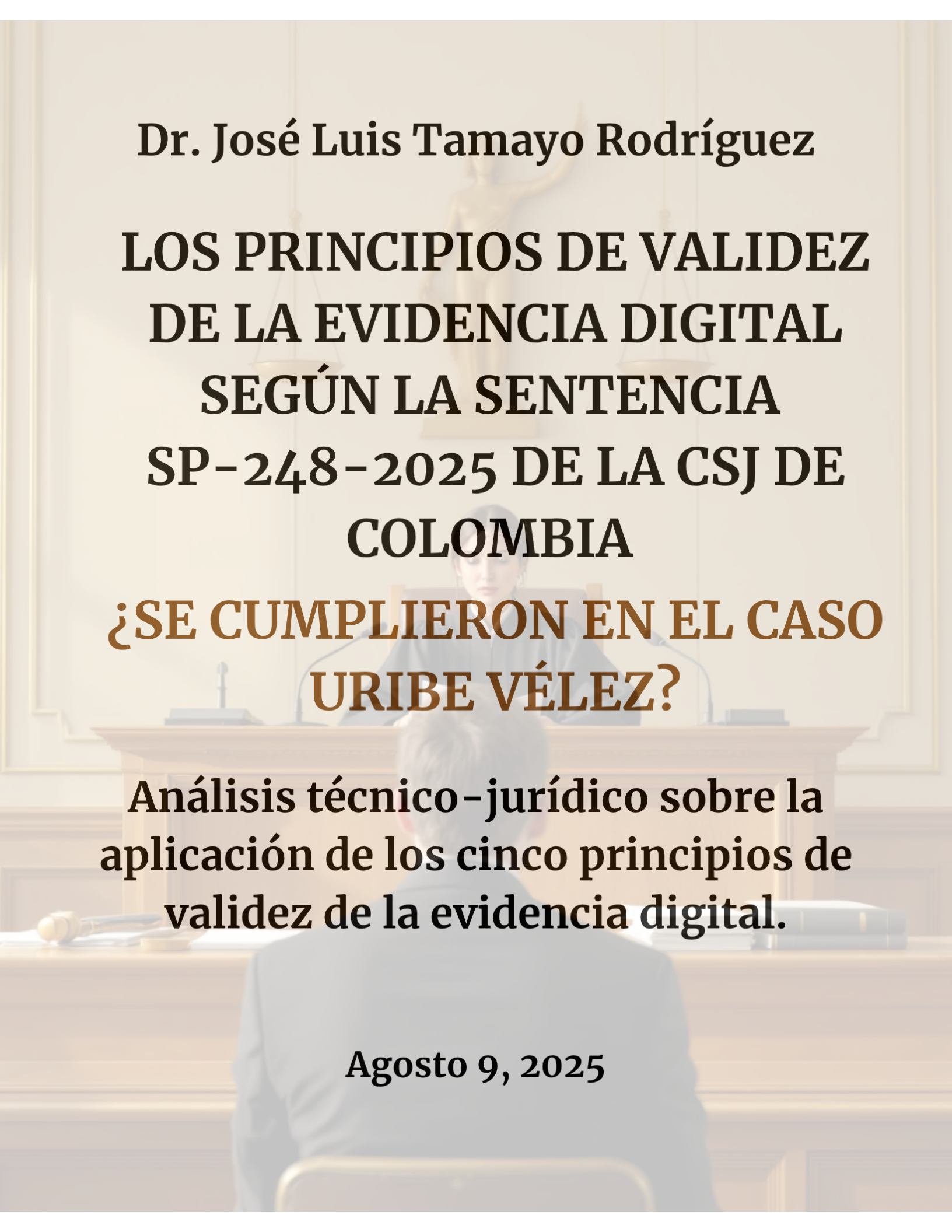




**Dr. José Luis Tamayo Rodríguez**

**LOS PRINCIPIOS DE VALIDEZ  
DE LA EVIDENCIA DIGITAL  
SEGÚN LA SENTENCIA  
SP-248-2025 DE LA CSJ DE  
COLOMBIA**

**¿SE CUMPLIERON EN EL CASO  
URIBE VÉLEZ?**

**Análisis técnico-jurídico sobre la  
aplicación de los cinco principios de  
validez de la evidencia digital.**

**Agosto 9, 2025**

# LOS PRINCIPIOS DE VALIDEZ DE LA EVIDENCIA DIGITAL SEGÚN LA SENTENCIA SP-248-2025 DE LA CSJ DE COLOMBIA ¿SE CUMPLIERON EN EL CASO URIBE VÉLEZ?

