EPICENTRO Ciencia Tecnología Innovación
N° 2 | Año: 2026 | ISSN: L 2805-1971

Cadena de custodia de datos volátiles en Panamá: Desafíos probatorios del IMELCF.

Ricci Valencia (✉)
ISAE Universidad
Correo electrónico: riccivalencia@hotmail.com
ORCID: 0009-0004-5896-7078

Edilia González
ISAE Universidad
Correo electrónico: edilia1622@gmail.com
ORCID: 0009-0002-9520-7065

René Omar Rodríguez González,
Universidad Tecnológica OTEIMA
rene.rodriguez@oteima.ac.pa,
ORCID: 0000-0002-2659-3276

Nicanor Jiménez,
Universidad Tecnológica OTEIMA
nicanorjimenez02@gmail.com

DOI: 10.61209/re.v4i2.185
Recibido: junio 2026
Aceptado: agosto 2026

Resumen
El ensayo analiza los desafíos jurídicos, técnicos e institucionales que enfrenta el Instituto de Medicina Legal y Ciencias Forenses para preservar datos volátiles dentro de la cadena de custodia de la evidencia digital en Panamá. El objetivo es determinar si el marco procesal vigente y los procedimientos forenses disponibles ofrecen condiciones suficientes para demostrar autenticidad, integridad, trazabilidad y reproducibilidad probatoria. Se aplicó una metodología cualitativa, documental y dogmático-jurídica, apoyada en una matriz de análisis de legislación panameña, protocolos institucionales, doctrina especializada y estándares internacionales de informática forense. El examen muestra que las reglas generales del Código Procesal Penal permiten sustentar la obtención y custodia de evidencia electrónica, pero no desarrollan expresamente el orden de volatilidad, la adquisición de memoria viva, la validación de herramientas, la documentación del impacto de la captura ni el tratamiento de datos alojados en la nube. La discusión evidencia una tensión inevitable entre la necesidad de intervenir un sistema encendido y la obligación de reducir al mínimo toda alteración. Se concluye que la integridad probatoria no depende de conservar los datos en un estado materialmente inmóvil, sino de demostrar, mediante procedimientos verificables, qué se hizo, por qué se hizo, quién intervino, qué herramienta se utilizó y cómo se comprobó la correspondencia entre la evidencia obtenida y la presentada ante el tribunal. Se propone adoptar un protocolo nacional específico, fortalecer la capacitación y establecer auditorías técnicas periódicas.

Palabras clave: cadena de custodia, datos volátiles, evidencia digital, informática forense, integridad probatoria, IMELCF.

Abastract
This academic essay examines the legal, technical, and institutional challenges faced by Panama's Institute of Legal Medicine and Forensic Sciences when preserving volatile data within the chain of custody of digital evidence. Its objective is to determine whether the current procedural framework and available forensic procedures provide sufficient conditions to demonstrate evidentiary authenticity, integrity, traceability, and reproducibility. A qualitative, documentary, and legal-dogmatic methodology was used, supported by an analytical matrix covering Panamanian legislation, institutional protocols, specialized scholarship, and international digital-forensics standards. The analysis shows that the general rules of the Panamanian Criminal Procedure Code provide a legal basis for collecting and safeguarding electronic evidence, but they do not expressly regulate the order of volatility, live-memory acquisition, tool validation, documentation of acquisition impact, or the treatment of cloud-based data. The discussion identifies an unavoidable tension between the need to interact with a running system and the duty to minimize alteration. It concludes that evidentiary integrity does not require data to remain materially immobile; rather, it requires a verifiable record of what was done, why it was done, who intervened, which tools were used, and how the correspondence between the acquired evidence and the evidence presented in court was confirmed. The essay recommends a specific national protocol, stronger specialized training, and periodic technical audits.

Keywords: chain of custody, volatile data, digital evidence, digital forensics, evidentiary integrity, IMELCF.

Introducción

La digitalización de las comunicaciones, los servicios financieros, la actividad empresarial y la gestión pública ha transformado la forma en que se investigan los delitos. En numerosos procesos penales, los hechos dejan rastros en teléfonos móviles, computadores, servidores, sistemas de videovigilancia, aplicaciones de mensajería, plataformas en la nube y dispositivos conectados. Estos registros pueden revelar comunicaciones, ubicaciones, accesos, movimientos financieros, identidades digitales y secuencias de actividad. Su utilidad probatoria, sin embargo, depende de que la información sea obtenida de manera lícita, preservada con métodos adecuados y explicada ante el tribunal mediante procedimientos que puedan ser verificados por las partes.

