ANÁLISIS · CIENCIAS FORENSES

Lo que quedó fuera: cómo delimitar un examen de evidencia digital

Juan Carlos Echeverri Garcés · 29 de noviembre de 2026



Ilustración editorial · No corresponde a un caso real

Una extracción íntegra solo acredita la estabilidad de aquello que se preservó. El informe pericial debe explicar qué fuentes, periodos y eventos pudo examinar, y qué permiten concluir los resultados negativos.

El límite del archivo es el límite de ciertas inferencias

Un informe puede ser técnicamente correcto al identificar un archivo íntegro y, sin embargo, equivocarse al describir el universo que ese archivo representa. Una exportación de registros abarca determinados eventos, periodos y campos; su huella digital puede ayudar a comprobar que el objeto recibido se mantiene sin cambios frente a una referencia confiable. Esa verificación no dice si el sistema registró todos los eventos de interés ni si la exportación los incluyó. Confundir esas cuestiones abre un espacio para conclusiones más amplias que los datos examinados.

NIST IR 8387 aborda la preservación de evidencia digital y distingue ese trabajo de la adquisición, salvo en los puntos donde se cruzan [1]. Su utilidad aquí es técnica. La preservación responde a la integridad y al manejo del objeto; la cobertura exige contrastar el contenido entregado con la pregunta investigativa, las fuentes disponibles y lo que se conoce del sistema.

Empezar por la pregunta autorizada

Un encargo como «revisar todo el sistema» no define una hipótesis, un universo ni un resultado verificable. Una formulación más acotada pregunta, por ejemplo, qué eventos asociados a la aprobación de una orden están registrados en una aplicación, durante un periodo determinado y en las fuentes entregadas al perito. Conviene identificar la autorización aplicable, la ventana temporal y los límites de acceso antes de escoger los materiales para el examen. El propósito legitima la selección; no amplía por sí solo la autorización para buscar datos distintos.

En el contexto penal colombiano, el artículo 254 de la Ley 906 de 2004 enumera factores relevantes de cadena de custodia para demostrar autenticidad, entre ellos identidad, estado original, condiciones de recolección y preservación, permanencia y cambios efectuados por custodios [2]. Una investigación interna puede adoptar controles de trazabilidad proporcionados sin atribuirse facultades de policía judicial ni presumir que la diligencia corporativa es equivalente a la actuación procesal.

Tres ausencias que un informe no debe mezclar

Primera, ausencia de objeto: una fuente fue identificada pero no se recibió o no pudo consultarse de forma autorizada. Segunda, ausencia de detección: en el conjunto revisado no se identificó el patrón definido, dadas la técnica y la cobertura descritas. Tercera, ausencia del hecho: afirmación sobre lo ocurrido fuera del archivo, que exige justificar por qué el evento de interés habría quedado registrado y por qué las fuentes pertinentes pudieron examinarse. Esas tres afirmaciones no tienen la misma fuerza.

Caso hipotético: se pide examinar si una orden se aprobó fuera del horario previsto. La exportación del sistema contiene cambios de estado, pero excluye el historial de aprobaciones y no documenta la zona horaria aplicada. Los registros conservados pueden respaldar que hubo un cambio de estado a la hora que figura en el archivo. No bastan para identificar a la persona que autorizó la orden, determinar la hora local efectiva de la aprobación o descartar otro evento fuera del intervalo exportado. La primera acción útil sería pedir aclaración sobre cobertura y zona horaria a quien administra la fuente, dentro del alcance autorizado.

Qué conviene dejar reproducible

Para cada fuente, registre qué objeto se recibió, quién lo entregó, periodo declarado, periodo observado, qué campos o tipos de eventos incluyó, requisitos de interpretación y qué quedó excluido. Si existen vistas de trabajo o tablas derivadas, conserve el vínculo con el objeto preservado, el criterio de transformación y el motivo de cualquier alteración de formato. Una descripción de los filtros y de la zona horaria interpretada ayuda a otro examinador a reproducir el resultado sin reencontrar datos ajenos al encargo.

Las conclusiones deben volver a la pregunta y mostrar la condición bajo la cual serían revisables. «No identificamos el evento en los archivos y ventanas descritos; el historial de aprobaciones no integró la entrega» delimita mejor el conocimiento disponible que «no hubo aprobación». Si hay indicios de retención incompleta o carencia de fuentes, describa qué contraste faltó y cuál sería el aporte de obtenerlo, sin prometer que existe o que su resultado cambiaría la conclusión.

Conclusión

Un examen aporta más cuando el lector puede separar qué se preservó, qué se examinó y qué se infirió. Sigue a Juan Carlos Echeverri Garcés y comenta: ¿qué limitación de cobertura debería aparecer antes de la conclusión en tus informes?

Referencias

1 NIST IR 8387, Digital Evidence Preservation

2 Colombia, Ley 906 de 2004, art. 254

Lecturas y servicios relacionados

- Publicaciones, artículos e investigación
- Portafolio relacionado de Risk Group