de contradecir la prueba de manera real, debido a la falta de expertos en la materia o por la denegación por parte del aparato que imparte justicia al acceso a la prueba con plazos correctos para su análisis.

Ahora bien, en materia civil, puede ofrecerse la prueba electrónica o digital siempre y cuando no se haya obtenido vulnerando derechos humanos (por ejemplo una intromisión a las comunicaciones privadas); en esta materia resulta trascendente en su ofrecimiento conservar una cadena de custodia privada con el objeto de no proporcionarle a la contra parte argumentos para que la prueba sea desechada por no resguardar adecuadamente la prueba para su exhibición.

En materia civil también es válido requerir la intervención de un fedatario público que haga constar la obtención de la evidencia; para qué acto jurídico se va sustanciar; bajo qué condiciones se resguarda el objeto sometido a investigación; y además se asiente con fe pública en el instrumento en conjunto la evidencia extraída con los medios de almacena-

11 Benham, Jeremías, Tratados de las prueba judiciales, Argentina, Valletta Ediciones, 2002, pp.3-6

miento como DVD o Memoria USB. En caso de un teléfono celular o móvil, después de la intervención del fedatario este puede quedar perfectamente embalado y resguardado en posesión de su propietario para posterior exhibición a la contra parte para el cotejo de los archivos que están en posesión del fedatario público; o la parte que tiene los extractos de evidencia en conjunto con el instrumento del fedatario público del ser el caso.

Haciendo un breve análisis de la evidencia electrónica o digital obtenida de la aplicación *WhatsApp*, tomándose esta como ejemplo al ser de los programa de mensajería instantánea más usados en el mundo, y dado que actualmente permite el borrado de mensajes (anteriormente también se realizaba pero requería de conocimientos avanzados en computación al no ser una herramienta del propio programa), los argentinos Gastón Enrique Bielli y Carlos Ordoñez en su libro La prueba electrónica teoría y práctica[12] proponen lo que ellos denominan tripe test de admisibilidad para los casos de *WhatsApp* que consiste en cuidar tres aspectos a saber: la autenticidad; la integridad; y la licitud. Con ello buscan que la prueba recabada de *WhatsApp* tenga los pilares jurídicos necesarios para que trascienda a las diferentes etapas del proceso.

En el primer elemento del Test de admisibilidad propuesto por Bielli y Ordoñez, es el relativo a la autenticidad, cuya finalidad es arrojarnos indicios del presunto autor aparente, lo anterior para descartar que el teléfono celular desde el cual se envía el mensaje haya sido tomado por una persona distinta a su propietario, robado o hackeado[13]. Mientras que en el tradicional documento escrito la autoría puede acreditarse con la firma del autor o su sello comercial en su defecto; para el documento electrónico en muchos casos se identifica el ordenador o dispositivo del cual se ha enviado el mensaje, pero no quién es su remitente.

La situación anterior nos coloca en la necesidad de verificar la autenticidad mediante otras características denominadas atributos del documento, que contiene fecha de generación del mensaje, el dispositivo del cual se generó, si la persona generadora y receptora coinciden, y en la mayoría de las veces incluso la versión del programa del cual se generó el archivo.

Reforzado lo anterior con la encriptación de usuario a usuario y su firma digital que vincula el número del celular o móvil, así como la cuenta del usuario del cual se originan los

12 Bielli, Gastón Enrique y Ordoñez, Carlos Jonathan, La prueba electrónica teoría y práctica, Argentina, La ley, p.553.

13 El hackeo hace referencia a las actividades que buscan comprometer los dispositivos digitales, como ordenadores, teléfonos inteligentes, tabletas e incluso redes enteras. Y aunque el hackeo puede no tener siempre fines maliciosos, actualmente la mayoría de las referencias tanto al hackeo como a los hackers, se caracterizan como actividad ilegal por parte de los ciberdelincuentes, motivados por la obtención de beneficio económico, por protesta, recopilación de información (espionaje), e incluso sólo por la “diversión” del desafío. disponible en: https://es.malwarebytes.com/hacker/

mensajes, tarjeta SIM[14], y el código IMEI [15] del celular, lo que resulta en un mínima presunción del autor.