La evidencia digital no se comporta como un objeto físico tradicional. Aunque puede almacenarse en un soporte tangible, su contenido es intangible, reproducible y susceptible de alteración mediante operaciones automáticas del sistema. La apertura de un archivo, el encendido de un dispositivo, la conexión a una red o la ejecución de una herramienta forense pueden modificar metadatos, registros temporales y áreas de almacenamiento. Por esta razón, la cadena de custodia digital exige algo más que identificar quién recibió un equipo y dónde fue guardado. Debe documentar la adquisición, la generación de copias forenses, los valores hash, los controles de acceso, las herramientas utilizadas y cualquier modificación inevitable producida durante el procedimiento (Casey, 2011).

que identificar quién recibió un equipo y dónde fue guardado. Debe documentar la adquisición, la generación de copias forenses, los valores hash, los controles de acceso, las herramientas utilizadas y cualquier modificación inevitable producida durante el procedimiento (Casey, 2011).

La dificultad aumenta cuando la información buscada es volátil. La memoria RAM, las conexiones activas, los procesos en ejecución, las sesiones autenticadas, las claves criptográficas temporales, las tablas de enrutamiento y otros datos dinámicos pueden desaparecer al apagar o reiniciar el sistema. En esos casos, la preservación no siempre consiste en desconectar el equipo y trasladarlo al laboratorio. El primer interviniente debe valorar si la pérdida de la información viva sería más perjudicial que la alteración controlada que produce su captura. Esa decisión exige capacitación, autorización jurídica, herramientas confiables y una documentación precisa del estado inicial y de cada actuación realizada.

En Panamá, el Instituto de Medicina Legal y Ciencias Forenses cumple una función esencial como auxiliar científico de la administración de justicia. Sus peritos apoyan las investigaciones dirigidas por el Ministerio Público y deben aplicar procedimientos que protejan la identidad e integridad de los indicios. El Manual de procedimiento del sistema de cadena de custodia del IMELCF establece criterios generales de identificación, embalaje, traslado, recepción, análisis y devolución de los elementos probatorios (Instituto de Medicina Legal y Ciencias Forenses [IMELCF], 2015). No obstante, el ritmo de cambio tecnológico obliga a examinar si esos criterios generales responden con suficiente detalle a la naturaleza de los datos volátiles.

El problema central no radica en la ausencia absoluta de fundamento jurídico. El Código Procesal Penal contiene principios de licitud, objetividad, control judicial, contradicción y responsabilidad en la investigación que permiten incorporar evidencia electrónica. La cuestión consiste en determinar cómo deben traducirse esas garantías en decisiones técnicas concretas cuando el dato puede desaparecer en segundos, se encuentra cifrado, está distribuido entre varios servicios o depende de infraestructura administrada fuera del territorio nacional. Un protocolo insuficientemente específico puede generar actuaciones dispares, pérdida de información, dificultades para reproducir el análisis y cuestionamientos sobre la fiabilidad de la prueba.

El objetivo de este ensayo es analizar los principales desafíos jurídicos y técnicos que enfrenta el IMELCF para garantizar la integridad probatoria de los datos volátiles. Para ello se emplea un enfoque cualitativo y documental, con métodos dogmático-jurídico y comparado. Se revisan la legislación procesal panameña, el manual institucional de cadena de custodia, literatura especializada y estándares internacionales como la ISO/IEC 27037, las guías del National Institute of Standards and Technology y los principios británicos de buenas prácticas para evidencia digital. La tesis que orienta el análisis sostiene que las normas generales son necesarias, pero deben complementarse con un protocolo operativo específico que establezca criterios de decisión, orden de volatilidad, validación de herramientas, documentación técnica, controles de calidad y mecanismos de auditoría.