Dr. José Luis Tamayo Rodríguez<sup>1</sup>

Agosto 9, 2025

## RESUMEN

Este artículo realiza un análisis crítico de la evidencia digital utilizada en el caso Álvaro Uribe Vélez, tomando como base la sentencia SP-248-205 de la Sala de Casación Penal de la Corte Suprema de Justicia de Colombia. A partir de este fallo, se examina el cumplimiento —o la ausencia— de los cinco principios esenciales para la validez de la evidencia digital: autenticidad, integridad, confiabilidad, accesibilidad y repetibilidad. Se incorporan estándares internacionales como las Normas ISO/IEC 27037:2012 y 27042:2015, así como las nociones de *sana crítica digital* y *máximas de experiencia digital*, advirtiendo sobre los riesgos de valorar pruebas electrónicas sin garantizar su trazabilidad técnica desde la fuente primaria.

## INTRODUCCIÓN

La sentencia SP-248-2025 de la Sala Penal de la Corte Suprema de Justicia de Colombia estableció cinco principios fundamentales para valorar la autenticidad y eficacia probatoria de la evidencia digital: **confiabilidad, integridad, accesibilidad, auditabilidad y repetibilidad**.

Estos principios se sustentan en estándares internacionales como las **Normas ISO/IEC 27037:2012 y 27042:2015**<sup>2</sup>, que a su vez sirven de base a la **Cartilla de Evidencia Digital** de la rama judicial colombiana.<sup>3</sup>

---

<sup>1</sup> Abogado binacional, venezolano, nacido en Caracas (1958), egresado de la Universidad Central de Venezuela en 1981, con reválida en México. Doctor en Derecho y profesor de pregrado y postgrado de Derecho penal y procesal penal en la misma Universidad. Exjuez asociado en los Tribunales penales, de primera y segunda instancia, en Caracas (1992-1999). Abogado litigante con cuarenta y cuatro años de experiencia. Especializado en Derecho Digital y Pruebas electrónicas. Autor de nueve libros y los e-book “*Pruebas Electrónicas y Código hash*” (2024). “*Pantallazos de WhatsApp: todo lo que el litigante debe saber*” (2025) y “*La prueba electrónica híbrida*” (2025).

<sup>2</sup>[https://escuelajudicial.ramajudicial.gov.co/sites/default/files/22\\_cartilla\\_evidencia\\_digital\\_-\\_procedimientos\\_tecnicos.pdf](https://escuelajudicial.ramajudicial.gov.co/sites/default/files/22_cartilla_evidencia_digital_-_procedimientos_tecnicos.pdf)

<sup>3</sup> Las Normas ISO/IEC, emitidas conjuntamente por la *International Organization for Standardization* (ISO) y la *International Electrotechnical Commission* (IEC), establecen estándares internacionales en materia tecnológica. La **ISO/IEC 27037:2012** fija directrices para la identificación, recolección, adquisición y preservación de la evidencia digital, garantizando su integridad y autenticidad. La **ISO/IEC 27042:2015** regula el análisis de dicha evidencia y su presentación en procedimientos judiciales, asegurando su valor probatorio.

En el caso Uribe Vélez, tanto en las **grabaciones obtenidas del sistema de interceptación** como en las **grabaciones de los relojes espía**, se advierten —por lo que se desprende de la sentencia y de lo expuesto en audiencia— graves vacíos técnicos que vulneran estos principios esenciales. Veamos.