Ahora bien, el segundo elemento al que hace alusión el Test de admisibilidad es la Integridad, así, en la informática se habla de integridad cuando la información se encuentra inalterada en su contenido original en conjunto con las características señaladas en los párrafos precedentes y la firma digital, de modo tal que existe seguridad de que el documento no fue modificado de ninguna forma.

El tercer elemento del Test es el de la licitud, que se encuentra estrechamente ligado con la prueba, en razón a la forma de la obtención y el modo de su obtención de su fuente originadora o del elemento proveniente.

Sin embargo, el autor de este documento incorporaría un cuarto elemento  al Test de admisibilidad, consistente en la verificación del equipo para saber si conserva o mantiene las características de fábrica y además los parches de seguridad, antivirus o antimalware[16], puesto que en la jerga informática es sabido que un sistema computacional de cualquier tipo es relativamente seguro en tanto conserve estas características.

En la práctica muchos de los teléfonos celulares que llegan a las manos de los peritos cuentan con los permisos root[17] habilitados en

14 La tarjeta *SIM* o *SubscriberIdentity Module* es una pequeña tarjeta de plástico que tiene un chip pegado a ella, y que tienes que insertar en tu teléfono móvil o smartphone. En este chip,almacena de manera segura tu número de teléfono, así como las claves de acceso de un usuario concreto en una operadora de telefonía. disponible en: https://www.xataka.com/basics/tarjeta-sim-como-funciona-como-saber-que-tipo-tuya

15 Se trata de un número de 15 dígitos que lo identifica. En inglés se llama *International Mobile EquipmentIdentity,* lo que en español se traduce como “identidad internacional de equipo móvil”. Pero todo el mundo lo conoce por sus siglas: IMEI. disponible en: https://www.bbc.com/mundo/noticias-42774859

16 “Hoy en día, Internet está lleno de *malware* programado para buscar automáticamente las debilidades de tu equipo. El mejor programa impide la instalación de malware de manera eficiente y eficaz, y si alguno consigue entrar en el sistema, lo elimina. Aunque seas el único que usa tu ordenador personal o portátil, el antimalware sigue siendo necesario para una seguridad en internet fiable y robusta. Disponible en: https://softwarelab.org/es/que-es-antimalware/

17 Rootear Android es la operación que hay que realizar para obtener permisos de superusuario, y así tener el permiso del móvil para hacer los cambios más profundos dentro del sistema operativo. Vamos, que tienes el control total de tu móvil para hacer lo que quieras con él. Esto te permite tener una versión de Android que no está controlada por el fabricante, sino por la comunidad de desarrolladores, algo que tiene algunas ventajas y también desventajas. Así pues, podemos decir que rootear tu dispositivo es algo así como desbloquearlo, quitarle los impedimentos con los que el fabricante te mantiene todo el rato al nivel de usuario. Una vez has rooteado el móvil, podrás instalar los permisos de superusuario mediante una aplicación, y entonces ya podrás obtener todo el control sobre él. Para qué sirve rootear Android Rootear Android todavía tiene algunas ventajas que hace que los usuarios más avanzados aún recurran a ello en algunos casos. La más extendida es la de poder instalar ROMs o versiones modificadas de Android, como por ejemplo LineageOS o Paranoid Android. Esto te permite tener una versión de Android que no está controlada por el fabricante de tu móvil, sino por la comunidad de desarrolladores. Gracias a esto, por ejemplo, podrás actualizar un móvil que ya está viejo y del que el fabricante

los sistemas Androide[18], lo que le permite al usuario del equipo tener acceso a todo el teléfono y por ende a todos los programas que están instalados en el dispositivo para que éste pueda modificarlos a su gusto, incluso las bases de datos de *WhatsApp;* así, una vez con permisos root habilitados se tendría que analizar si han instalado aplicaciones tendientes a modificar las bases de datos en el teléfono, para de este modo dar certeza de que los mensajes están intactos (integridad).