Desarrollo Argumentativo

La prueba digital como objeto jurídico y técnico

La prueba penal cumple una función de conocimiento y de garantía. Permite reconstruir hechos

relevantes para la decisión judicial, pero al mismo tiempo limita la potestad punitiva, porque exige que la acusación se fundamente en elementos obtenidos e incorporados de conformidad con la Constitución y la ley. En un sistema acusatorio, la fuerza de una evidencia no depende únicamente de su contenido. También depende de la posibilidad de conocer su origen, discutir el procedimiento de obtención, examinar al perito y contrastar los resultados con métodos independientes. La evidencia digital, por tanto, debe ser comprendida como información técnicamente interpretable y procesalmente controvertible.

La información electrónica puede aparecer como contenido visible, metadatos, registros de actividad, archivos eliminados, datos de geolocalización, credenciales, comunicaciones o huellas de ejecución. Su valor surge de la relación entre el dato, el sistema que lo generó y el contexto investigado. Un mensaje aislado puede ser insuficiente si no se determina la cuenta asociada, la fecha, la zona horaria, la integridad del archivo, el dispositivo de origen y la forma en que fue adquirido. De igual manera, un valor hash demuestra que dos conjuntos de datos coinciden, pero no prueba por sí solo que la fuente era lícita, que el contenido pertenece a determinada persona o que la interpretación del perito es correcta.

Esta doble dimensión explica por qué la cadena de custodia no puede reducirse a una serie de firmas. En la evidencia física, el registro de entrega y recepción permite controlar el objeto. En la evidencia digital, además, debe explicarse la relación entre el soporte original, la copia forense, los archivos exportados y los productos derivados del análisis. Cada transformación debe ser identificable. Cuando se realiza una imagen bit a bit, se calculan funciones hash antes y después de la transferencia, se protege el original y se analiza una copia de trabajo. Cuando la adquisición es lógica o selectiva, debe indicarse qué información pudo quedar fuera y por qué el método escogido fue adecuado para el propósito pericial (ISO, 2012).

La autenticidad se refiere a la demostración de que el dato es lo que se afirma que es; la integridad, a que no ha sido modificado de manera no autorizada o no explicada; la trazabilidad, a la reconstrucción de las intervenciones; y la reproducibilidad, a la posibilidad de obtener resultados comparables mediante el mismo procedimiento. Estos conceptos están relacionados, pero no son equivalentes. Una evidencia puede conservar su hash y, aun así, haber sido obtenida sin autorización. También puede haber sufrido cambios técnicamente inevitables durante una captura en vivo y conservar valor probatorio si tales cambios fueron minimizados, documentados y explicados con rigor.

Datos volátiles y orden de adquisición

Los datos volátiles son aquellos cuya permanencia depende del funcionamiento del sistema o de condiciones temporales. Entre ellos se encuentran el contenido de la memoria RAM, procesos activos, conexiones de red, puertos abiertos, sesiones remotas, usuarios autenticados, cachés, llaves de cifrado, tablas ARP, rutas y otros registros que pueden cambiar de manera continua. Su importancia radica en que muestran el estado operativo del equipo en un momento determinado. Pueden revelar malware residente en memoria, comunicaciones no grabadas en disco, contenedores cifrados abiertos o credenciales temporales que desaparecerían con el apagado.

La informática forense ha desarrollado el principio del orden de volatilidad: la información con mayor riesgo de desaparición debe ser adquirida antes que aquella más estable. La guía RFC 3227

recomienda considerar la rapidez con que cada fuente puede perderse y documentar la secuencia de recolección (Internet Engineering Task Force [IETF], 2002). Este criterio no funciona como una fórmula rígida. La prioridad depende del caso, de la autorización disponible, del riesgo para terceros, de la posibilidad de propagación de un ataque y de las capacidades del equipo interviniente. Un servidor comprometido conectado a una infraestructura crítica no puede tratarse de la misma manera que un computador personal aislado.

La captura en vivo genera una paradoja. Para preservar la memoria y las conexiones activas es necesario ejecutar comandos o herramientas sobre el sistema, pero esa interacción modifica precisamente el entorno que se pretende documentar. La solución técnica no consiste en afirmar que no ocurrió ninguna alteración. Consiste en reducirla al mínimo, utilizar herramientas previamente evaluadas, registrar su versión y configuración, conservar los archivos de salida, anotar los comandos ejecutados y explicar el impacto esperado. Los principios ACPO aceptan que una intervención pueda modificar datos cuando sea indispensable, siempre que la realice personal competente capaz de justificar sus acciones y sus consecuencias (Association of Chief Police Officers [ACPO], 2012).