## DESARROLLO

### 1. Confiabilidad

La sentencia SP-248-2025 exige que la obtención, preservación y análisis de la evidencia digital se realicen mediante **procedimientos fiables y acreditados por personal idóneo**, incluyendo la creación de **imagen forense** y cálculo del **hash** tanto del original como de la copia.<sup>4</sup>

#### En el caso Uribe Vélez:

- **Interceptaciones:**

Por lo que se desprende de la sentencia, no consta que las grabaciones originales —es decir, las obtenidas a través del sistema institucional de interceptaciones— hayan sido **extraídas directamente del servidor** de dicho sistema, ni que se haya generado el valor hash de cada grabación desde esa **fuentes primaria u original**.<sup>5</sup> Tampoco se acredita que el hash de sus respectivas imágenes forenses coincidiera con el de cada grabación original.

Todo indica que el cálculo del hash se realizó únicamente sobre las “**copias espejo**” mencionadas en la sentencia (aunque esta no lo expresa de forma explícita), las cuales fueron grabadas en CDs o DVDs por dos ingenieros informáticos asignados para esa labor. Sin embargo, estos ingenieros no declararon en el juicio oral.

---

<sup>4</sup> En la Sentencia SP248-2025, se lee textualmente: “**i) Confiabilidad:** En la forma como se ha generado, extraído, archivado o comunicado el documento, registro, información o mensaje de datos, a partir de procedimientos fiables y acreditados por el área de conocimiento específico. Preferiblemente, por personal capacitado e idóneo en el proceso de recolección y análisis de la evidencia digital.- En este punto, cobran relevancia conceptos como el de imagen forense digital, para lo cual se suele emplear un bloqueador de lecto/escritura o White Blockers, así como programas o software para el copiado de la información y la generación de la imagen, que será almacenada en un disco de destino u otro dispositivo de almacenamiento, especialmente destinado a ello”.

<sup>5</sup> Como bien se ha dicho, el principio de integridad digital exige que cualquier tratamiento pericial de los datos informáticos se realice directamente sobre su fuente primaria. Esta no es una exigencia meramente técnica, sino una garantía de legalidad y confiabilidad. Por otra parte, y como bien se ha sostenido mente, una evidencia almacenada en una unidad óptica (CD, DVD) sin constancia de imagen forense ni hash del contenido original carece de toda garantía pericial. Su análisis compromete la validez del dictamen.

Para que dichas “copias espejo” pudieran considerarse técnicamente confiables, era indispensable dejar constancia de la coincidencia de los valores hash entre las copias y las grabaciones originales.

Este extremo no fue acreditado en juicio, precisamente porque los ingenieros responsables de las copias no comparecieron a declarar, lo que impidió verificar **qué procedimientos y protocolos forenses emplearon**, algo indispensable para acreditar la confiabilidad de las evidencias (grabaciones).

En consecuencia, todo parece indicar que las grabaciones incorporadas al juicio mediante “copias espejo”, carecen de trazabilidad que permita a las partes verificar su correspondencia exacta con los originales.

- **Relojes espía:**

Las grabaciones fueron extraídas por una persona que no era perito (Deyanira) y entregadas en una memoria USB en el año 2018. No se practicó —o al menos no se acredita en la sentencia— una pericia informática directa sobre el reloj espía para generar su imagen forense y verificar la coincidencia de valores hash.

Tanto la Corte Suprema de Justicia como la Fiscalía se conformaron con recibir pura y simplemente una memoria USB y omitieron cumplir con la obligación de acreditar la **fuentes original** de las grabaciones mediante un peritaje forense del propio reloj espía en ese mismo año 2018. La extracción inicial fue realizada de forma manual por Deyanira, lo que hace imposible acreditar la confiabilidad técnica de tales archivos.

La situación se **agrava** aún más si se considera que la fuente original de las grabaciones —el reloj espía— permaneció durante cinco años en poder de Deyanira, de sus abogados o de otras personas no identificadas, pues no fue sino hasta 2023 cuando dicho dispositivo (o los dispositivos) se incorporó formalmente al proceso.

Lo **más grave** es que, incluso en ese momento (2023), no se practicó un peritaje forense para extraer las grabaciones directamente del dispositivo, calcular su código hash, generar las imágenes forenses con su respectivo hash y, posteriormente, comparar las grabaciones obtenidas por el perito informático con aquellas extraídas y copiadas por Deyanira en 2018.

