PROTOCOLO DE PROCESO FORENSE
DE EVIDENCIA DIGITAL
(VERSIÓN GRUPO LAZARUS)

Valencia Estado Carabobo, Venezuela — Julio 2026

Prólogo

El vertiginoso avance tecnológico ha transformado la realidad social, económica y jurídica, imponiendo a los operadores del sistema de justicia el desafío de comprender y gestionar la evidencia digital como un elemento probatorio esencial en la investigación penal. Este manual nace con el propósito de ofrecer una guía técnica y procesal para el tratamiento de la evidencia digital, fundamentada en los principios científicos y forenses que garantizan su integridad, autenticidad y admisibilidad en el proceso judicial.

Su basamento legal descansa en el Manual Único de Cadena de Custodia de Evidencias Físicas y en el Compendio de Protocolos de Actuación para el Fortalecimiento de la Investigación Penal en Venezuela, instrumentos normativos que establecen los criterios rectores para la obtención, resguardo y disposición final de las evidencias. A diferencia de otros documentos, este manual se circunscribe estrictamente a la informática forense, abarcando el análisis de dispositivos computacionales, sistemas digitales y telefonía celular.

Esta obra constituye la primera actualización de un proyecto en permanente evolución, por lo que se encuentra abierta a sugerencias, modificaciones y aportes de la comunidad forense y jurídica. El manual ha sido ideado en el marco de la práctica forense del Máster en Ciberdelincuencia de la Universidad Internacional de La Rioja en España, del Dr. Jaime A. Riera Seivane, abogado con ejercicio en los Estados Unidos, y de la Abg. Nuria Álvarez, del reconocido bufete Lazarus, Álvarez & Asociados, S.C, quienes han conjugado su experiencia internacional y nacional para ofrecer una herramienta clara, útil y técnicamente rigurosa.

Agradecemos profundamente al Centro de Investigación Informática Lazarus, C.A, en la persona del Prof. Julio Cesar Baudi, experto en Informática Forense por sus valiosos aportes en la corrección, actualización y validación técnica de este manual, basados en la experiencia cotidiana de su Laboratorio Forense. La rigurosidad y el conocimiento práctico de su equipo, del cual forma parte la Abg. Nuria Álvarez, han sido fundamentales para ajustar los procedimientos a la realidad operativa de la investigación digital, garantizando que esta obra responda a los estándares más exigentes de la práctica forense contemporánea. Su compromiso con la excelencia y la formación especializada constituye un pilar indispensable para el desarrollo de esta disciplina en el país.

El presente manual no pretende sustituir, en modo alguno, las normativas vigentes en materia de investigación penal y cadena de custodia, sino que se erige como una herramienta complementaria que las afianza, amplía y especifica desde una óptica técnica y práctica. Incorpora apreciaciones legales actualizadas que reflejan la interpretación más reciente de los marcos normativos, y se adapta al desarrollo de nuevas tecnologías, ofreciendo lineamientos específicos para el abordaje de dispositivos, sistemas y entornos

digitales emergentes, sin que ello implique modificación o interpretación contraria a las disposiciones legales que están vigentes.

Confiamos en que este manual sirva como un faro orientador para peritos, abogados y funcionarios judiciales, facilitando la comprensión y manejo de la evidencia digital en el marco del debido proceso y el respeto a los derechos humanos.

Autores

Abg. Jaime A. Riera Seivane

Abogado con amplia trayectoria internacional, ejerce en los Estados Unidos con admisiones ante el Tribunal Supremo de los EE.UU., cortes de apelaciones federales y tribunales estatales de Maryland, Puerto Rico, Washington D.C. y Massachusetts. Su experiencia abarca el litigio civil y administrativo, la supervisión de procesos de descubrimiento de prueba en materia de lavado de dinero, Ley de Secretos Bancarios y delitos financieros, así como la revisión de documentos electrónicos y la coordinación de equipos forenses en casos de alta complejidad. Su dominio de herramientas tecnológicas y su visión estratégica han sido fundamentales para la estructuración de este manual, asegurando que los procedimientos descritos respondan a los más altos estándares de la práctica forense internacional.

