

---

# FALLAS Y FALENCIAS DE LAS PERICIAS INFORMÁTICAS Y SU IMPACTO EN EL DEBIDO PROCESO

**Dr. José Luis Tamayo Rodríguez**

*Doctor en Ciencias, Mención Derecho (UCV) · Especialista en Derecho Digital · Fundador de Academia SOMA · INPREABOGADO N° 17.744*

Publicado originalmente: 26 de enero de 2023 · Versión ampliada y revisada: julio de 2026

---

## Resumen

El presente trabajo analiza las fallas y falencias más frecuentes que exhiben los dictámenes periciales informáticos en la práctica forense actual, con especial énfasis en las pericias de vaciado de contenido de teléfonos inteligentes, y su impacto directo sobre el debido proceso y el derecho a la defensa. Se identifican los ocho lineamientos básicos que debe satisfacer todo peritaje informático para superar el denominado juicio de fiabilidad, se examina el rol del principio de mismidad y de la cadena de custodia digital como garantes de dicho juicio, y se ofrecen criterios jurisprudenciales y recomendaciones prácticas para que jueces y abogados litigantes puedan valorar e impugnar con rigor técnico las conclusiones periciales, evitando que estas se conviertan en una "palabra sagrada" aceptada de manera acrítica.

---

## Palabras clave

Pericia informática. Dictamen pericial. Vaciado de contenido. Juicio de fiabilidad. Cadena de custodia digital. Principio de mismidad. Debido proceso.

---

## Abstract

This paper analyzes the most frequent flaws and shortcomings found in computer forensic expert reports in current forensic practice, with special emphasis on smartphone content-extraction examinations, and their direct impact on due process and the right to a defense. It identifies the eight basic guidelines that every computer forensic examination must satisfy to pass the so-called reliability test, examines the role of the sameness principle and the digital chain of custody as guarantors of that test, and offers case-law criteria and practical recommendations so that judges and trial lawyers can rigorously assess and challenge expert conclusions, preventing them from being accepted uncritically as a "sacred word."

---

## Keywords

Computer forensic examination. Expert report. Content extraction. Reliability test. Digital chain of custody. Sameness principle. Due process.

---

## Sumario

- 1. Introducción
- 2. La pericia informática como "prueba reina": alcance y riesgos
- 3. El juicio de fiabilidad, el principio de mismidad y la cadena de custodia digital
- 4. Los ocho lineamientos básicos de todo peritaje informático
- 5. El carácter especial de la evidencia digital
- 6. Criterios jurisprudenciales para la valoración de la pericia
- 7. Recomendaciones para el abogado litigante
- 8. Conclusiones
- Referencias

## 1. Introducción

---

Merced de la disrupción de las evidencias digitales y pruebas electrónicas de toda índole en los procesos judiciales, sean estos de naturaleza penal, de violencia intrafamiliar, civil, laboral, administrativa, etc., la Pericia Informática o Dictamen Pericial Informático se ha venido erigiendo paulatinamente en la "prueba reina" dirimente de la controversia o pleito judicial de que se trate a favor de una de las partes en conflicto.

En materia penal, las denominadas pericias de vaciado de contenido de los teléfonos celulares inteligentes o smartphones, a través de las cuales se obtienen los datos y registros en ellos contenidos, en especial los denominados "chats de WhatsApp", incluidos sus "pantallazos", son las que generalmente determinan la absolución o condena del imputado o acusado de la comisión de un determinado delito, sobre todo en los denominados "cyberdelitos" o delitos informáticos.

En la práctica forense actual, las conclusiones a las cuales arriban los peritos informáticos en sus respectivos dictámenes periciales, complementadas con las preguntas y repreguntas que se les hacen en los correspondientes interrogatorios y contrainterrogatorios durante el desarrollo del juicio oral y público, se han convertido en una suerte de "palabra sagrada" a la que el juez asigna, casi de manera automática y sin mayores consideraciones, absoluto y pleno valor probatorio al momento de dictar sentencia, a lo que mucho contribuye la pasividad de las partes en la aceptación tácita de esa "palabra sagrada" por carecer de las herramientas y conocimientos básicos necesarios para increpar y cuestionar con efectividad el dicho del perito.

