



Utilizamos cookies tanto propias como de terceros para evaluar la actividad general y el uso que se hace de nuestras Plataformas Online, mejorar su experiencia de navegación y ofrecerle información comercial personalizada. Si usted continua navegando, consideramos que acepta su uso. Puede cambiar la configuración y obtener más información haciendo clic [aquí](#)

[Conozca ADN](#) | [Auditsoft](#) | [Conecta](#) | [Práctica Procesal](#) | [Revistas](#) | [Suite Jurídica 2](#)

Acceso clientes

Librería virtual







[Inicio](#) | [Actualidad](#) | [Tribuna](#) | [Publicaciones](#) | [Productos](#) | [Corporativa](#) | [Especiales](#) | [Law & Tic](#) | [Observatorio](#)

Propiedad Intelectual e Industrial

Privacidad

Internet y Tecnología

Ciberseguridad

En colaboración con:

Telecomunicaciones

e-Commerce

e-Administración

Marketing de despachos



PRUEBA DIGITAL

# Adquisición y presentación en un procedimiento judicial de una prueba informática

Por [Javier Rubio Alamillo](#)

Perito informático

| 03.04.2017

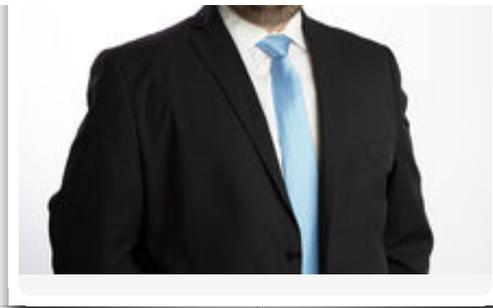
Comentar



Existe mucha confusión a la hora de cómo se debe introducir una prueba informática en un proceso judicial. En general, según la STS 300/2015 y la STS 754/2015, confirmando esta última la doctrina de la primera, la distinción para la introducción de una prueba informática...



COMENTARIOS  
JURISPRUDENCIALES



directriz para la introducción de una prueba informática o digital en un proceso judicial, es mediante la presentación de un informe pericial informático. Estas sentencias obligan a la práctica de una prueba pericial si se quiere introducir una prueba informática en el proceso y descartan expresamente la presentación de pruebas informáticas mediante “pantallazos”, impresiones, etc. Así pues, cualquier “pantallazo” o impresión que se presente, sin prueba pericial que garantice su autenticidad, de un mensaje de correo electrónico, de mensajes de WhatsApp, de contenido en redes sociales como Facebook o Twitter, etc., podrá ser inmediatamente impugnado. El encargado de practicar una prueba pericial para este tipo de evidencias es el perito informático. Según la Ley de Enjuiciamiento Civil, en su artículo 340, los peritos han de estar titulados en la materia objeto del dictamen y, según la Ley de Enjuiciamiento Criminal, en su artículo 457, los peritos que están titulados en la materia objeto del dictamen, son considerados “titulares”, mientras que, los no titulados, son considerados “no titulares”.

La Ingeniería Informática es la única profesión de ingeniería, incomprensiblemente, que no se encuentra regulada por el Estado en España, pese a que otros países de la Unión Europea sí la tienen regulada y, de hecho, actualmente, la Comisión Europea mantiene abierto un expediente (código “EU PILOT 7415/15”), para investigar por qué el Gobierno de España no ha regulado aún la Ingeniería Informática (existen poderosos lobbies profesionales y empresariales en contra). Debido a esta grave situación, existen en el mercado numerosos profesionales que se autodenominan “peritos informáticos”, incurriendo en intrusismo profesional, pese a que las leyes procesales son taxativas y exigen la posesión del título oficial relacionado con la materia del dictamen.