Abg. Nuria Álvarez

Abogada egresada de la Universidad Arturo Michelena y Licenciada en Relaciones Industriales por la Universidad de Carabobo. Cursante de Postgrado en Derecho Penal y Criminología, directora del Escritorio Jurídico Lazarus, Álvarez & Asociados, S.C. y Asesora Legal del Centro de Investigación Informática Lazarus, C.A, combina su sólida formación en derecho con una profunda experiencia en Derecho Laboral e Informático. Se ha desempeñado como analista de evidencia digital y facilitadora en cursos y talleres sobre ciberseguridad, Pentester, OSINT, delitos informáticos y aspectos jurídicos de la informática forense, los cuales han sido impartidos tanto en instituciones privadas como en organismos de investigación penal y universidades. Su labor como investigadora y articulista en temas de derecho informático la ha consolidado como una referente en la materia, y su trabajo en el Laboratorio Forense del Centro de Investigación Informática Lazarus ha sido determinante para la actualización y validación práctica de este manual, garantizando su aplicabilidad en el contexto forense venezolano.

Valencia Estado Carabobo, Venezuela — Julio 2026

ÍNDICE GENERAL

Valencia Estado Carabobo, Venezuela — Julio 2026

1. Introducción

Este manual tiene como objetivo estandarizar la actuación de peritos, expertos, funcionarios y abogados en el manejo de las evidencias digitales (Evidencias de Dispositivos Digitales - EvDD y Evidencias Digitales - EvSSD) dentro del proceso penal venezolano. Se fundamenta en los principios de la cadena de custodia, establecidos en el Manual Único de Cadena de Custodia de Evidencias Físicas y el Compendio de Protocolos de Actuación para el Fortalecimiento de la Investigación Penal, vigentes en Venezuela, garantizando la integridad, autenticidad y preservación de la información digital desde su obtención hasta su disposición final, en apego al respeto de los derechos humanos y el debido proceso.

2. Marco Normativo de referencia

Propósito de esta sección
Identifica las fuentes normativas internacionales y venezolanas que rigen cada fase del protocolo.

2.1 Estándares Internacionales

Norma / Estándar	Descripción
ISO/IEC 27037:2012 ISO/IEC 27037:2016	Directrices para identificación, recolección, adquisición y preservación de evidencia digital.
ISO/IEC 27042:2016	Directrices para análisis e interpretación de evidencia digital.
NIST SP 800-86	Guía para integrar técnicas forenses en la respuesta a incidentes de seguridad y solucionar problemas operativos de TI
RFC 3227	Directrices para recolección y archivo de evidencias digitales tras un incidente de seguridad.

2.2 Marco Jurídico Venezolano

Instrumento Legal	Artículos Relevantes
Constitución de la República Bolivariana de Venezuela G.O.E N° 36.860 de fecha 30 de diciembre de 1.999	Arts. 28, 48, 49, 60
Manual Único de Cadena de Custodia de Evidencias Físicas G.O Nº 41.247 agosto de 2017	Proceso de Cadena de Custodia de evidencias
Ley Orgánica de Reforma del Código Orgánico Procesal Penal (COPP) G.O.E 6.644 17 de septiembre de 2021	Arts. 181-183, 186-188, 194, 223-228
Ley Especial contra los Delitos Informáticos (LECDI) G.O Nº 37.313 del 30 de octubre de 2001	Arts. 1-33 (tipos penales)
Resolución conjunta mediante la cual se crea el Compendio de Protocolos de Actuación para el Fortalecimiento de la Investigación Penal[1]	Protocolos de investigación y cadena de custodia
Decreto con Fuerza de Ley sobre Mensajes de Datos y Firmas Electrónicas G.O Nº 37.148 del 28 de febrero del 2001	Arts. 4-7, 9, 16 y 18.
Ley de Infogobierno G.O N.º 40.274 del 17 de agosto de 2013	Art. 5

2.3 Marco Conceptual[2]

Adquisición Digital (pág. 21): "Proceso por el cual se obtiene una copia exacta o imagen forense de un sitio de suceso digital o directamente de las evidencias contenidas en él, aplicando para ello, técnicas especializadas de copiado y que permitan verificar su integridad.".

[1] En adelante le llamaremos Compendio de Protocolos de Investigación Penal.
[2] Compendio de Protocolos de Actuación para el Fortalecimiento de la Investigación Penal en Venezuela.

Adquisición en vivo (pág. 21): "Levantamiento de datos o información desde su origen, sin interrumpir la continuidad de un servicio en línea. En sistemas o dispositivos que no puedan ser interrumpidos."

Adquisición por selección (pág. 21): "Proceso de adquisición definido de acuerdo a escogencia previa de datos o información."