En la práctica, la decisión entre apagar, aislar o capturar un equipo debe quedar sustentada. Apagar puede preservar el disco, pero destruir la memoria y cerrar sesiones cifradas. Mantenerlo encendido puede conservar información valiosa, aunque incrementa el riesgo de acceso remoto, borrado automático o alteración por procesos del sistema. Aislar la red puede detener comunicaciones maliciosas, pero también modificar estados de conexión. Por ello, el protocolo debe contemplar una evaluación inicial, fotografías o video del entorno, identificación de usuarios conectados, hora oficial de referencia, condiciones de energía, estado de la red, herramientas disponibles y autorización para intervenir.

Cadena de custodia e integridad probatoria

La cadena de custodia persigue demostrar continuidad e identidad. En el ámbito digital, esa continuidad se apoya en registros humanos y controles técnicos. El acta debe individualizar el dispositivo, su marca, modelo, número de serie, estado, conexiones y ubicación. La adquisición debe producir un identificador criptográfico, conservar la fecha y hora del procedimiento y vincular cada archivo generado con el caso. El almacenamiento requiere medios protegidos, control de acceso, copias de respaldo y mecanismos que permitan detectar cualquier modificación. El análisis debe realizarse sobre copias autorizadas, manteniendo separado el original.

Las funciones hash son un recurso esencial, pero su empleo debe ser comprendido correctamente. Un hash es una representación matemática del contenido de un archivo o conjunto de datos. La coincidencia de valores permite demostrar que las copias comparadas son idénticas a nivel de bits. No sustituye el resto de la cadena de custodia ni explica por sí solo el origen del dato. Además, el laboratorio debe establecer qué algoritmos acepta, cómo registra los valores, en qué momento los calcula y cómo responde ante formatos que cambian durante una exportación legítima. El uso de algoritmos robustos como SHA-256 o superiores reduce riesgos asociados a funciones antiguas.

La integridad de datos volátiles exige un enfoque de integridad explicada. La captura de memoria crea un archivo nuevo; no existe un objeto previo que pueda sellarse antes de la adquisición. En consecuencia, el valor probatorio depende de la fidelidad del procedimiento: herramienta utilizada,

privilegios de ejecución, tamaño esperado, mensajes de error, duración, destino del archivo, hash posterior y condiciones del sistema. También debe conservarse un registro de actividad que permita a otro especialista evaluar si la herramienta pudo omitir regiones, alterar estructuras o fallar frente a mecanismos de seguridad.

La documentación debe ser contemporánea a la actuación. Los apuntes elaborados después, basados únicamente en la memoria del perito, debilitan la trazabilidad. Un formulario específico para evidencia volátil debería incluir la decisión técnica adoptada, el orden de adquisición, la justificación de cada paso, la hora sincronizada, el nombre de la herramienta, versión, licencia, parámetros, medio de destino, hash, observaciones y responsables. Cuando se realizan capturas de pantalla o fotografías, estas también deben incorporarse al registro y vincularse con el expediente.

La reproducibilidad no significa que siempre sea posible repetir la adquisición original. El estado vivo del sistema desaparece o cambia. Lo reproducible debe ser el análisis del archivo capturado y la evaluación del método. Por ello, se deben conservar la imagen de memoria, los registros de adquisición, la versión de la herramienta y, cuando sea legalmente posible, los archivos de configuración necesarios para ejecutar nuevamente el examen. El informe pericial debe diferenciar entre datos observados, inferencias técnicas y conclusiones relacionadas con la hipótesis del caso.

Marco procesal panameño y función del IMELCF

El Código Procesal Penal panameño proporciona bases generales para el tratamiento de la prueba. El principio de licitud exige que la información sea obtenida con respeto a la Constitución, la ley y los derechos fundamentales. La dirección de la investigación corresponde al Ministerio Público, mientras que los organismos auxiliares y peritos actúan dentro de la finalidad investigativa y bajo controles procesales. Estas reglas permiten ordenar diligencias sobre dispositivos y sistemas, pero exigen autorización judicial cuando la intervención afecta ámbitos protegidos como la intimidad, el secreto de las comunicaciones o los datos personales (Panamá, 2008).