De manera que todo conduce a afirmar que las experticias forenses de la Fiscalía se realizaron exclusivamente sobre los archivos *cumple.avi* y los archivos *red-alpiso0003.avi* y *red-alpiso004.avi*, entregados por Deyanira, el primero el 26 de febrero de 2018 y los otros dos el 2 de abril de 2018, lo que contraviene el artículo 277 del Código de Procedimiento Penal colombiano, que impone a la Fiscalía la carga de demostrar la autenticidad del elemento probatorio cuando --como ocurre

en este caso-- los elementos probatorios entregados (tres grabaciones en formatos .avi<sup>6</sup>) carece de cadena de custodia por provenir de un particular.

## 2. Integralidad

La integralidad implica que la evidencia se presente en las mismas condiciones en que fue obtenida, preservando su estado original y evitando cualquier alteración. La sentencia SP-248-2025 indica que esto se garantiza comparando los **códigos o valores hash** del original y de la copia.<sup>7</sup>

### En el caso Uribe Vélez:

- **Intercepciones:** Al parecer, no se generaron ni documentaron los códigos hash de las grabaciones originales obtenidas directamente desde el sistema de interceptación, ni se efectuó su comparación con los hash de los archivos contenidos en los soportes secundarios (CDs y DVDs) que, según se afirma, corresponden a copias espejo. Esta omisión impide verificar la autenticidad e integridad de dichas copias respecto de los originals.
- **Relojes espía:** No se registró el hash de los archivos contenidos en los dos relojes espía ni tampoco el de la copia entregada; esta fue creada por una persona no perito, lo que incrementa el riesgo de alteraciones.

La ausencia de estos pasos rompe la cadena de integridad de evidencia y deja abierta la posibilidad de manipulación.

## 3. Accesibilidad

---

<sup>6</sup> El formato **.avi** (*Audio Video Interleave*) es un contenedor de audio y video ampliamente utilizado por dispositivos de grabación, incluidos algunos relojes espía. Sin embargo, la sola extensión del archivo no acredita su origen ni su integridad, lo que requiere un análisis forense de metadatos y parámetros técnicos propios del dispositivo.

<sup>7</sup> En la sentencia SP-248, se lee textualmente: **“ii) Integralidad e inalterabilidad:** Referida a que la información sea presentada en su forma original, en las mismas condiciones en que fue obtenida, extraída, en forma completa e inalterada. Lo que también implica que sea conservada o preservada en esa misma condición, evitando su deterioro o destrucción.- En este aparte, se tratan conceptos como el de certificados digitales, de que trata el artículo 30 de la Ley 527 de 1999, así como el numeral 3º del artículo 426 de la Ley 906 de 2004, como método de autenticidad e identificación del documento.- Asimismo, los **códigos o valores hash**, han sido entendidos como una identificación única o huella digital de cada archivo. Para ello, en términos generales, mediante un software que emplea algoritmos, se toma un archivo, una carpeta o dispositivo de almacenamiento como entrada, para generar un hash o salida, que corresponde a un resumen único de la información ingresada o código alfanumérico.- Este método permite: «estar seguros de que algunas comunicaciones o archivos no fueron alterados de alguna forma, se pueden examinar los valores hash creados antes y después de la transmisión de los datos. Si los dos valores hash son idénticos, significa que no ha habido ninguna alteración».

La sentencia SP-248-2025 señala que la evidencia digital debe ser accesible para posteriores verificaciones, incluyendo sus metadatos (fecha, hora, ubicación, dispositivo, etc.).<sup>8</sup>

### En el caso Uribe Vélez:

- **Interceptaciones:** La defensa no tuvo acceso al servidor original ni a las grabaciones en su formato primario u original, lo que impidió toda verificación técnica independiente.