Aquí cabe señalar que los equipos *Iphone* no están exentos de sufrir modificaciones en sus bases de datos, en el caso de estos dispositivos es a través de la aplicación jailbreak[19], que se tiene acceso al teléfono logrando con ello poder instalar aplicaciones no oficiales tendientes a modificar bases de datos.

Sin embargo hay que aclarar que el modo root o jailbreak, no es dañino per se; puesto que éstos se ocupan por los Informáticos forenses para poder realizar estudios profundos a los dispositivos sujetos a investigación; entonces qué es el root o jailbreak, simplemente el tener acceso a todas la características del software instalado en el teléfono y a todos sus programas; lo cual de primera intención no implica modificación de contenido sensible generado por el usuario del dispositivo o terceros.

se ha desentendido a nuevas versiones de Android con todas sus ventajas. Rootear también te puede ayudar a exprimir el hardware al máximo aprovechando todo el potencial de los componentes internos del móvil. Por ejemplo, podrás instalar aplicaciones para modificar la frecuencia del procesador, o aplicaciones para analizar la batería y evitar que otras apps se queden funcionando de fondo y consumiendo recursos. Además de esto, rooteando Android también vas a poder desinstalar cualquier aplicación de tu dispositivo, incluso esas que por lo general nunca puedes desinstalar por decisión del fabricante o de la propia Google. Aunque eso sí,desinstalar algunas aplicaciones puede hacer que el móvil deje de funcionar correctamente.Y por último, gracias a esas versiones modificadas o cocinadas(el término que usan los desarrolladores) de Android también puede servir para tener nuevas funciones en el móvil, o incluso tener una mayor capacidad de personalización para darle exactamente el aspecto que quieras sin los límites que ha impuesto el fabricante. Disponible en:https://www.xataka.com/basics/root-android-que-sirve-cuales-sus-inconvenientes

18 Es el sistema operativo que utilizan 2,500 millones de dispositivos activos. Desde teléfonos con 5G hasta las más increíbles tablets, la tecnología de Android está presente en todos ellos. Disponible en: https://www.android.com/intl/es-419_mx/what-is-android/

19 En términos técnicos, el *jailbreak* es la instalación de parches de kernel modificados que permiten que ejecutes software no autorizado por Apple. En términos más sencillos, jailbreak es el proceso mediante el cual se superan las restricciones del dispositivo, lo que permite al usuario cambiar el sistema operativo o la instalación de ciertas aplicaciones.
Por lo tanto, el *Jailbreak* te permite tener accesos de administrador al dispositivo que has hackeado. Tendrás la posibilidad de cambiar la configuración que en un principio no podías, bajar las aplicaciones que no cumplen con la normativa de *Apple Store* y personalizar los funciones como quieras.
A menudo, el *jailbreak* de *iOS* es comparado con el de *Android rooting*, pero ambos procesos difieren mucho entre sí. Apple integra una seguridad bastante estricta en sus dispositivos, como el gestor de arranque que evita que los usuarios modifiquen el sistema operativo.
A pesar de que no es ilegal hacerle un *jailbreak* a un *iPhone,* su instalación va en contra los términos y condiciones de uso. Disponible en: https://opendatasecurity.io/que-es-el-jailbreak/

A continuación, se analizan algunas tesis, que nos permiten vislumbrar los lineamientos que la Suprema Corte de Justina de la Nación, ha ido estableciendo para la valoración de pruebas electrónicas o digitales.

**“CADENA DE CUSTODIA. SU TRANSGRESIÓN NO TORNA ILÍCITOS LOS DATOS DE PRUEBA.**

La transgresión a los principios legales de cadena de custodia, no torna ilícitos los datos de prueba relacionados con la evidencia respectiva. La ilicitud es un tema que atañe a la manera en que se obtiene la prueba en tanto que la cadena de custodia es la manera en que se preserva la misma. Conforme al artículo 264 del Código Nacional de Procedimientos Penales, los datos de prueba obtenidos contra derechos fundamentales conllevan su exclusión o nulidad; en cambio, los indicios alterados por violación a la cadena de custodia repercuten en su valoración, pues el numeral 228 del mismo código, determina que aquéllos no perderán su valor probatorio a menos que la autoridad competente verifique que han sido modificados de tal forma que pierdan su eficacia.”[20]