Es por tanto evidente que, para la elaboración de un dictamen pericial informático, se deberá requerir la pericia de un Ingeniero o Ingeniero Técnico en Informática o, con las nuevas titulaciones de Bolonia, de un titulado en el Máster o el Grado de Ingeniería Informática. La única forma de tener constancia de que el perito es “titular”, según dispone la Lecrim y, por tanto, titulado universitario, es que el profesional se halle adscrito a un Colegio Profesional. Los peritos no titulados suelen actuar bajo la figura de asociaciones con nombres rimbombantes, siendo la única asociación de titulados universitarios en Ingeniería Informática, excluyente por titulación universitaria y actuante a nivel nacional, la ALI, punta de lanza de la regulación profesional y de la creación de los Colegios Profesionales en toda España, de la que el profesional que suscribe también forma parte.

### Introducción de la prueba informática en el proceso judicial y mantenimiento de la cadena de custodia

Como ya se ha indicado, entonces, la única forma posible de introducir, con todas las garantías, una prueba digital en un procedimiento judicial, es mediante la práctica de una prueba pericial llevada a cabo por un perito informático colegiado. El perito se servirá de herramientas, tanto de



### Protección de datos y derecho a la intimidad y honor. Listas negras. Carga de la prueba

Sentencia del Tribunal Supremo de 12 de noviembre de 2015.



### Productos designados con una marca que se despachan a libre práctica y se incluyen en el régimen suspensivo de impuestos especiales sin el consentimiento del titular de la marca

Derecho del titular a oponerse a esa inclusión. Sentencia del Tribunal de Justicia de 16 de julio de 2015, Bacardi (C-379/14).

## CASE STUDY & MASTER CLASS

### Determinación del régimen jurídico de los perfiles generados por las cookies en función de su tipología

La empresa tecnológica X acaba de lanzar su solución de software "The red carpet welcome", un servicio de pago, bajo modelo de suscripción, destinado a su comercialización inicialmente a empresas...



### Redes sociales y menores: La cuestión de prueba del conocimiento y del consentimiento que ha de prestar el responsable legal

Juan con motivo de la celebración de la Primera Comunión de su hijo Luis, de nueve años de edad, decide regalarle un smartphone...



### Interpretación y aplicación del derecho al olvido en España

Antonio es un empresario que se ha dado cuenta de que al teclear su

*hardware* como de *software* -propietario y libre, en función de las necesidades del caso- y, si dicho profesional lo considera necesario, de un notario que dé fe de la clonación o volcado de las evidencias relacionadas con la causa y, en su caso, de la elevación a documento público del *hash* obtenido para cada una de dichas evidencias. Un *hash* es un código alfanumérico consistente en un resumen del contenido de una evidencia, calculado mediante un algoritmo matemático, teniendo como características la irreversibilidad y la univocidad, lo cual quiere decir que, con el código *hash*, no se puede obtener el contenido original de la evidencia -es decir, es irreversible- y, además, dicho código es único para el contenido del cual se ha obtenido -con lo cual, existe una correspondencia unívoca entre el contenido y el *hash*-, lo cual implica que cualquier mínimo cambio en el contenido, provocaría un cambio en el *hash*. El *hash* es la única garantía del mantenimiento de la cadena de custodia sobre la evidencia. El notario, por tanto, es el encargado de elevar a público, mediante un acta de constancia, el "estado" de la evidencia (el *hash*) en el momento de ser volcada, para evitar cualquier posible impugnación alegando una manipulación del perito sobre la misma. Cualquier otro perito podrá, posteriormente, calcular de nuevo el *hash* de la evidencia y comprobar que no ha existido tal manipulación, al menos desde que fue calculado el código *hash* ante notario.

Es importantísimo reseñar que el notario no sustituye al perito informático, es decir, un notario no puede realizar las funciones de un perito informático, entre otras cosas, porque se lo prohíbe el artículo 199 del Reglamento de la organización y régimen del notariado, que impide al notario intervenir allí donde sean necesarios conocimientos periciales. Es necesario poner un ejemplo para verlo más claro: un notario puede acudir a un edificio y levantar un acta pública de presencia, certificando que en el edificio existen grietas (ya que es algo que el notario puede percibir a través de sus sentidos, concretamente, de su vista), sin embargo, el notario no puede saber, de ningún modo, si el edificio va a caerse, algo que únicamente podrá certificar un arquitecto o un aparejador, mediante un informe pericial, señalando si las grietas afectan a pilares maestros y si, por tanto, el edificio corre peligro de derrumbe. Aplicado a una prueba informática, el notario puede dar fe de que unos mensajes de WhatsApp o un correo electrónico se encuentran en un determinado soporte, o determinado comentario en un muro de Facebook aparece publicado, pero en modo alguno puede garantizar su autenticidad e integridad.

