TU ABOGADO DIGITAL®

CONCEPTOS Y MARCO JURÍDICO

Guía académica — Módulo 1

Bienvenido

Bienvenido al taller sobre evidencias digitales: **“Domina la prueba digital en el litigio moderno”**. Esta guía organiza los fundamentos conceptuales y el marco jurídico venezolano aplicable a la obtención, preservación y valoración de evidencia digital, con énfasis en integridad técnica, adquisición forense y cadena de custodia. El material está diseñado para apoyar el estudio, la discusión guiada y la práctica profesional, evitando transcribir de forma extensa artículos normativos, pero destacando su contenido esencial.

Índice

1. Propósito y alcance

El objetivo del Módulo 1 es establecer un lenguaje común sobre evidencia digital, su integridad técnica y su adquisición, así como identificar el marco jurídico venezolano que condiciona su admisibilidad y valoración en sede penal. Se abordan definiciones operativas, distinciones relevantes (nativa/digitalizada; dato/información/evidencia) y nociones técnicas mínimas para comprender por qué la forma de obtención y preservación determina la fuerza probatoria.

2. Conceptos básicos fundamentales

2.1 Evidencia digital

Se entiende por evidencia digital la información almacenada, transmitida o generada en formato digital que puede tener valor probatorio, y que requiere procedimientos técnicos de identificación, recolección, adquisición y preservación para mantener su integridad y trazabilidad durante el proceso investigativo y judicial (ISO/IEC, 2012).

2.2 Diferencias esenciales

• **Nativa vs. digitalizada:** evidencia producida originalmente en entornos digitales (p. ej., correo electrónico) frente a la conversión de un soporte físico a uno digital (p. ej., documento escaneado).
• **Fuente vs. medio de prueba:** la fuente es el dato/dispositivo originario; el medio de prueba es el mecanismo procesal para su incorporación y valoración.
• **Dato vs. información vs. evidencia:** el dato es la unidad básica; la información agrega contexto; la evidencia es información con relevancia jurídica y trazabilidad técnica suficiente para sostener una afirmación en juicio.

3. Integridad técnica (hash, metadatos y cabeceras)

3.1 Hash criptográfico

Un valor hash es una huella digital calculada mediante una función criptográfica (p. ej., SHA-256) que permite verificar si un archivo o conjunto de datos se mantiene idéntico respecto a una referencia. En forensia, el hash soporta la afirmación de integridad, pero por sí solo no prueba autoría ni veracidad del contenido; su valor probatorio crece cuando se concatena con una cadena de custodia documentada.
Representaciones comunes: hexadecimal (frecuente en herramientas forenses) y Base64 (común en transmisión y APIs). Para SHA-256, la salida típica se expresa en 64 caracteres hexadecimales. Para fundamentos técnicos sobre SHA-256, véase IETF (2011).

3.2 Metadatos

Los metadatos son “datos sobre los datos”: atributos técnicos asociados a un archivo (p. ej., fechas, software, modelo de dispositivo) que pueden aportar contexto probatorio (por ejemplo, EXIF en imágenes). Deben analizarse con cautela porque pueden perderse en transferencias, o ser alterados mediante herramientas de edición, lo que exige validación por consistencia cruzada y correlación con otras fuentes.

3.3 Cabeceras de correo (EML)

Las cabeceras de un correo electrónico registran la ruta técnica del mensaje (servidores intervinientes, marcas de tiempo, resultados de autenticación como SPF/DKIM, etc.). Son clave para atribución técnica, detección de suplantación y trazabilidad de entrega. La estructura general de los mensajes se define en estándares como IETF (2008).

4. Adquisición digital (en frío, en vivo y en caliente)

La adquisición digital es el proceso técnico de obtención de datos digitales preservando integridad y reproducibilidad, documentando cada etapa y evitando la alteración del original en la medida de lo posible (IETF, 2002).

4.1 Adquisición en frío (post■mortem)

Extracción con el dispositivo apagado. Usualmente se realiza una copia bit a bit del medio de almacenamiento, empleando bloqueadores de escritura (hardware o software) para minimizar alteraciones en el soporte original. Es el enfoque tradicional para discos y unidades físicas.

4.2 Adquisición en vivo (live)

Extracción con el sistema encendido y operativo para capturar información volátil (memoria RAM, procesos, conexiones, claves en uso). Implica reconocer y documentar que la interacción con el sistema puede generar cambios (logs, memoria), por lo que la metodología debe ser estricta y explicable en sede judicial.

4.3 Adquisición en caliente (hot)

Extracción lógica en entornos que no pueden interrumpirse (p. ej., servidores críticos, servicios en producción o ciertos entornos en la nube) mientras continúan operando. La mutabilidad inherente del sistema obliga a definir con precisión el alcance, el momento de captura y el objeto exacto de la extracción (registros, snapshots, exportaciones).

5. Esteganografía

La esteganografía es una técnica de ocultamiento: inserta información dentro de otros archivos aparentemente inocuos (imagen, audio o video) para dificultar su detección. No equivale al cifrado: el cifrado protege el contenido mediante clave; la esteganografía busca ocultar la existencia del mensaje. En investigaciones digitales, puede formar parte de tácticas de evasión

(anti■forensics) y requiere análisis especializado.