Por cuanto a esta tesis se comparte su contenido en lo inherente al señalar que los datos obtenidos con violación a derechos fundamentales traen aparejados la exclusión o la nulidad de los mismos; cuestión que a nivel de diversos tratadistas sostienen en sus argumentos como válido. En cambio, no se comparte el criterio adoptado, al establecer que los indicios alterados por la violación de cadena de custodia repercuten en su valoración, situación que resulta muy delicada en informática forense debido a la facilidad que tiene cualquiera de las partes involucradas para alterar las pruebas.

Si no se han tomado los recaudos técnicos necesarios previos para detectar la alteración, se corre un riesgo muy elevado de estar juzgando con pruebas falsas. Usted lector se preguntará por qué es esto posible, la respuesta es simplemente por la facilidad de copia de los archivos siendo idénticos en otro dispositivo; no se pueden diferenciar a menos que al inicio se identifique el medio original a través de etiquetas y su respectiva copia. Por lo tanto, aceptar datos de prueba con cadenas de custodia no escrupulosamente atendidas caemos en la posibilidad de que estas sean alteradas en el proceso legal; de tal forma que mientras en las pruebas físicas se podrá en muchas de las ocasiones con un peritaje adecuado detectar la alteración con mayor facilidad, tratándose de pruebas electrónicas o digitales es más complejo percibir su alteración debido a las razones señaladas en líneas precedentes.

**“PRUEBA ELECTRÓNICA O DIGITAL EN EL PROCESO PENAL. LAS EVIDENCIAS PROVENIENTES DE UNA COMUNICACIÓN PRIVADA LLEVADA A CABO EN UNA RED SOCIAL, VÍA MENSAJERÍA SINCRÓNICA (CHAT), PARA QUE TENGAN EFICA-**

20 Registro No. 2021845
Localización: Décima Época
Instancia: Tribunales Colegiados de Circuito
Fuente: Gaceta del Semanario Judicial de la Federación.
Libro 77, Agosto de 2020, Tomo VI.
página: 5981
Tesis: I.4o.P.36 P (10a.)
Materia: Penal

**CIA PROBATORIA DEBEN SATISFACER COMO ESTÁNDAR MÍNIMO, HABER SIDO OBTENIDAS LÍCITAMENTE Y QUE SU RECOLECCIÓN CONSTE EN UNA CADENA DE CUSTODIA.**

(...) se extiende a las llevadas a cabo mediante cualquier medio o artificio técnico desarrollado a la luz de las nuevas tecnologías, desde el correo o telégrafo, pasando por el teléfono alámbrico y móvil, hasta las comunicaciones que se producen mediante sistemas de correo electrónico, mensajería sincrónica (chat), en tiempo real o instantánea asincrónica, intercambio de archivos en línea y redes sociales (...)"[21]

Bien puntualiza esta tesis al señalar que la evidencia de una comunicación privada que es obtenida de una red social vía mensajería comúnmente conocido como chat, para que tenga eficacia probatoria como mínimo debe haber sido obtenidas lícitamente es decir sin vulneración a los derechos humanos, y que su recolección conste en una cadena de custodia. Como se dijo en el análisis de la tesis anterior, flexibilizarse las cadenas de custodia, hace propenso el riesgo de la manipulación informática.

Otro de los aspectos más relevantes de esta tesis, es el parámetro de en qué momento las conversaciones en que intervenimos y que pretendemos ofrecer como dato de prueba deja de tener el carácter de secreto, siendo a través de la autorización de la parte oferente o bien mediante la autorización judicial.

El autor está de acuerdo con esta tesis que señala que dada la naturaleza de los medios electrónicos que son intangibles y que son fácilmente manipulables y susceptibles de alteración, se exige para constatar la veracidad de su origen y contenido la existencia de registros adecuados con cadena de custodia bien estipulada marcando la trazabilidad de la evidencia logrando preservar el principio de mismidad que persigue la implementación de la cadena de custodia. Cayendo en falta de requisitos de ilicitud o en su defecto de fiabilidad.