En este punto es necesario señalar que, en los últimos tiempos, se está poniendo de moda, por parte de los notarios, la realización de actas notariales de constancia de mensajes de aplicaciones de mensajería instantánea, tipo WhatsApp, de correos electrónicos, o de contenido en Internet. El notario no puede garantizar, bajo ningún concepto, ni la autenticidad ni la integridad de los contenidos y, por tanto, un acta notarial de constancia de contenidos informáticos no debería poder utilizarse a nivel policial ni judicial. Este profesional ha trabajado en causas judiciales en las que una de las partes fue detenida y/o encausada a raíz de la aportación de un acta notarial de constancia de contenido informático en un dispositivo móvil o en Internet y, posteriormente, fue absuelta una vez fue demostrado por este profesional que, la prueba, había sido alterada o no se había conservado sobre la misma una cadena de custodia que permitiese garantizar la autenticidad e integridad del contenido.



¿Cada vez que al teclear su nombre y apellidos en la página Web de google, hay un enlace que hace referencia a su pasado que desea que desaparezca. ¿Cómo debe actuar para que desaparezca ese enlace?

## ENTREVISTAS



**Javier Sánchez García,**  
**vicepresidente del Consejo**  
**General de Procuradores de**  
**España**

"Los procuradores somos una profesión desaprovechada que podemos aportar mucho más"



**William Malcolm, Senior**  
**Privacy Counsel en**  
**Google sobre privacidad,**  
**seguridad y derecho al olvido**

"El derecho al olvido es un derecho fundamental inalienable, pero a la vez restringido, que debe equilibrarse con la libertad de expresión"



**Emmanuel Roesler. Director**  
**comercial de IBM Security**  
**Systems para España**

"Estamos empezando a ver cómo Watson puede luchar contra el cibercrimen"

## GESTIÓN DE DESPACHOS



**Los 10 consejos claves de SEO**  
**que un profesional jurídico debe**  
**tener en cuenta para mejorar su**  
**presencia online.**

Cada vez es más importante para muchos despachos de abogados y asesorías tener un portal web que no solo dé una visión moderna de la empresa, sino que genere suficiente tráfico para cumplir sus

A este respecto cabe reseñar que, por ejemplo, este perito demostró, en octubre de 2015, con gran impacto mediático en todos los principales medios de comunicación nacionales, que los mensajes de WhatsApp se podían manipular sin dejar rastro, perteneciendo por tanto a la realidad de las cosas que se puede alterar el contenido que subyace sobre este tipo de tecnología y, por tanto, que es vital mantener la cadena de custodia sobre la evidencia, de tal forma que se evite la posibilidad de poner en sospecha la integridad de la misma. Así pues, si los mensajes se pueden manipular sin dejar rastro, es evidente que un notario no puede garantizar ni la autenticidad ni la integridad de los mismos y que, lógicamente, un acta notarial de constancia de mensajes, no se puede utilizar para encausar a nadie.

### ¿Cómo debe presentarse una prueba informática en un procedimiento judicial?

Si se trata de una prueba como un correo electrónico corporativo, un fichero informático, el contenido de una página web, etc., la prueba se debe presentar, siempre, en formato digital o informático. El perito informático podrá incluirla en papel para facilitar la labor de los juristas (abogados, fiscal y juez), pero la prueba, o una copia *forense* (1) de la misma, debe incluirse siempre en soporte informático, preferiblemente óptico o, si no hay más remedio debido al tamaño de la misma, magnético, pero detallando en el informe pericial las debidas indicaciones de que el soporte magnético, únicamente deberá conectarse siguiendo protocolos adecuados de bloqueo de escritura. Un soporte óptico es un CD-ROM o un DVD, mientras que un soporte magnético sería un disco duro o memoria USB. Cuando la prueba consista en un soporte magnético completo, es decir, un disco duro o memoria USB, será necesario, como ya se ha indicado, realizar una clonación ante notario del soporte completo y obtener el código *hash* del mismo, que será anotado en el acta notarial.