El presente trabajo se propone, en primer lugar, identificar y sistematizar las fallas y falencias más recurrentes de los dictámenes periciales informáticos; en segundo lugar, precisar los lineamientos técnicos mínimos que todo peritaje debe satisfacer para superar el juicio de fiabilidad; y, en tercer lugar, ofrecer criterios jurisprudenciales y pautas prácticas que permitan a jueces y litigantes ejercer un control de calidad efectivo sobre esta prueba, en resguardo del debido proceso y del derecho a la defensa.

## 2. La pericia informática como "prueba reina": alcance y riesgos

---

En los últimos tiempos han proliferado de manera exponencial las condenas dictadas sobre la base de las informaciones extraídas merced de un deplorable y deficiente "vaciado de contenido" realizado a los teléfonos

celulares ocupados o aportados por las partes durante la fase de investigación, que los peritos informáticos plasman en sus dictámenes, sin advertir las partes e incluso el propio juez las grandes y notorias fallas y falencias que estos presentan. Entre ellas, cabe destacar:

- La falta de análisis descriptivo y detallado de las evidencias digitales recibidas.
- La falta de explicación detallada y precisa acerca del método utilizado para el examen de la evidencia y de las técnicas empleadas para la extracción de la información digital.
- La falta de descripción de las herramientas o equipos utilizados para ello, sus principales características y funcionalidades.
- La no incorporación del dispositivo electrónico en el cual ha de constar la información clonada extraída de la evidencia examinada, con miras a garantizar la repetibilidad de los análisis realizados y constatar la verificabilidad y confiabilidad de los resultados obtenidos y las subsiguientes conclusiones.

Todo lo anterior incide en que la pericia realizada no supere el denominado juicio de fiabilidad, referido a la posibilidad de poderse comprobar la autenticidad e integridad de los datos y registros digitales obtenidos y su no manipulación.

La ausencia de esta información —vital para la eficacia probatoria de la pericia y del dicho del experto que la suscribe— y que ha de ser plasmada obligatoriamente en el texto del dictamen pericial en aras del cumplimiento de los preceptos de "inalterabilidad, conservación y posibilidad de repetición de los resultados", que garantizan el derecho a la defensa de la parte contra la cual obran los resultados de la pericia, hace poco fiables y carentes de real sustento técnico las conclusiones obtenidas. No obstante, en la práctica se toman las más de las veces como "plena prueba" de la información extraída del dispositivo electrónico peritado, y "santa palabra" el dicho de los peritos vertido de viva voz en el juicio.

De hecho, la posibilidad de repetición de la prueba pericial es lo que permite su efectiva contradicción, y para ello es preciso que el perito clone la información y la almacene en un dispositivo electrónico distinto (pendrive, CD, memoria externa, etc.), obteniendo previamente su código hash. Sin embargo, esto rara vez ocurre en la práctica forense.

### **3. El juicio de fiabilidad, el principio de mismidad y la cadena de custodia digital**

---

Todo lo anterior debe examinarse sin perder de vista la contaminación previa que puede haber sufrido —y que generalmente sufre en la práctica forense— la evidencia digital por el incumplimiento de los protocolos de actuación indispensables por parte de los funcionarios o personas responsables de la cadena de custodia de la evidencia, que es la garante del juicio de fiabilidad, desde el momento de su hallazgo o descubrimiento hasta el momento en que es recibida en el laboratorio del perito. Con ello, el principio de mismidad queda seriamente comprometido merced de la ruptura de dicha cadena, y, por ende, la pericia resulta ineficaz en principio para formar convencimiento válido en el juez que en su momento ha de apreciarla y valorarla.

El principio de mismidad —que hemos desarrollado con mayor extensión en trabajos anteriores sobre el anclaje normativo del código hash— exige que el documento, archivo o evidencia digital que se presenta en juicio sea exactamente el mismo que fue originalmente recolectado o generado, sin alteraciones de forma, contenido,

metadatos o contexto técnico. El cálculo y registro del código hash, antes y después de cada intervención pericial, es precisamente el mecanismo técnico que permite verificar objetivamente el cumplimiento de este principio; su ausencia en el dictamen es, por sí sola, un indicio grave de falta de rigor metodológico.