**"VIDEOGRABACIONES. SU VALOR PROBATORIO EN EL PROCEDIMIENTO LABORAL.**

El artículo 776 de la Ley Federal del Trabajo, vigente hasta el 30 de noviembre de 2012, estatuye que son admisibles en el proceso todos los medios de prueba que no sean contrarios a la moral y al derecho, destacando entre éstos la fracción VIII, referida a las fotografías y, en general, a aquellos medios aportados por los descubrimientos de la ciencia. Ahora bien, es importante tomar en cuenta que en la actualidad, muchas de las empresas, por seguridad para un manejo más eficaz en el desempeño de sus actividades cotidianas, se valen del empleo de determinados descubrimientos de la ciencia como son ciertos sistemas audiovisuales basados en medios digitales o electrónicos que sirven para dejar

21 Registro No. 2013524
Localización: Décima Época
Instancia: Tribunales Colegiados de Circuito
Fuente: Gaceta del Semanario Judicial de la Federación.
Tomo: Libro 38, Enero de 2017, Tomo IV, página
página: 2609
Tesis: I.2o.P.49 P (10a.)
Materia: Penal

constancia de lo acontecido, entre ellos, la cámara de video, la cual, según el Diccionario de la Lengua Española de la Real Academia Española, consiste en un: "Aparato portátil que registra imágenes y sonidos y los reproduce."; las que pueden ser almacenadas y preservadas en un registro o soporte electrónico. Además, todo lo ahí contenido logra reproducirse mediante grabaciones en formatos digitales conocidos comúnmente como "DVD", entre otros. Consecuentemente, las videograbaciones deben considerarse como pruebas en el procedimiento laboral porque son herramientas electromagnéticas que constituyen avances tecnológicos de la ciencia; no obstante lo anterior, una vez que son extraídas del lugar donde se encuentran almacenadas, por sí solas, no constituyen prueba plena, sino únicamente un indicio porque, por su naturaleza, son susceptibles de ser manipuladas por los encargados de copiar las grabaciones y, por ello, requieren estar reforzadas o adminiculadas con otra probanza."[22]

El contenido de esta tesis corrobora lo expuesto por el suscrito en párrafos precedentes, en lo inherente a las prevenciones que se deben tener en cuenta al manejar la prueba electrónica o digital consistente en videograbaciones, puesto que generalmente únicamente se extrae la trama del video que nos interesa debido a que estos aparatos tienen su propio sistema de encriptación (único) y aunque se extraiga el disco duro no se podrá leer fuera de su consola original.

Sin embargo, a criterio del suscrito se considera exagerado el hecho que de acuerdo a la tesis anteriormente transcrita la prueba (videograbación) por sí misma no constituya una prueba plena, sino únicamente un indicio, porque podría darse el caso que una videograbación registre el momento en que un empleado realice actos que impliquen la falta de probidad (causa de un cese en materia laboral), y sea de los únicos elementos que lo vinculen con el hecho, a este debería otorgársele valor pleno, si se observan determinadas pautas para su recolección, por ejemplo llevar a un fedatario público que de constancia del dispositivo que contiene la grabación, la forma en que se realiza la copia del segmento que interesa, así como del resguardo de la copia, lo cual además se encuentre acompañado de una cadena de custodia privada de ser el caso y fortalecido con una pericial en informática forense que avale la no alteración del contenido de la videograbación.

Otro elemento que llama la atención es la preconcepción de que todos los encargados de suministrar los videos están en el ánimo de falsear o alterar la realidad.