El *hash*, como ya se ha reseñado, es un elemento importantísimo, pero debe indicarse que, en los discos de unidad de estado sólido (SSD), cada vez más utilizados frente a las unidades de disco rígido (HDD), debido a su clarísima mejora en cuanto a la velocidad a la hora de acceder a los datos, el cálculo del *hash* nunca va a ser igual. Esta circunstancia es debida a la arquitectura interna de un disco SSD que, por su propia naturaleza, siempre está optimizando la información en cuanto se conecta a la corriente. La mejor opción, en este caso, es realizar una clonación del SSD fuente a un HDD destino que será utilizado como fuente y, posteriormente, clonar el nuevo HDD fuente a un HDD destino. El nuevo HDD fuente quedará en depósito notarial y el HDD destino será para que el perito informático realice su análisis forense.

En caso de que la prueba informática sea volátil, es decir, que pueda desaparecer a partir de una acción humana ejecutada en cualquier instante del tiempo (como, por ejemplo, unos comentarios o fotografías en Facebook, un comentario en Twitter, un entrada en un blog, un comentario en un foro de Internet, una noticia, etc.), la mejor opción para presentarla en un juicio es certificarla a través de un *notario digital* o, en caso de que la tecnología no lo permita, auxiliarse de un notario *clásico*, en ambos casos, siempre dirigido por las indicaciones del perito informático.

En el caso de decidirse por la utilización de *notarios digitales* o, en terminología técnica, *terceros*

construye planes para cumplir sus objetivos de negocio.



### Business Intelligence. El arte de conocer a tus clientes.

Lo importante no es que yo sepa que soy bueno, sino que lo sepan los demás. Por ello, siempre he pensado, que puedes ser jurídicamente muy bueno, pero si no tienes clientes, no eres nada.

## REDES SOCIALES & ABOGADOS



### Medición de resultados: Google Analytics y los factores a tener en cuenta

Analizar resultados de nuestro bufete de abogados virtual es una tarea que hemos de realizar con una periodicidad fija para saber cuál es el siguiente paso. Internet nos ofrece diversas herramientas que nos facilitarán estas tareas, entre las que destaca Google Analytics, y que nos ayudaran a medir nuestro trabajo y nuestros resultados.

## COLABORA CON NOSOTROS

Envíanos un artículo sobre nuevas tecnologías aplicadas al ámbito jurídico



Colaborar

Autores

Artículos

de confianza, los cuales han proliferado en los últimos años, será necesario que, como mínimo, dichos prestadores de servicios, cumplan con los requerimientos de la Directiva 2000/31/CE, del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior, así como con los requerimientos de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico. Asimismo, será muy importante también que dichas empresas hayan pasado por un proceso de madurez tecnológica y, por tanto, hayan sido certificadas, tras cumplir con las pertinentes auditorías, en los estándares ISO 9001 y familia ISO 20000 y, por último y debido a su naturaleza, también deberán cumplir con la familia de estándares ISO 27000. La mejor manera de asegurarse de que el *notario digital* o *tercero de confianza* cumple con toda la normativa técnica y legal, evitando la posible impugnación de las pruebas, es contratando un perito informático colegiado que dirija el proceso de certificación de las evidencias que van a presentarse.