6. Cadena de custodia digital

La cadena de custodia es el conjunto de procedimientos y registros que garantizan la trazabilidad ininterrumpida de la evidencia desde su obtención hasta su presentación en juicio. En el ámbito digital, suele incorporar identificación del expediente, identificación del soporte, registro de hash, fecha/hora, identificación del funcionario o perito, condiciones de resguardo y registro de transferencias.

7. Marco legal venezolano

7.1 Constitución de la República Bolivariana de Venezuela (CRBV)

Puntos guía para evidencia digital (síntesis):
• **Art. 2:** Estado de Derecho y Justicia: la actuación probatoria debe respetar valores superiores y el ordenamiento jurídico (República Bolivariana de Venezuela, 1999).
• **Art. 48:** Secreto e inviolabilidad de las comunicaciones: la interceptación o injerencia requiere orden de tribunal competente (República Bolivariana de Venezuela, 1999).
• **Art. 49:** Debido proceso: nulas las pruebas obtenidas con violación del debido proceso; orienta exclusión de evidencia obtenida ilegalmente (República Bolivariana de Venezuela, 1999).
• **Art. 60:** Derecho a la intimidad y límites al uso de la informática para proteger honor e intimidad personal/familiar (República Bolivariana de Venezuela, 1999).

7.2 Ley sobre Mensajes de Datos y Firmas Electrónicas

Esta ley reconoce eficacia jurídica al mensaje de datos y establece la equivalencia funcional con documentos tradicionales cuando se cumplan condiciones de accesibilidad, integridad y posibilidad de ulterior consulta. Asimismo, regula la firma electrónica y su validez jurídica, y plantea bases para servicios de certificación (República Bolivariana de Venezuela, 2001).

7.3 Código Orgánico Procesal Penal (COPP) — artículos exigidos

• **Art. 181 (Lícitud de la prueba):** orienta la admisibilidad hacia medios lícitos, conectando técnica forense con respeto a garantías constitucionales (Tu Gaceta Oficial, s. f.).
• **Art. 187 (Cadena de custodia / planilla):** resalta la documentación formal de la cadena de custodia y el manejo de evidencias; su incumplimiento genera cuestionamientos sobre autenticidad e integridad (Universidad Bicentenaria de Aragua, 2021; Tribunal Supremo de Justicia, s. f.).
• **Art. 223 (Inspección y experticia):** habilita actuaciones de inspección y experticia sobre “cosas” cuando se requieran conocimientos especiales, sustentando la experticia informática (Leyes.io, s. f.).

• **Art. 224 (Idoneidad del perito):** exige título cuando la ciencia/arte/oficio esté reglamentado; en su defecto, designación por experiencia reconocida (Leyes.io, s. f.).
• **Art. 225 (Dictamen pericial):** establece el contenido mínimo: motivo, descripción, estado, exámenes practicados, resultados y conclusiones; y su presentación escrita, firmada y sellada (Wikiderecho, 2022).

8. Bibliografía (formato APA)

International Organization for Standardization & International Electrotechnical Commission. (2012). *ISO/IEC 27037:2012 — Guidelines for identification, collection, acquisition and preservation of digital evidence*. ISO.

Internet Engineering Task Force. (2002). *RFC 3227: Guidelines for Evidence Collection and Archiving*. https://www.rfc-editor.org/rfc/rfc3227

Internet Engineering Task Force. (2008). *RFC 5322: Internet Message Format*. https://www.rfc-editor.org/rfc/rfc5322

Internet Engineering Task Force. (2011). *RFC 6234: US Secure Hash Algorithms (SHA and SHA-based HMAC and HKDF)*. https://www.rfc-editor.org/rfc/rfc6234

República Bolivariana de Venezuela. (1999). *Constitución de la República Bolivariana de Venezuela*. WIPO Lex.

República Bolivariana de Venezuela. (2001). *Ley sobre Mensajes de Datos y Firmas Electrónicas* (Gaceta Oficial N.° 37.148, 28 de febrero de 2001). Acceso vía VLEX.

Tribunal Supremo de Justicia. (s. f.). *Sentencia sobre cadena de custodia (referencia al Art. 187 COPP)*. https://www.tsj.gob.ve/decisiones/scon/abril/313206-00028-27420-2020-2019-000800.HTML

Tu Gaceta Oficial. (s. f.). *Artículo 181 — Código Orgánico Procesal Penal (Venezuela)*. https://tugacetaoficial.com/codigo-organico-procesal-penal-copp/articulo-181

Universidad Bicentenaria de Aragua. (2021). *Manual de cadena de custodia y referencias normativas* [PDF].

Wikiderecho. (2022). *La declaración del imputado, el testimonio y la experticia en el proceso penal venezolano* (cita del Art. 225 COPP). https://www.wikiderecho.net/la-declaracion-del-imputado-el-testimonio-y-la-experticia-en-el-proceso-penal-venezolano/

Leyes.io. (s. f.). *Artículos 223 y 224 del Código Orgánico Procesal Penal (Venezuela)*. https://leyes.io/venezuela/codigo-organico-procesal-penal/223 y https://leyes.io/venezuela/codigo-organico-procesal-penal/224