La evidencia digital plantea preguntas que deben resolverse antes de la actuación técnica. No toda información accesible en un equipo puede ser examinada sin límites. La orden debe definir, en la medida posible, el objeto, alcance y finalidad de la diligencia. En situaciones urgentes, la preservación puede requerir una respuesta inmediata, pero la urgencia no elimina la obligación de documentar su fundamento y someter la medida al control correspondiente. La amplitud excesiva de una extracción puede incorporar datos de terceros o información irrelevante, generando conflictos de proporcionalidad y afectando el derecho de defensa.

El IMELCF tiene la responsabilidad de convertir la orden jurídica en un procedimiento científico. Su manual de cadena de custodia constituye una base institucional importante porque organiza la recepción, manejo, traslado y análisis de indicios. Sin embargo, un protocolo general no siempre resuelve preguntas propias de la memoria viva: quién autoriza la captura, qué herramientas están validadas, qué secuencia debe seguirse, cómo se documenta el impacto, qué hacer si el sistema está cifrado, cómo gestionar una conexión remota o qué procedimiento adoptar cuando la información se encuentra en un servicio extranjero.

La coordinación con el Ministerio Público debe comenzar antes de la diligencia cuando la complejidad

del caso sea previsible. El fiscal necesita comprender las consecuencias de apagar o mantener encendido un dispositivo; el perito necesita conocer el alcance de la autorización y los hechos que orientan la búsqueda. Una planificación conjunta permite preparar equipos de escritura, medios de almacenamiento, herramientas de captura, mecanismos de aislamiento, fuentes de energía, documentación y personal suficiente. También reduce improvisaciones y evita que decisiones técnicas críticas sean tomadas por funcionarios que no poseen formación especializada.

La defensa y el tribunal deben tener acceso a información suficiente para ejercer contradicción. Esto no significa divulgar datos sensibles sin control, sino facilitar el informe, los valores hash, la metodología, los registros de cadena de custodia y, cuando corresponda, una copia forense o un mecanismo de revisión independiente. La transparencia metodológica fortalece la prueba. Cuando la pericia se apoya en una herramienta propietaria, el informe debe explicar sus funciones, limitaciones y validación, evitando que la conclusión dependa de una caja negra imposible de examinar.

Principales desafíos técnicos e institucionales

El primer desafío es la rapidez. Los datos volátiles pueden desaparecer antes de que el equipo especializado llegue al lugar. Esto exige capacitar a primeros respondientes para reconocer escenarios digitales, proteger el área, evitar acciones destructivas y solicitar apoyo. No se pretende que todo funcionario realice adquisiciones complejas, sino que identifique cuándo no debe apagar, manipular o conectar un dispositivo. Una guía de decisión breve, acompañada de comunicación inmediata con el laboratorio, puede prevenir pérdidas irreversibles.

El segundo desafío es la validación de herramientas. La informática forense utiliza programas comerciales y de código abierto que se actualizan con frecuencia. Una versión nueva puede corregir fallos, cambiar formatos o producir resultados distintos. El laboratorio debe mantener un inventario controlado, verificar versiones, documentar pruebas de funcionamiento y conservar registros de validación. Los lineamientos del NIST destacan la necesidad de integrar técnicas forenses con procedimientos de respuesta que preserven la fiabilidad de la evidencia (National Institute of Standards and Technology [NIST], 2006).

El tercer desafío corresponde a la capacitación y especialización. La adquisición de memoria, el análisis de sistemas operativos, la respuesta ante malware, el examen de dispositivos móviles y la extracción de datos en la nube requieren competencias diferentes. La experiencia individual no puede sustituir un programa institucional de formación. Se necesitan perfiles definidos, entrenamiento periódico, ejercicios de simulación, evaluación de competencias y actualización frente a nuevas tecnologías. La rotación de personal sin transferencia de conocimiento debilita la consistencia del servicio.

El cuarto desafío es la infraestructura. La preservación de evidencia digital demanda almacenamiento seguro, redes separadas, estaciones forenses, sistemas de respaldo, control ambiental y capacidad para manejar grandes volúmenes. Los casos modernos pueden incluir imágenes de varios terabytes, copias de dispositivos móviles y datos de múltiples cuentas. Si el laboratorio carece de capacidad, puede verse obligado a retrasar análisis, utilizar medios no estandarizados o mantener evidencia en condiciones que dificultan el control. La planificación presupuestaria debe considerar renovación tecnológica, licencias, mantenimiento y obsolescencia.