Y tal parece que la Fiscalía tampoco se preocupó por el cumplimiento riguroso de los protocolos forenses, en el sentido de exigir a los ingenieros encargados de la extracción de las grabaciones y realizar sus “copias espejo”, que se realizaran las imágenes forense de cada grabación original y que se hicieran constar los hashes de la grabación original y de su respectiva imagen. De allí que, sin imagen forense debidamente certificada con hash, no es posible tener acceso a una verificación posterior.

- **Relojes espía:** El dispositivo (o los dispositivos) fue presentado inservible en 2023, cinco años después, imposibilitando cualquier acceso a la fuente original y sus metadatos.

Esta falta de accesibilidad imposibilitó materialmente que la defensa ejerciera plenamente el principio de contradicción. De hecho, el perito de la defensa dejó constancia expresa de la imposibilidad de acceso a la fuente original de la grabación (relojes espía), dejando constancia de múltiples irregularidades relacionadas con las grabaciones peritadas por él provenientes de los relojes espías y extraídas por Deyanira.

## 4. Auditabilidad

---

<sup>8</sup> En la sentencia SP-248-2025, se lee textualmente: “**iii) Accesibilidad:** En cuanto se debe garantizar el acceso para posteriores consultas de los documentos, registros, informaciones o mensajes de datos extraídas, así como su origen y destino, fecha y hora de creación, en que fue enviado o recibido el mensaje o producido el documento, entre otros, o metadatos. Por ello, de requerirse su reproducción esta debe corresponder, con exactitud, al momento en que fue generado el documento, enviado o recibido el mensaje de datos.- En ese sentido, conforme a la evolución constante de la tecnología, es claro que otros criterios han sido reconocidos en parámetros internacionales, como los previstos en la norma ISO/IEC 27037 del 2012, expedida por la Organización Internacional de Estandarización (ISO) y la Comisión Internacional Electrotécnica (IEC), para el manejo de la evidencia digital y que resultan atendibles, a manera de orientación, para establecer el valor probatorio de los datos contenidos en recursos electrónicos o digitales, idóneos para acreditar un hecho jurídicamente relevante. Estos, interpretados de la norma en cita, son:...” (Auditabilidad y Repetibilidad).” (Nuestro el paréntesis).

La auditabilidad exige que todo el proceso de obtención y análisis esté documentado, de manera que pueda ser revisado por peritos y autoridades judiciales.<sup>9</sup>

#### En el caso Uribe Vélez:

- **Interceptaciones:** No se acreditó en el juicio oral y público un registro detallado de los pasos seguidos por los dos ingenieros que hicieron las “copia espejo”, ni tampoco se acreditó si los hashes mencionados en la sentencia corresponden a cada una de las grabaciones interceptadas y copiadas por dichos ingenieros. En la sentencia solo se hace mención a los “códigos de archivos hash”, sin conocerse a ciencia cierta a cuáles códigos hash hace referencia la juzgadora.
- **Relojes espía:** La extracción por parte de una persona no perito no fue acompañada de ningún registro técnico verificable, ni en el 2018 ni el 2023. La imposibilidad de auditar estos procesos impide confirmar que se cumplieron las buenas prácticas forenses.

#### 5. Repetibilidad

La repetibilidad significa que otro perito, aplicando los mismos métodos y condiciones, obtendría idénticos resultados.<sup>10</sup>

#### En el caso Uribe Vélez:

- **Interceptaciones:** Sin el hash de la fuente primaria u original ni la documentación del procedimiento, no es posible reproducir la pericia y verificar si los resultados coincidirían.
- **Relojes espía:** En estos, la ausencia de análisis directo sobre el dispositivo original impide cualquier intento de repetición.

### CONCLUSIÓN

Conforme a la sentencia SP-248-2025, a las normas ISO/IEC 27037-2012 y 27042-2015, y a la Cartilla de Evidencia Digital, la ausencia de análisis forense de la fuente primaria u original, la falta de hashes y la omisión de testimonios clave de los peritos extractores constituyen **graves deficiencias técnicas**. Tales vacíos debieron

---

<sup>9</sup> En la sentencia SP-248-2025, se lee textualmente: “**iv) Auditabilidad:** En cuanto el proceso de recolección de la evidencia digital, así como su posterior análisis debe estar documentado y justificado, con el fin de que pueda ser revisado, no solo por las partes sino por la autoridad judicial”.