En el caso que se expone en la tesis nos permite ejemplificar también uno de los supuestos manejados en párrafos precedentes, siendo el relativo a que la pericial de informática forense puede ser tan compleja como se decida, o combinarla con otras periciales que le darán mayor fuerza de convicción, así retomando el

22 Registro No. 2008744
Localización: Décima Época
Instancia: Tribunales Colegiados de Circuito
Fuente: Gaceta del Semanario Judicial de la Federación.
Tomo Libro 16, Marzo de 2015, Tomo III.
página 2551
Tesis: IV.3o.T.26 L (10a.)
Materia: Laboral

supuesto de que una videograbación registre el momento en que un empleado realice actos que impliquen la falta de probidad (causa de un cese en materia laboral), la pericial en informática forense determinará si el video expuesto ha sido manipulado o no, así también si fue recabado de la forma adecuada, así al corroborarse lo anterior, lo siguiente sería emitir una pericial que determine que la persona o sus rasgos físicos que aparece en los videos o su voz, de ser el caso, coincide con los de la persona que se investigue; advirtiéndose así la importancia del correcto desarrollo de dicha pericial, puesto que una da lugar a otra, así si se desvirtúa la veracidad del video resultaría innecesario realizar otras periciales como las antropométricas puesto que surge de algo viciado.

La tesis al establecer que las videograbaciones por sí solas, no constituyen prueba plena, sino únicamente un indicio porque, por su naturaleza, son susceptibles de ser manipuladas por los encargados de copiar las grabaciones y, por ello, requieren estar reforzadas o adminiculadas con otra probanza, bien puede referirse por otra probanza a la pericial en informática forense, que puede entre otras situaciones basándose en las técnicas especializadas lograr autenticar que un video no fue modificado, resaltando la no alteración de los fotogramas[23] que conforman el video. Además de los metadatos que pudiera contener el archivo de video aparejado en el archivo extraído de la consola de videograbación. Y sí además se le incorpora una firma digital de creación queda más que garantizada la no adulteración si es que la consola lo hace de manera automática al generar el archivo de video vigilancia o en defecto firmando también automáticamente aquel que se extrae de la consola de video vigilancia.

Como puede observarse existen formas para advertir si un archivo de video fue manipulado de manera artificiosa, así, una vez demostrado que no cuanta con edición debería reconsiderarse su escala de valor.

**“PRUEBAS DE AUDIO Y VIDEOGRABACIÓN EN EL JUICIO LABORAL. ATENDIENDO A SU NATURALEZA, SU DESECHAMIENTO POR NO ACOMPAÑARSE EN SU OFRECIMIENTO LOS ELEMENTOS NECESARIOS PARA SU DESAHOGO CONSTITUYE UNA VIOLACIÓN A LAS LEYES DEL PROCEDIMIENTO.**

Si bien es cierto que el artículo 780 de la Ley Federal del Trabajo establece la obligación de ofrecer las pruebas acompañadas de todos los elementos necesarios para su desahogo, también lo es que tratándose de la prueba consistente en casetes, uno de audio y otro de video, resulta improcedente que la autoridad laboral la deseche con base en que al ser ofertada no se exhibieron los instrumentos electrónicos necesarios para su práctica, ya que, en todo caso, debe conminar a su oferente para que el día y hora que fije para su desahogo, allegue los medios con los que pueda llevarse a cabo su reproducción, pues dada su naturaleza, resultaría ilógico pretender que al escrito de ofrecimiento deban acompañarse, además de los respectivos casetes, un audio reproductor, una videoreproductora y un aparato de televi-

23 De *foto* y *grama*.m. Cada una de las imágenes que se suceden en una películacinematográfica. Disponible en: https://dle.rae.es/fotograma

sión, mecanismos que estarían en poder de la responsable durante todo el tiempo que transcurra hasta su diligenciación, lo cual sería oneroso para el oferente; consecuentemente, si la prueba es desechada, ello constituye una violación a las reglas del procedimiento que afecta las defensas del oferente y trasciende al resultado del fallo."[24]

De los aspectos más llamativos de la Tesis anteriormente citada, la constituye el hecho de que la misma se emitió ante una situación recurrente como lo era el desechar una prueba digital al no haberse ofrecido los elementos necesarios para su desahogo que tratándose de este tipo de pruebas, lo pueden constituir un reproductor de video o audio, aquí cabe señalar que en la actualidad una pericial en informática forense, bien solicitada, puede hacer prescindibles la exhibición o uso de aparatos reproductores de audio o video, puesto que, al corroborarse la no alteración o manipulación del medio que se ofrezca se pueden obtener las secuencia fotográficas de sus contenidos, o las versión estenográfica del audio, lo que facilita manejar la prueba.