El quinto desafío es la computación en la nube. La información puede estar distribuida en varios países, ser administrada por un proveedor y cambiar por procesos automáticos. En esos casos, no existe necesariamente un dispositivo físico bajo control del perito. La cadena de custodia debe incorporar solicitudes de preservación, respuestas del proveedor, registros de descarga, autenticación de cuentas, sellos de tiempo y hash de los archivos recibidos. También se requiere coordinación jurídica internacional y claridad sobre la competencia, la privacidad y la conservación de datos.

El sexto desafío es el cifrado. Una computadora encendida puede contener claves en memoria que permiten acceder a volúmenes cifrados. Apagarla podría hacer imposible la recuperación posterior. La captura viva puede ser decisiva, pero debe cumplir los límites de la orden y evitar exploraciones indiscriminadas. El protocolo debe contemplar la identificación de contenedores abiertos, la preservación de llaves cuando sea técnicamente posible y la documentación de toda acción. La decisión requiere equilibrio entre eficacia investigativa, necesidad, proporcionalidad y protección de información ajena al caso.

El séptimo desafío es la sincronización temporal. Los registros digitales dependen de relojes que pueden estar desajustados, configurados en otra zona horaria o manipulados. El perito debe registrar la hora mostrada por el sistema, compararla con una fuente confiable y explicar las correcciones aplicadas. Una línea temporal construida sin considerar estos factores puede atribuir acciones a momentos equivocados. La documentación de la zona horaria, el desfase y la fuente de referencia resulta indispensable para interpretar conexiones, mensajes y eventos.

El octavo desafío es la calidad del informe. Un reporte excesivamente técnico puede resultar incomprensible; uno demasiado simple puede ocultar limitaciones. El perito debe explicar el procedimiento en lenguaje claro, distinguir hallazgos de interpretaciones y declarar cualquier error o incertidumbre. También debe evitar conclusiones jurídicas que corresponden al tribunal. La calidad probatoria depende de que las partes puedan seguir la lógica del análisis, identificar sus premisas y examinar las alternativas.

Estándares internacionales y lecciones comparadas

La ISO/IEC 27037 ofrece directrices para la identificación, recolección, adquisición y preservación de evidencia digital. Su utilidad radica en diferenciar estas fases y establecer que las actuaciones deben ser justificables, documentadas y realizadas por personas competentes (ISO, 2012). La ISO/IEC 27041 se enfoca en la idoneidad de los métodos de investigación; la ISO/IEC 27042 orienta el análisis e interpretación; y la ISO/IEC 27043 desarrolla principios y procesos de investigación de incidentes. En conjunto, estos estándares permiten diseñar un sistema de calidad que abarque desde la escena hasta el informe.

Las guías del NIST aportan procedimientos aplicables a respuesta a incidentes, medios informáticos y dispositivos móviles. Su principal enseñanza no consiste en copiar una herramienta o secuencia, sino en integrar la actuación forense a la gestión del incidente, proteger la evidencia y documentar las decisiones. La adquisición debe adaptarse al objetivo, al tipo de dispositivo y al riesgo de pérdida. En dispositivos móviles, por ejemplo, el aislamiento de red, el estado de bloqueo, la batería y el cifrado pueden determinar el método apropiado (Ayers, Brothers, & Jansen, 2014).

Los principios ACPO, aunque surgieron en el Reino Unido, mantienen relevancia por su claridad. Exigen que ninguna acción cambie datos que puedan presentarse ante un tribunal; cuando la modificación sea inevitable, solo una persona competente debe intervenir y explicar sus efectos. También requieren un registro completo que permita a un tercero independiente examinar el proceso y obtener resultados comparables (ACPO, 2012). Esta formulación reconoce la realidad de las capturas vivas sin renunciar a la responsabilidad profesional.

La lección comparada para Panamá es que la ley procesal no necesita contener cada comando técnico. La norma debe establecer garantías, competencias y controles; los protocolos deben traducirlas en procedimientos actualizables. Un protocolo nacional puede incorporar anexos por tipo de escenario: computadores encendidos, servidores, dispositivos móviles, entornos virtuales, nube, incidentes de red y sistemas industriales. Así se evita que la legislación quede obsoleta y, al mismo tiempo, se reduce la discrecionalidad no documentada.