<sup>10</sup> En la sentencia SP-248-2025, se lee textualmente: “**v) Repetibilidad:** En el sentido de garantizar que, si un investigador o perito utiliza los mismos métodos y condiciones para la obtención y análisis de una evidencia digital, empleado por otro, obtendrá el mismo resultado”.

disminuir drásticamente —cuando no anular de plano— el valor probatorio de estas evidencias.

En mi artículo sobre la sentencia SP-248-2025 de la Corte Suprema de Justicia de Colombia,<sup>11</sup> advertí que una de las fallas estructurales más graves observadas en la administración de justicia es la ausencia de **máximas de experiencia digital** en la gran mayoría de jueces. Esta carencia impide que puedan aplicar una verdadera **sana crítica digital** al momento de valorar pruebas electrónicas.

Si el juez no domina nociones esenciales sobre obtención, preservación, análisis y validación técnica —como la generación y verificación de códigos hash, la creación de imágenes forenses y el aseguramiento de la cadena de custodia digital—, queda limitado a aceptar pruebas cuyo origen y tratamiento son inciertos.

Este déficit de conocimientos técnicos conduce, como ocurrió en el caso que analicé, a que se otorgue valor probatorio a elementos electrónicos cuya autenticidad e integridad no han sido acreditadas conforme a estándares internacionales como las normas ISO/IEC 27037-2012 y 27042-2015.

## COLOFÓN:

### LA AUSENCIA ABSOLUTA DE SANA CRÍTICA DIGITAL

La valoración judicial de las grabaciones provenientes de los dos **relojes espía** evidencia, a mi juicio, una preocupante ausencia de lo que denomino **sana crítica digital**: la aplicación rigurosa de principios técnicos y jurídicos específicos de la evidencia electrónica, integrados a la sana crítica tradicional. La jueza no sometió a examen la fiabilidad de la **cadena de custodia digital** ni la **autenticidad e integridad de la fuente primaria u original**, omitiendo preguntas esenciales:

- ¿Se obtuvieron los datos conforme a protocolos forenses reconocidos?
- ¿Se preservó la trazabilidad técnica desde la captura hasta su presentación en juicio?
- ¿Coincidieron los **valores hash** del original con los de las copias analizadas?

Más grave aún, se echa de menos el uso de **máximas de experiencia digital** en el razonamiento probatorio. Sin conocimientos mínimos sobre extracción, preservación y validación técnica (imagen forense, hash, metadatos, cadena de custodia digital), el juzgador corre el riesgo de otorgar fiabilidad elementos

---

<sup>11</sup> Mi artículo completo está disponible en mi cuenta de Instagram: basta con comentar **248** en cualquier *reel* de mi *feed* para recibirlo.

probatorios sin garantías técnicas, debilitando su función de control de legalidad y de fiabilidad probatoria.

De allí que resulten **precipitados** los apoyos de la sentencia en los “**códigos de archivo hash**” y en la técnica de “**copia espejo**”, a los que atribuye “**un contexto suficiente**” sobre la extracción y su consecuente valor probatorio, sin exigir la comparación de hashes entre **fuentes primaria y copia**, ni el testimonio de quienes la ejecutaron.

Esta falta de *sana crítica digital* se acentúa cuando la jueza afirma que “**...el debate no involucró aspectos técnicos forenses de fondo**”.

Precisamente por ello era su deber, como garante de la **tutela judicial efectiva** y del **debido proceso probatorio**, exigir y ponderar ese examen técnico antes de conferir validez plena a las pruebas de grabación.