En cuanto a pruebas obtenidas a partir de dispositivos móviles, es necesario realizar un volcado forense de las mismas utilizando herramientas estándar de mercado. La herramienta más conocida y potente para realizar investigaciones sobre dispositivos móviles es la Cellebrite UFED Touch, de Cellebrite, que actualmente va por su segunda edición (Touch 2), así como el software asociado a esta herramienta, denominado UFED Physical Analyzer. Esta herramienta es la utilizada tanto por el Cuerpo Nacional de Policía como por la Guardia Civil, principalmente en sus investigaciones contra el crimen organizado. Existen otras herramientas, como Oxygen, Magnet Axiom, etc., muy usadas en el entorno internacional, aunque en España se utiliza más Cellebrite, especialmente por ser la herramienta usada por las Fuerzas y Cuerpos de Seguridad del Estado, siendo necesario que cualquier laboratorio de informática forense avanzado, como el del perito que suscribe, tenga una de estas unidades para realizar periciales y contrapericiales.

Es necesario reseñar que, para realizar la adquisición de datos de un dispositivo móvil, lo que se conoce en la jerga como *extracción*, es necesario conectar el terminal, activándose por tanto su sistema operativo. Esta acción tiene una consecuencia muy importante y es que el código *hash* será distinto cada vez. El sistema operativo es el programa principal que gobierna un ordenador (o un teléfono inteligente), de tal forma que, al activarse, consulta y modifica de forma recurrente varios registros internos, por lo que el cálculo del *hash*, que engloba todos los archivos de la memoria del terminal, siempre será distinto. Por tanto, es muy recomendable realizar la *extracción* de cualquier terminal móvil ante un fedatario público, como un notario o un secretario judicial, dejando en depósito del fedatario público el terminal.

Para realizar una correcta *extracción* del terminal y, teniendo en cuenta que es necesario conectar el mismo para poder realizar la adquisición, es importantísimo aislarlo y evitar que emita o reciba cualquier tipo de comunicación, a fin de que el contenido de la evidencia permanezca invariable desde el momento en que se entregó al perito informático. La solución a este problema es utilizar un artilugio conocido como *jaula de Faraday*, que aísla al terminal de las ondas de radiofrecuencia.



### [Pablo García Mexía](#)

Abogado, Cofundador de Syntagma, Centro de estudios estratégicos.



1



### [Carlos Pérez Sanz](#)

Socio del área de Information Technology y Compliance de ECIJA.



1



### [Raúl Rubio](#)

Partner, Information Technology & Communications Baker & McKenzie



1

 Reciba LAW & TIC de forma gratuita.

Subscribirse

## CONTENIDOS RELACIONADOS

ADN Judicial

[ADN Judicial: última jurisprudencia seleccionada](#)

## ¿Quién puede realizar una pericial informática?

Para responder a esta pregunta, lo mejor es acudir a la ley. Si bien la Ingeniería Informática, como ya se ha advertido, es la única profesión de Ingeniería no regulada por el Estado, no es menos cierto que ya existen Colegios de Ingenieros e Ingenieros Técnicos en Informática en prácticamente todas las Comunidades Autónomas, existiendo sendos Consejos de Colegios nacionales que los aglutinan.

Así pues, como ya se advirtió al principio, en el artículo 340 de la Ley de Enjuiciamiento Civil se indica, textualmente, que “el perito que emita un dictamen debe ser titulado oficial en la materia objeto del dictamen”. El matiz que otorga la palabra *oficial* al conjunto es muy importante ya que, evidentemente, el cursillo que pueda impartir una academia o una asociación, como muchas que han proliferado en los últimos años, no otorga la habilitación para realizar periciales informáticas. Los únicos títulos *oficiales* de que tiene constancia este profesional que permitirían realizar periciales informáticas, son los de Ingeniero en Informática, Máster en Ingeniería Informática, Ingeniero Técnico en Informática, Grado en Ingeniería Informática, así como las diversas titulaciones de Formación Profesional en Informática, que también son títulos *oficiales*. Es recomendable que, como mínimo, el titulado sea Ingeniero Técnico en Informática o Grado en Ingeniería Informática.

Por otra parte, en el artículo 457 de la Ley de Enjuiciamiento Criminal, se establece que los titulados *oficiales* en la materia objeto del dictamen serán *peritos titulares* y, los no titulados (es decir, aquellas personas que tengan cursillos de academias o asociaciones), peritos *no titulares*, con lo que se establece una distinción importantísima en quién puede realizar una pericial de cualquier materia, en este caso, informática, con todas las garantías.