## 4. Los ocho lineamientos básicos de todo peritaje informático

---

La deficiencia del grueso de los Dictámenes Periciales Informáticos es fácilmente constatable por la carencia de uno o varios de los siguientes lineamientos básicos que debe cumplir todo peritaje informático:

1. **Verificabilidad.** Se debe poder comprobar la veracidad de las conclusiones extraídas a partir de la realización del análisis pericial. Un dictamen que no permita a un tercero —perito de contraparte, tribunal o auditor— constatar de forma independiente cómo se llegó a cada conclusión, incumple este requisito.
2. **Reproducibilidad.** Se deben poder reproducir en todo momento las pruebas realizadas durante el peritaje, de manera que, aplicando la misma metodología sobre la misma evidencia (o su copia forense certificada), cualquier otro experto obtenga resultados equivalentes.
3. **Documentabilidad.** Todos los exámenes y análisis realizados por el experto deben quedar debidamente explanados y detallados en el dictamen pericial: herramientas, versiones de software, comandos ejecutados, capturas de pantalla del proceso y bitácora cronológica de actuaciones.
4. **Independencia.** Las conclusiones obtenidas deben ser las mismas, independientemente de la persona que realice el proceso y de la metodología utilizada, siempre que ambas sean técnicamente válidas y se apliquen sobre la misma evidencia íntegra.
5. **Autenticidad.** El dictamen debe ser susceptible de verificación para constatar su autenticidad y que no ha sufrido manipulación alguna, garantizando y asegurando para ello su total integridad, típicamente mediante firma electrónica del perito y códigos hash de los anexos digitales.
6. **Compleitud.** La pericia debe ser completa desde un punto de vista objetivo y técnico, sin valoraciones personales ni prejuicios, cubriendo todos los extremos relevantes para el objeto de la experticia, incluyendo los hallazgos que pudieran no favorecer a la parte promovente.
7. **Credibilidad.** El dictamen debe ser comprensible por los órganos judiciales profanos en la materia, lo que exige del perito un ejercicio de traducción del lenguaje técnico al lenguaje jurídico-llano, sin sacrificar precisión científica.
8. **Confiabilidad.** Las técnicas utilizadas para su obtención no deben generar ninguna duda sobre su veracidad y autenticidad, debiendo corresponder a estándares reconocidos por la comunidad forense internacional (ISO/IEC 27037, ISO/IEC 27042, entre otros).

## 5. El carácter especial de la evidencia digital

---

Téngase en cuenta que la pericia informática ostenta un carácter especial, derivado de las características particulares de las evidencias digitales, dado su carácter intangible (el soporte que las contiene es digital), su volatilidad y facilidad de clonación y alteración, que las distingue del resto de las evidencias (físicas) utilizadas en otro tipo de pericias y, en particular, de las evidencias documentales tradicionales, que tienen un soporte

físico (papel) que las hace tangibles. De allí que las exigencias de cumplimiento de los protocolos mínimos de la cadena de custodia de la evidencia digital sean mucho mayores que las de la evidencia material o física.

## 6. Criterios jurisprudenciales para la valoración de la pericia

---

A la hora de valorar la prueba, muchos jueces no toman en consideración extremos claves —que han venido siendo establecidos jurisprudencialmente, sobre todo en España—, que resultan determinantes para aceptar o no las conclusiones de la pericia, tales como:

*La dificultad de la materia sobre la que verse el dictamen, la preparación técnica de los peritos, su especialización, el origen de la elección del perito, su buena fe, las características técnicas del dictamen, la firmeza de los principios y leyes científicas aplicados, los antecedentes del informe (reconocimientos, períodos de observación, pruebas técnicas realizadas, número y calidad de los dictámenes obrantes en los autos, concordancia o disconformidad entre ellos, resultado de la valoración de las otras pruebas practicadas, las propias observaciones del Tribunal, etc.). (Sentencia 1102/2007, del 21 de diciembre, del Tribunal Supremo Español).*

No tomar en cuenta esos extremos claves al momento de dictar sentencia, al igual que los aludidos lineamientos básicos que debe cumplir todo peritaje informático, y, pese a ello, aceptar como ciertas y valederas las conclusiones que este arroja, violenta el debido proceso y el derecho a la defensa de la parte contra quien obren, por no estar en presencia de un juicio llevado a cabo "con todas las garantías".