Archivos temporales (pág. 21): "Con el fin de contener información de forma transitoria durante el tiempo que se crea un archivo estándar, y luego al cerrarse dicho programa, de manera automática el archivo temporal debería eliminarse".

Audio (pág. 22): "Es la codificación digital de una señal eléctrica, que representa una onda sonora o secuencia de ondas, que ha sido convertida a un formato numérico, para ser almacenado en un medio digital".

Autenticidad (pág. 22): "Acreditado de cierto positivo por los caracteres, requisitos o circunstancias que en ello concurre".

Binario (pág. 22): "Es todo aquello que solo tiene dos estados posibles, y desde el punto de vista puramente físico, todos los datos de un ordenador digital lo son (estén ya en memoria primaria o secundaria), ya que están compuestos de cadenas de bits que solo pueden tomar valores de 0 o 1".

Búsqueda (pág. 22): "Acción de buscar. Hacer algo para hallar a alguien o algo. Hacer lo necesario para conseguir algo".

Caché (pág. 23): "Capa de almacenamiento de datos de alta velocidad que almacena un subconjunto de datos, normalmente transitorios, de modo que las solicitudes futuras de dichos datos se atienden con mayor rapidez que si se debe acceder a los datos desde la ubicación de almacenamiento principal."

Código fuente: (Ley de Infogobierno) "Texto escrito en un lenguaje de programación específico, contentivo de un conjunto de instrucciones que se puede compilar para generar un programa que se ejecuta en un computador, es el conjunto de líneas de texto escritas en un lenguaje de programación específico, que al ser procesadas por los compiladores e interpretadores adecuados, generan exactamente dicho programa que es ejecutado por el computador".

Computador: (LECDI) "dispositivo o unidad funcional que acepta data, la procesa de acuerdo con un programa guardado y genera resultados, incluidas operaciones aritméticas o lógicas".

Contraseña (password): (LECDI) "secuencia alfabética, numérica o combinación de ambas, protegida por reglas de confidencialidad utilizada para verificar la autenticidad de la autorización expedida a un usuario para acceder a la data o a la información contenidas en un sistema".

Copia instantánea (snapshot) (pág. 23): "Copia instantánea de volúmenes"

Data (pág. 23): "Hechos, conceptos, instrucciones o caracteres representados de una manera apropiada para que sean comunicados, transmitidos o procesados por seres humanos o por medios automáticos y a los cuales se les asigna o se les puede asignar significado".

Dato o información digital de interés procesal (pág. 24): "Referido a datos o información digital(intangible), almacenada o transmitida en binario, en un medio tecnológico no accesible directamente, tales como: texto, audio, traza telefónica, vídeo, imagen y datos híbridos, entre otro; cuya forma de adquisición de la información, es a través de los entes y órganos del Estado e instituciones de carácter privado que ofrecen servicios públicos por medio del principio de oficiosidad y aquellos de acceso directo a través de su procesamiento técnico especializado en la Web, Internet, plata formas tecnológicas, entre otros; realizado por los(as) expertos(as), peritos(as), especialistas o forenses que son autorizados o facultados."

Datos volátiles (pág. 24): "Datos que son especialmente propensos a perderse y modificar fácilmente."

Dispositivo Digital (pág. 24): "Equipo electrónico de naturaleza (tangible), que puede ser utilizado para procesar, almacenar y transmitir datos o información digital."

Documento: (LECDI): "registro incorporado en un sistema en forma de escrito, video, audio o cualquier otro medio, que contiene data o información acerca de un hecho o acto capaces de causar efectos jurídicos".

Embalaje (pág. 24): "Envolver las evidencias de acuerdo a sus características."

Entorno computacional (pág. 24): "Combinación de hardware y software que permite realizar una serie de actividades para un fin común".

eSIM (pág. 24): "Chip integrado en la placa base del propio teléfono, que hace las mismas funciones que la SIM tradicional".

Especialista calificado (pág. 25): "Son especialistas en la provisión de servicios forenses digitales e informáticos, que comienzan a abordar el incidente siendo el principal respondedor al análisis forense digital, dentro de la estructura afectada; teniendo como objetivo consignar la evidencia digital a los peritos informáticos, el rol del Especialista Calificado le permitirá un conjunto de principios y técnicas para detectar, mitigar, minimizar, controlar, identificar, recopilar, documentar de ser necesario adquirir con herramientas especializadas la evidencia digital."

Etiqueta (pág. 25): "Señal, marca, rotulado que se adhiere a un objeto para su identificación, clasificación o valoración, en su mayoría es empleado en los vehículos importados".