En cualquier procedimiento judicial, si el perito informático no se identifica y no manifiesta ser titulado *oficial* (ya se ha indicado que no valen cursillos), si el perito va *de parte*, sería pertinente solicitar formalmente la *tacha* del informe y, si el perito es *judicial*, solicitar incluso la *recusación* del mismo.

Para garantizar inequívocamente que el perito informático es titulado *oficial* y, por tanto, *perito titular*, la mejor opción es acudir al Colegio Profesional de Ingenieros en Informática de la Comunidad Autónoma en la que se encuentre o, si se dirige directamente al profesional, solicitarle su carné de colegiado y observar, de forma fehaciente, que la palabra COLEGIADO aparece en el mismo, y no la palabra *asociado*, existiendo muchos que manifiestan estar colegiados cuando en realidad se hallan asociados en alguna de las múltiples asociaciones que han aparecido últimamente y que admiten a todo tipo de personas sin ningún filtro. La única asociación nacional activa, que realiza filtro de titulación oficial universitaria de Ingeniería Informática, es la histórica ALI (Asociación de Titulados en Ingeniería en Informática), creada a principios de los años 1980 e impulsora de la mayoría de los Colegios existentes en las Comunidades Autónomas, así como de los Consejos de Colegios.

### Cumplimiento de la legalidad por parte del perito informático

SELECCIONADA

CGPJ

El 64% de los miembros de la Carrera Judicial son mujeres menores de 50 años

Ministerio de Empleo y Seguridad Social

La reforma laboral de 2012 en España

Por último, es muy importante reseñar que, el perito informático, debe estar siempre sometido al imperio de la ley y provisto de un seguro de responsabilidad civil, que le permita afrontar cualquier tipo de error que pueda cometer en el ejercicio de su profesión. Este profesional tiene constancia de que, en los últimos tiempos, se están incoando procedimientos penales contra peritos informáticos por no cumplir con la legalidad (de forma consciente o inconsciente), especialmente por violar un derecho fundamental como el secreto de las comunicaciones u, otro derecho de rango un poco menor, pero también muy importante, como el derecho a la propia intimidad. Ni que decir tiene que cualquier prueba obtenida por un perito informático debe ser lícita y ajustarse a Derecho, razón por la cual serán anuladas por el juzgador todas aquellas pruebas que no cumplan con estas premisas fundamentales.

(1) Del latín *forensis*, relativo al *Foro*. En la Antigua Roma, los asuntos públicos y que afectaban al pueblo y al mismo Estado, se debatían en el *Foro*. Por tanto, *forense* significa *público*. Un procedimiento *forense* es un procedimiento *público*, es decir, *repetible*, de tal forma que, tras practicar un análisis a una evidencia, con los mismos condicionantes, deben obtenerse siempre los mismos resultados y conclusiones.

Lefebvre - EL Derecho no comparte necesariamente ni se responsabiliza de las opiniones expresadas por los autores o colaboradores de esta publicación

tesauro

[Internet](#), [Tecnología](#), [Redes Sociales](#), [Juez](#)

Comentar



## 0 Comentarios

[Escribe tu comentario](#)

## Añadir comentario

\* Nombre

Comentario

\* Correo electrónico

(\*) Datos obligatorios

He leído y acepto las condiciones de la [Política de Privacidad](#) y el [Aviso Legal](#)

Enviar



- [Contacto](#)
- [Mapa Web](#)
- [Tesauro](#)
- [Hemeroteca](#)

- [RSS](#)
- [Aviso Legal](#)
- [Condiciones de compra](#)
- [Política de privacidad](#)

- [Publicidad](#)
- [Widget de noticias](#)
- [Programa de afiliados](#)

**Otros sites:**

- [Francis Lefebvre](#)
- [Espacio Asesoría](#)
- [El Derecho Local](#)

**Atención al cliente:** De lunes a viernes de 9 a 20 horas ininterrumpidamente. Tel 902 44 33 55 Fax. 915 78 16 17

© Lefebvre – El Derecho S.A.