En coherencia con lo anterior, paso a la motivación decisiva del fallo (p. 212, 7.2.1.5.2, “De la autenticidad”), donde se lee:

*“La defensa, contó con la oportunidad de realizar pericia técnica con posterioridad al descubrimiento efectuado por la FGN, con el objeto de identificar cómo se obtuvieron, el cumplimiento de los protocolos forenses, cuál fue la información digital recuperada, verificar con la línea de tiempo, cuánto de ella fue fraccionada, eliminada y/o borrada, cómo pudo ser recuperada, si hubo signos de alteración, si allí se perciben grabaciones desconocidas, todo con el objeto de demostrar su tesis que dichos documentos inculpativos no provenían de los reloj espías mencionados.*

*Si bien, el perito cuestiona la extracción de la información de los reloj por no contar con los medios y formas para preservarse y reproducirse lo que conllevó a su inutilidad, y por ende, no pudo demostrar que de allí se extrajo el video, ello no es suficiente para probar que aquel no fue la herramienta de grabado, ni para negar la identidad entre el archivo original, el entregado a la Corte y la imagen reproducida en el juicio oral, simplemente la defensa no pudo corroborarlo, lo que sí pudo hacer la FGN con los testimonios de Juan Guillermo Monsalve Pineda, Deyanira Gómez Sarmiento y Héctor Romero Agudelo.*

*Concluye el despacho que no se afecta el valor de los documentos magnetofónicos, pues el cuestionamiento de su mismidad es hipotético no demostrativo, mírese, aunque existió una verificación, realizada por el perito, omitió especificar la gravedad de los datos encontrados que consideró irregulares, no pudo indicar cuál fue la información significativa eliminada o adicionada que variara los hechos de la acusación o la versión del testigo”.*

Este razonamiento confirma la **ausencia absoluta** de *sana crítica digital* por tres razones:

1. **Sustitución de prueba técnica por testimonios:** se valida la supuesta autenticidad con declaraciones de personas **interesadas**, en lugar de con verificación forense de **origen e integridad**.
2. **Inversión de la carga probatoria:** la sentencia reprocha a la defensa que “no pudo corroborar” que el archivo de video presentado en juicio **no provenía del reloj espía** y que **no existía identidad** entre el archivo original, el entregado a la Corte y la imagen reproducida en el juicio oral.

Sin embargo, el propio fallo admite que la extracción resultó inútil por carecer de medios y procedimientos adecuados para preservar y reproducir la información, lo que imposibilitó técnicamente que la defensa realizara tal verificación.

En lugar de exigir a la Fiscalía —como parte que presentó la prueba— la **demostración técnica de su autenticidad e integridad**, conforme al artículo 277 del Código de Procedimiento Penal colombiano, la jueza trasladó indebidamente esa carga a la defensa. Esta inversión del peso de la prueba constituye una evidente **subversión del orden procesal**, al imponer a la contraparte la obligación de acreditar la autenticidad de una evidencia cuya verificación era responsabilidad exclusiva de la Fiscalía.

**Nota técnica:** En materia de evidencia digital, la autenticidad y la integridad sólo pueden acreditarse mediante el análisis de la **fuentes primaria** —en este caso, los propios relojes espía— y la aplicación de protocolos forenses reconocidos (imagen forense bit a bit, cálculo de hash, preservación de metadatos, cadena de custodia). Al no haberse practicado pericia directa sobre el dispositivo original, sino sobre copias de origen incierto, cualquier exigencia de corroboración a la defensa resulta jurídicamente inviable. Pretender suplir esta grave falencia con testimonios de personas interesadas, como hizo la jueza, refleja una **ausencia total** de *sana crítica digital* y una valoración probatoria caprichosa y arbitraria, incompatible con los principios de confiabilidad, integridad y trazabilidad que rigen la evidencia digital.

3. **Imposibilidad lógica de “mismidad” sin fuente primaria:** Sin acceso a la fuente original ni constancia del procedimiento (imagen forense + hash comparado), la identidad entre “archivo original”, “entregado” e “imagen reproducida”, es **jurídicamente indemostrable**.

En suma, la motivación prescinde del estándar técnico que la evidencia digital exige y se apoya en hipótesis y testimonios subjetivos. Sin *sana crítica digital* ni *máximas de experiencia digital*, el juicio de autenticidad queda vaciado de contenido técnico y el valor suasorio de la prueba debió, en consecuencia, ser **seriamente disminuido** —cuando no negado—.