Evidencia digital (pág. 25): "Información o datos, almacenados o transmitidos en forma binaria, vinculados a un hecho punible y se clasifican en: (me quedo con esta, la definición propuesta me parece engorrosa a la interpretación de muchos)".

Experto (pág. 25): "Persona con conocimientos especiales y experiencia sobre determinada ciencia o arte, y con nombramiento jurídico para realizar un peritaje en determinado hecho punible."

Expoliación (pág. 25): "Acto de hacer o permitir cambios a la evidencia digital potencial, que disminuye su valor probatorio."

Fijación (pág. 26): "Acción y efecto de fijar o fijarse. Pieza que sirve para fijar. Hacer fija o estable una cosa".

Firmware: (LECDI): "programa o segmento de programa incorporado de manera permanente en algún componente de hardware".

Fragmento (pág. 26): "Parte de un todo que se separa de manera voluntaria o involuntaria".

Función hash (pág. 26): "Es un algoritmo matemático que transforma cualquier bloque arbitrario de datos en una nueva serie de caracteres con una longitud fija. Independientemente de la longitud de los datos de entrada, el valor hash de salida tendrá siempre la misma longitud. Es la huella digital matemática única e irrepetible generada a partir de un archivo, un disco o un conjunto de datos. Funciona mediante un algoritmo criptográfico (como SHA-256 o SHA-512) que procesa la información y la convierte en una cadena alfanumérica de longitud fija"

Hardware: (LECDI) "equipos o dispositivos físicos considerados en forma independiente de su capacidad o función, que forman un computador o sus componentes periféricos, de manera que pueden incluir herramientas, implementos, instrumentos, conexiones, ensamblajes, componentes y partes"

Hecho punible (pág. 26): "Acción ilícita que merece castigo o ser sancionado por una pena."

Herramientas forenses (pág. 26): "Programas (software) y equipos (hardware) que permiten adquirir de manera segura la información almacenada en cualquier medio físico o digital sujeto a evaluación informática forense."

Hibridas (pág. 26): "Resultado de la combinación de audio, video, texto e imagen."

Hora del sistema (pág. 27): "Hora generada por el reloj del sistema y utilizada por el sistema operativo, no la hora calculada por el sistema operativo.". En este concepto se debe hacer una observación forense, la Hora del Sistema es la hora legible por el usuario, generada por el reloj de tiempo real (RTC) del hardware y leída por el sistema operativo. Es modificable mediante ajustes manuales o sincronización con servidores de tiempo (NTP), por lo que no debe considerarse como una referencia absoluta y fiable para fines de cadena de custodia, por lo cual debe manejarse la hora del Reloj Monotónico que es un Contador interno del procesador que se incrementa de manera constante e ininterrumpida desde el inicio del sistema. No es modificable por el usuario ni por procesos externos, lo que lo convierte en una referencia sólida para medir intervalos de tiempo y establecer la secuencia cronológica de eventos en un análisis forense. Debe tomarse en cuenta en la fase de adquisición de datos volátiles.

Huella (pág. 27): "Vestigio, señal, rastro o indicio. Es el rastro único (metadatos, *hash*, dirección IP o datos biométricos) que deja un usuario en la tecnología."

Identificar (pág. 27): "Establecer, demostrar o reconocer la identidad de una cosa o persona. Acción de reunir las características o elementos que diferencian a una persona de las demás."

Imagen (pág. 27): "Es la representación exacta en forma digital de un objeto, persona o animal, en forma bidimensional y vectorial, por objetos geométricos, dependientes cada uno de ellos, definido por atributos matemáticos de forma, de posición, a partir de una matriz numérica, frecuentemente en binario."

Imagen forense (pág. 27): "Proceso de creación de una copia bit a bit de un medio de almacenamiento digital"

IMEI (International Mobile Station Equipment Identity) **(pág. 28): "**Código de 15 dígitos pregrabado por el fabricante para identificar cada equipo móvil a nivel mundial. Está compuesto por un código de identificación de marca y modelo otorgado a los fabricantes por la GSMA (Global System Mobile Association)."

Incidente de seguridad informática (pág. 28): "Es una falla, ataque o intento del mismo, que afecta una infraestructura tecnológica y atenta contra los principios y políticas de seguridad establecidas." Es el activador del protocolo forense.