Propuesta de fortalecimiento para el IMELCF

El primer componente debe ser un protocolo específico para datos volátiles, aprobado institucionalmente y coordinado con el Ministerio Público. Este documento debe definir conceptos, roles, criterios de activación, autorización, orden de volatilidad, secuencia de captura, herramientas permitidas, controles de tiempo, generación de hash, tratamiento de errores, embalaje, almacenamiento y elaboración del informe. También debe contener formularios uniformes y listas de verificación que reduzcan omisiones sin convertir la actuación en una rutina mecánica.

El segundo componente es un programa de validación y control de calidad. Antes de utilizar una herramienta en casos reales, el laboratorio debe comprobar su comportamiento en escenarios conocidos, registrar los resultados y establecer limitaciones. Las actualizaciones deben someterse a pruebas. Los casos complejos pueden requerir revisión por pares, especialmente cuando la conclusión depende de artefactos novedosos, sistemas poco comunes o datos recuperados parcialmente. Las auditorías internas y externas ayudan a detectar inconsistencias y fortalecer la confianza institucional.

El tercer componente es la formación diferenciada. Los primeros respondientes necesitan reconocimiento y preservación inicial; fiscales y jueces, comprensión de alcance, autorización y contradicción; defensores, capacidad para examinar la metodología; y peritos, competencias avanzadas de adquisición y análisis. La capacitación conjunta favorece un lenguaje común y permite que las decisiones jurídicas consideren consecuencias técnicas. Los ejercicios simulados deben incluir escenarios de urgencia, cifrado, nube y pérdida de conectividad.

El cuarto componente es la gestión segura de evidencia. Debe implementarse un sistema digital de trazabilidad que registre accesos, movimientos, copias, análisis y devoluciones. Los repositorios deben contar con controles de identidad, privilegios mínimos, registros inalterables, respaldo y verificación periódica de integridad. La cadena física y la digital deben vincularse mediante identificadores únicos. La automatización no elimina la responsabilidad humana, pero reduce errores de transcripción y facilita auditorías.

El quinto componente es la transparencia metodológica. Los informes deberían incluir una sección estándar sobre herramientas, versiones, parámetros, hash, fuentes de tiempo, limitaciones y cambios

inevitables. Cuando no sea posible reproducir la adquisición, debe explicarse por qué y qué controles compensatorios fueron aplicados. La defensa debe contar con mecanismos razonables para revisar la evidencia sin comprometer datos de terceros o información sensible. La contradicción técnica no debilita la investigación; la hace más confiable.

El sexto componente es la actualización periódica. Un comité técnico-jurídico podría revisar el protocolo al menos una vez al año o cuando aparezcan cambios significativos. Su integración debería incluir especialistas del IMELCF, fiscales, defensores, jueces, académicos y profesionales de seguridad informática. La revisión debe considerar experiencias de casos, incidentes de calidad, nuevas versiones de estándares y tecnologías emergentes. Un procedimiento estático pierde eficacia rápidamente frente a la evolución digital.

Finalmente, es necesario reconocer las limitaciones del presente análisis. Al tratarse de un ensayo documental, no examina expedientes reservados ni mide tiempos reales de respuesta, capacidad instalada o frecuencia de impugnaciones. Estas variables requieren investigaciones empíricas con autorización institucional. Futuros estudios pueden evaluar la consistencia de formularios, la disponibilidad de herramientas, las necesidades de capacitación y la percepción de fiscales, peritos, defensores y jueces. Esa evidencia permitiría priorizar inversiones y medir el impacto de las reformas.

Conclusiones

La cadena de custodia de los datos volátiles constituye uno de los puntos más sensibles de la investigación penal digital. Su dificultad no deriva únicamente de la fragilidad técnica de la información, sino de la necesidad de adoptar decisiones inmediatas bajo límites jurídicos. Apagar un sistema puede destruir datos esenciales; mantenerlo encendido puede permitir alteraciones o accesos remotos; capturar la memoria modifica parcialmente el entorno. Ninguna opción es neutra. Por ello, la validez del procedimiento depende de que la decisión sea razonable, autorizada, ejecutada por personal competente y documentada de forma completa.