Vale la pena anotar, a título comparativo, que el sistema anglosajón enfrenta un problema análogo a través del denominado estándar Daubert (Daubert v. Merrell Dow Pharmaceuticals, 509 U.S. 579, 1993), que exige al juez actuar como "gatekeeper" o guardián de la fiabilidad científica de toda prueba pericial, valorando, entre otros factores, si la técnica ha sido sometida a verificación empírica, si ha sido objeto de revisión por pares y publicación, su tasa de error conocida o potencial, y su grado de aceptación en la comunidad científica pertinente. Estos factores guardan una correspondencia notable con los ocho lineamientos antes enunciados, lo que confirma que no se trata de exigencias caprichosas del foro latinoamericano, sino de estándares de fiabilidad científica reconocidos transversalmente en el derecho probatorio comparado.

## 7. Recomendaciones para el abogado litigante

---

De cara a la contradicción efectiva de una pericia informática deficiente, se sugiere al abogado litigante:

- a) Verificar, como primer paso, si el dictamen incorpora el código hash de la evidencia original y de la copia forense analizada, tanto antes como después del examen pericial.
- b) Constatar si el dictamen describe con precisión la cadena de custodia de la evidencia desde su recolección hasta su análisis, identificando a cada custodio y el momento de cada traslado.
- c) Confrontar al perito, en el interrogatorio o contrainterrogatorio, sobre cada uno de los ocho lineamientos básicos (verificabilidad, reproducibilidad, documentabilidad, independencia, autenticidad, completitud, credibilidad y confiabilidad), exigiendo respuestas concretas y no evasivas.
- d) Solicitar, cuando sea procedente, una contrapericia o experticia de parte que permita reproducir el análisis sobre la copia forense certificada, ejerciendo así el derecho a la repetibilidad de la prueba.

e) Invocar expresamente ante el tribunal los criterios jurisprudenciales de valoración de la prueba pericial (como los de la STS 1102/2007), para que el juez no acepte las conclusiones del perito de manera acrítica o automática.

## 8. Conclusiones

---

9. La pericia informática se ha erigido en la práctica forense actual como una auténtica "prueba reina", cuyo peso decisorio exige un control de calidad técnico y jurídico proporcional a su importancia.
10. Las fallas más recurrentes en los dictámenes periciales informáticos son la falta de análisis descriptivo detallado, la ausencia de explicación metodológica, la falta de descripción de herramientas empleadas y la no incorporación del soporte con la información clonada, todo lo cual impide superar el juicio de fiabilidad.
11. El principio de mismidad y la cadena de custodia digital son garantes indispensables del juicio de fiabilidad; su ruptura compromete la eficacia probatoria de la pericia con independencia de la calidad técnica del análisis posterior.
12. Todo peritaje informático debe satisfacer ocho lineamientos básicos —verificabilidad, reproducibilidad, documentabilidad, independencia, autenticidad, completitud, credibilidad y confiabilidad— cuya ausencia, parcial o total, debe ser advertida y objetada por las partes.
13. El carácter intangible, volátil y fácilmente alterable de la evidencia digital exige protocolos de cadena de custodia más exigentes que los aplicables a la evidencia física tradicional.
14. Los criterios jurisprudenciales de valoración de la prueba pericial —desarrollados en España y con equivalentes funcionales como el estándar Daubert en el derecho anglosajón— constituyen una herramienta valiosa, y hoy insuficientemente utilizada, para que jueces y litigantes ejerzan un control de fiabilidad riguroso sobre la pericia informática.
15. Aceptar de manera acrítica y automática las conclusiones de una pericia informática deficiente, sin verificar el cumplimiento de los lineamientos técnicos y los criterios jurisprudenciales aplicables, vulnera el debido proceso y el derecho a la defensa de la parte contra quien dicha pericia obra.

## Referencias

---

- Tribunal Supremo de España. Sentencia 1102/2007, de 21 de diciembre (Sala de lo Penal), sobre criterios de valoración de la prueba pericial.
- Daubert v. Merrell Dow Pharmaceuticals, Inc., 509 U.S. 579 (1993), Corte Suprema de los Estados Unidos — estándar de admisibilidad de prueba pericial científica.
- ISO/IEC 27037:2012 — Guidelines for identification, collection, acquisition and preservation of digital evidence.
- ISO/IEC 27042:2015 — Guidelines for the analysis and interpretation of digital evidence.
- Tamayo Rodríguez, José Luis. El Anclaje Normativo del Hash en México y el Rol del Perito Informático en el Análisis de la Evidencia Digital (2025), sobre el principio de mismidad y la función hash como garantes de la cadena de custodia digital.