

LA SENTENCIA EXTRANJERA SÍ APLICA

Por qué la evidencia digital comparte una misma base técnica en cualquier país

La afirmación "esa sentencia es de otro país, no aplica aquí" es uno de los errores más comunes al litigar con evidencia digital. Esta mini-guía resume, en tres ideas, por qué eso es falso.

1. Tecnología universal, procedimientos nacionales

Un chat, un audio o una captura de pantalla se producen mediante el mismo proceso técnico en Caracas, Madrid, Bogotá o Ciudad de México: la misma estructura binaria, los mismos algoritmos de hash, los mismos metadatos. Lo que sí varía entre países son las reglas procesales sobre cómo se promueve, contradice y admite esa prueba.

VARÍA POR PAÍS	ES IGUAL EN CUALQUIER PAÍS
Promoción, contradicción, desconocimiento, admisión y evacuación de la prueba	Estructura del archivo digital, funciones hash, metadatos, límites técnicos de una captura
Requisitos formales de admisibilidad procesal y, eventualmente, de valoración.	Riesgos de alteración, manipulación y pérdida de integridad

2. Ocho principios universales de validez

Sea cual sea el formato —chat, correo, video, base de datos, contenido en la nube— valorar evidencia digital exige responder siempre las mismas preguntas. De ahí surgen ocho principios que no dependen de ninguna legislación particular:

Autenticidad	Integridad	Fiabilidad	Trazabilidad
¿Es lo que dice ser?	¿Fue alterada?	¿El método usado es confiable?	¿Se puede reconstruir su manejo?
Reproducibilidad	Complejidad	Licitud	Pertinencia
¿Otro experto llega al mismo resultado?	¿Se presenta con contexto?	¿Se obtuvo legalmente?	¿Guarda relación con el hecho?

No existe una integridad "venezolana" ni una autenticidad "española": son condiciones mínimas para confiar racionalmente en cualquier información digital.

3. El rol de ISO/IEC 27037 y 27042

La ley exige integridad y autenticidad, pero rara vez explica cómo lograrlas. Ahí entran los estándares técnicos internacionales, que sistematizan la metodología forense y sirven como parámetro auxiliar de la sana crítica.

NORMA	REGULA	PREGUNTA CLAVE QUE RESPONDE
ISO/IEC 27037:2012	Identificación, recolección, adquisición y preservación de evidencia digital potencial (computadoras, móviles, redes, dispositivos).	¿Se preservó la evidencia sin alterarla y de forma documentada?
ISO/IEC 27042:2015	Análisis e interpretación de la evidencia ya recolectada.	¿El análisis es continuo, válido, reproducible y revisable?
RFC 3227 / NIST SP 800-101	Guías técnicas complementarias sobre recolección de evidencia y preservación forense de dispositivos móviles.	Referencias operativas ampliamente citadas en la literatura forense.

IDEA CLAVE

Estas normas no sustituyen la ley ni se vuelven derecho interno automáticamente. Su función es distinta: permiten saber si el perito, el investigador o el litigante actuó de forma confiable — sin importar en qué país se dictó la sentencia que se invoca como referencia.