El marco procesal panameño ofrece principios suficientes para fundamentar la licitud, la contradicción y el control de la prueba digital. Sin embargo, esos principios generales no sustituyen un protocolo técnico específico. La evidencia volátil requiere reglas operativas sobre orden de adquisición, captura en vivo, aislamiento, sincronización temporal, hash, validación de herramientas, registro de errores, almacenamiento y acceso de las partes. La ausencia de criterios uniformes puede producir respuestas diferentes ante situaciones similares y dificultar la defensa de la pericia en juicio.

La integridad probatoria no debe entenderse como una inmovilidad absoluta del dato. En una adquisición viva, cierta modificación puede ser inevitable. Lo decisivo es demostrar qué cambios se produjeron, por qué eran necesarios, cómo se limitaron y qué controles permiten confiar en el resultado. La trazabilidad, la reproducibilidad del análisis y la transparencia metodológica son las garantías que convierten una captura técnicamente compleja en evidencia jurídicamente defendible.

El IMELCF puede fortalecer su respuesta mediante un protocolo nacional de datos volátiles, un programa de validación de herramientas, capacitación diferenciada, revisión por pares, infraestructura segura y auditorías periódicas. La coordinación previa con el Ministerio Público y la disponibilidad de información para la contradicción deben formar parte del sistema. Estas medidas no solo mejoran la

eficacia investigativa; también protegen la intimidad, el derecho de defensa y la legitimidad de la decisión judicial.

La actualización no debe concebirse como una reforma aislada. La tecnología cambia con rapidez y obliga a revisar procedimientos, capacidades y riesgos de manera continua. La convergencia entre Derecho, informática forense y gestión de calidad permitirá que Panamá responda a la criminalidad digital sin debilitar las garantías del proceso penal. Una evidencia bien preservada es aquella cuyo recorrido puede explicarse, verificarse y discutirse desde la primera intervención hasta su presentación ante el tribunal.

Referencias

Acurio del Pino, S. (s. f.). Manual de manejo de evidencias digitales y entornos informáticos (versión 2.0). Organización de los Estados Americanos.

Association of Chief Police Officers. (2012). ACPO good practice guide for digital evidence (5th ed.). ACPO.

Ayers, R., Brothers, S., & Jansen, W. (2014). Guidelines on mobile device forensics (NIST Special Publication 800-101, Revision 1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-101r1

Brezinski, D., & Killalea, T. (2002). Guidelines for evidence collection and archiving (RFC 3227). Internet Engineering Task Force. https://doi.org/10.17487/RFC3227

Casey, E. (2011). Digital evidence and computer crime: Forensic science, computers, and the Internet (3rd ed.). Academic Press.

Consejo de Europa. (2001). Convenio sobre la Ciberdelincuencia. Consejo de Europa.

Instituto de Medicina Legal y Ciencias Forenses. (2015). Manual de procedimiento del sistema de cadena de custodia (versión 02). IMELCF.

Instituto de Medicina Legal y Ciencias Forenses. (s. f.). Objetivos y funciones institucionales. IMELCF.

International Organization for Standardization. (2012). ISO/IEC 27037:2012, Information technology—Security techniques—Guidelines for identification, collection, acquisition and preservation of digital evidence. ISO.

International Organization for Standardization. (2015a). ISO/IEC 27041:2015, Information technology—Security techniques—Guidance on assuring suitability and adequacy of incident investigative method. ISO.

International Organization for Standardization. (2015b). ISO/IEC 27042:2015, Information technology—Security techniques—Guidelines for the analysis and interpretation of digital evidence. ISO.

International Organization for Standardization. (2015c). ISO/IEC 27043:2015, Information technology—Security techniques—Incident investigation principles and processes. ISO.

Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). Guide to integrating forensic techniques into incident response (NIST Special Publication 800-86). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-86

López Delgado, M. (2007). Análisis forense digital. Organización de los Estados Americanos.

Panamá. (2008). Ley 63 de 28 de agosto de 2008, que adopta el Código Procesal Penal. Gaceta Oficial de la República de Panamá.

Palmer, G. (2001). A road map for digital forensic research. Digital Forensic Research Workshop.

Sosa, M. E. (2023). Evidencia digital: Su importancia en la investigación. Revista Pensamiento Penal.