# GLOSARIO DE TÉRMINOS CLAVE SOBRE EVIDENCIA DIGITAL

## 1. Código o valor hash

Secuencia alfanumérica única generada mediante un algoritmo matemático (como MD5, SHA-1, SHA-256, entre otros) que identifica de manera irreplicable un conjunto de datos.

Funciona como una “huella digital” de un archivo o dispositivo.

Si el contenido se altera, aunque sea mínimamente, el valor hash cambia, lo que permite verificar la **integridad** de la evidencia digital.

---

## 2. Imagen forense

Copia **bit a bit** de la totalidad de la información contenida en un dispositivo digital, obtenida mediante herramientas forenses certificadas y bajo un protocolo formal de adquisición.

Incluye:

- Preservación de metadatos.
- Cálculo de hash antes y después de la copia.
- Documentación exhaustiva en la cadena de custodia.

Es el estándar reconocido en **Normas ISO/IEC** (como la 27037-2012 y la 27042:2015) y protocolos nacionales de evidencia digital, pues garantiza la **integridad, autenticidad y trazabilidad** desde la fuente original.

---

## 3. Copia espejo

Expresión genérica que describe una copia idéntica, bit a bit, del contenido de un soporte digital.

Aunque técnicamente puede parecer similar a una imagen forense, **no necesariamente cumple con los protocolos forenses de adquisición**, ni con la documentación de la cadena de custodia.

Por ello, toda copia espejo para ser válida como evidencia digital debe realizarse bajo el procedimiento y controles propios de una imagen forense.

En la práctica, puede considerarse una *especie* dentro del género imagen forense **solo cuando** se obtenga siguiendo metodología certificada.

---

#### 4. Bloqueador de escritura (Write Blocker)

Dispositivo o herramienta que permite acceder al contenido de un medio de almacenamiento **sin modificarlo**.

Su función es impedir cualquier alteración durante la lectura o adquisición forense, asegurando la preservación de la integridad de la evidencia.

---

#### 5. Fuente primaria de evidencia digital

Soporte o ubicación original donde se encuentra almacenada la información.

En el caso de grabaciones interceptadas, la fuente primaria sería el sistema institucional de interceptación, no las copias posteriores.

El análisis pericial debe **partir siempre de la fuente primaria** o de su imagen forense, nunca de una copia sin verificar.

---

#### 6. Cadena de custodia digital

Registro documental contínuo que detalla cada acción, traslado, persona y herramienta que ha intervenido en el manejo de una evidencia digital, desde su obtención hasta su presentación en juicio.

Su objetivo es garantizar que la evidencia **no ha sido alterada ni manipulada**.

---

## 7. Metadatos

Datos ocultos o no visibles directamente por el usuario que describen características técnicas del archivo o del dispositivo (fecha de creación, modificaciones, autor, coordenadas GPS, etc.).

En pruebas electrónicas, los metadatos son cruciales para verificar la autenticidad y reconstruir el contexto de los hechos.

---

## 8. Herramientas forenses

Programas o dispositivos diseñados para adquirir, analizar y preservar evidencias digitales de forma certificada.

Ejemplos: EnCase, FTK, X-Ways Forensics, Autopsy, Magnet AXIOM.

Su uso permite cumplir estándares internacionales y asegurar la admisibilidad probatoria.

---

## 9. Cartilla de Evidencia Digital (Colombia)

Protocolo oficial que establece procedimientos técnicos y jurídicos para la identificación, recolección, preservación y análisis de evidencia digital.

Es el equivalente en Venezuela al **Protocolo Anexo sobre Evidencia Digital** que forma parte del **Compendio de Protocolos de Actuación para el Fortalecimiento de la Investigación Penal** (Manual Único de Cadena de Custodia de Evidencias Físicas de la Fiscalía General de la República, Tomo I, primer protocolo).

En México, su equivalente es el **Anexo 11 sobre Evidencia Digital de la Norma Mexicana NOM-151-SCFI-2016**.

Todas estas normativas están inspiradas en estándares internacionales como la **ISO/IEC 27037-2012 y 27042-2015**, así como en diversos protocolos de actuación sobre evidencia digital a nivel global.