## CONCLUSIÓN

Finalmente y a modo de conclusión, es importante vislumbrar los alcances y efectividad que puede tener la adecuada recolección, manejo y resguardo de evidencia relativa a pruebas digitales o electrónicas; aun más si se toma en consideración la automatización creciente en todos los aspectos de nuestras vidas cotidianas, que nos hace depender cada vez más de medios electrónicos o digitales para la consecución de nuestras tareas más simples a las más complejas, actos que anteriormente realizábamos de manera presencial en la actualidad se realizan a distancia a través de algún dispositivo electrónico sin ninguna complicación, por ejemplo los trámites bancarios, no obstante esta situación también nos hace proclives a ser víctimas de los delitos cibernéticos, en los cuales la realización de una pericial en materia de informática forense es imprescindible y para lo cual como abogados lo menos que debemos conocer son los aspectos mínimos que la misma debe observar, así también nos es de gran utilidad saber la forma en que se deben manejar los dispositivos que resguardan información electrónica o digital con el fin de no destruirlos y ofrecerlos como prueba lo mejor posible.

Si bien los temas informáticos son complejos, y la gran mayoría de los abogados no estamos habituados a manejarlos con facilidad, es importante que en nuestro quehacer jurídico auxiliarnos o apoyarnos de los expertos que, si conocen la materia, con la finalidad de ofrecer la prueba lo mejor posible, asimismo para advertir alguna irregularidad en la que ofrezca nuestra contra parte.

Como último punto se sugiere, siempre estar al pendiente de la cadena de custodia, como se vio en el cuerpo del presente el hecho de que se traten de pruebas electrónicas o digitales no exime la obligación que tienen las autoridades y particulares de llenar la cadena de custodia toda vez que, si bien el contenido en sí es digital (no palpable), los medios en que se resguardan si lo son, así que darle prioridad a estas situaciones nos facilitará que

24 Registro No. 177866
Localización: Novena Época
Instancia: Tribunales Colegiados de Circuito

nuestra prueba logre el fin que esperamos, y que por el contrario no sea desvirtuada por no haberse observado un protocolo en su recolección.

## BIBLIOGRAFÍA

**Libros:**

*Benham*, Jeremías, Tratados de las prueba judiciales, Argentina, Valletta Ediciones, 2002, pp.3-6

Bielli, Gastón Enrique y Ordoñez, Carlos Jonathan, La prueba *electrónica teoría y práctica,* Argentina, La ley, p.553.

Quadri, G,H, La prueba en el proceso civil comercial, Abeledo-Perrot, Buenos Aires, 2011 T.1, p.1109

*Cibercriminalidad fundamentos de investigación en México*, 3ed., 2018, p.553

Darahuge, María, Elena y Arellano, González, Luis E., *Manual de informática forense (prueba indiciaria informática forense)bases metodológicas: científicas, sistemática, criminalística, tecnológica-pericial y Marco Legal,* Buenos Aires enrrepar, 2011, p.9

**Internet:**

- https://www.antena3.com/noticias/economia/sensacion-tocar-objetos-personas-distancia_20150501571df6d66584a8abb5822ff1.html
- https://softwarelab.org/es/usb/
- https://www.camarasdevigilanciabarcelona.com/noticias/sabes-cual-es-la-diferencia-entre-dvr-nvr-y-ndvr/index.html
- https://latam.kaspersky.com/blog/que-es-un-hash-y-como-funciona/2806/
- https://dle.rae.es/foniatría
- https://capanutri.com.mx/blog/antropometria-en-nutricion/
- http://humanidadesdigitales.net/blog/2012/10/27/que-es-la-estilometria-y-para-que-sirve/
- https://es.malwarebytes.com/hacker/
- https://www.xataka.com/basics/tarjeta-sim-como-funciona-como-saber-que-tipo-tuya
- https://www.bbc.com/mundo/noticias-42774859
- https://softwarelab.org/es/que-es-antimalware/
- https://www.android.com/intl/es-419_mx/what-is-android/
- https://sjf2.scjn.gob.mx/busqueda-principal-tesis