Individualización (pág. 28): "Diferenciación que se hace atribuyendo características distintivas. Consiste en señalar las características particulares que hace que un individuo o cosa sea diferente de los demás de su especie o clase".

Información (pág. 28): "Significado que el ser humano le asigna a la data utilizando las convenciones conocidas y generalmente aceptadas".

Informática Forense (pág. 28): "Disciplina auxiliar de las ciencias forenses que permite recopilar y analizar datos de sistemas informáticos, redes, comunicaciones inalámbricas y dispositivos de almacenamiento, y de cualquier medio físico o digital que almacene datos e información, para presentarlos como una prueba admisible frente a autoridades judiciales, es decir, los tribunales."

Infraestructuras críticas: (Ley de Infogobierno): "Infraestructuras críticas también conocidas como estratégicas, son aquellas que proporcionan servicios esenciales y cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre tales servicios".

Instrumentos (pág. 28): "Son todos aquellos objetos que se usan como medio para arribar a un fin; es por lo tanto un medio o recurso, para lograr lo que se desea conseguir, es un término general aplicable a todos los medidores, recipientes y otras herramientas que se pueda imaginar para realizar síntesis y análisis en el ámbito de los diversos trabajos criminalísticos".

Línea de tiempo (Timeline) (pág. 29): "Parámetro de variante de tiempo que denota un punto en el tiempo con respecto a una referencia de tiempo común. Permite la reconstrucción cronológica ordenada de todos los eventos digitales relevantes extraídos de un dispositivo. Es la narrativa histórica que asiste a los investigadores comprender la secuencia exacta de las acciones ocurridas en el(los) dispositivo(s)."

Medios de almacenamientos limpios (sonetizados) (pág. 30): "Aplicación de técnicas de limpieza y borrados seguro en dispositivos de almacenamientos para que puedan ser utilizados como repositorios de evidencias digitales".

Memoria RAM (pág. 30): "Memoria de acceso aleatorio, es la memoria principal que permite almacenar datos de un sistema a corto plazo, para que un equipo pueda accesar de forma más rápida a programas y procesos dentro de ella". Si bien la memoria RAM se considera tradicionalmente una de las evidencias más volátiles, el perito debe tener en cuenta que, en sistemas que utilizan tecnologías de memoria no volátil (NVM) o persistente, la información puede no perderse al cortar la alimentación eléctrica. En estos casos excepcionales, la "volatilidad" de la RAM se ve alterada, por lo que el orden de recolección debe ajustarse a la

realidad técnica del dispositivo intervenido, priorizando siempre la captura de aquellos datos que, por su naturaleza o el contexto del caso, corran un riesgo inminente de desaparición.

Mensajes de Datos (LSMDFE) "Toda información inteligible en formato electrónico o similar que pueda ser almacenada o intercambiada por cualquier medio.

Metadata (pág. 30): "Son un conjunto de datos que describen el contenido informativo de un recurso, de archivos o de información de los mismos. Permite identificar los documentos, eliminando errores e inconsistencias, de manera que se facilita su manejo cotidiano. Permite identificar, de forma estructurada el origen, las características, el uso y las modificaciones de un archivo digital por su autor, fechas de creación y/o modificación, su geolocalización y/o el dispositivo empleado".

Métodos (pág. 30): "Modo estructurado y ordenado de obtener un resultado, descubrir la verdad de forma objetiva con suficientes garantías y sistematizar los conocimientos."

Micro SIM (pág. 30): "En 2003 se desarrolló este nuevo tipo de tarjeta, aunque no fue hasta la llegada deliPad que Apple hizo que toda la industria empezase a adoptarla. Con un tamaño de12×15 milímetros, se creó para ampliar la memoria y seguridad de las SIM, pero acabó aprovechándose para hacerla más pequeña."

Mini SIM (pág. 30): "Es la que actualmente conocemos como SIM a secas, pero que no fue el primer modelo existente. Fue el estándar desarrollado para que la tarjeta SIM cupiera en los teléfonos móviles, y tiene un tamaño de 15×25 milímetros".

Nano SIM (pág. 30): "Una evolución sobre las Micro SIM, con la que se consiguió crear una tarjeta todavía más pequeña de sólo 12×9 milímetros. Empezó a llegar en 2012, y su misión fue la de optimizar el espacio del hardware de un teléfono, manteniendo su tamaño externo, pero con mayor volumen para ciertos componentes."

Log (o registro): Es el archivo o conjunto de datos donde un sistema, aplicación o dispositivo registra cronológicamente los eventos, actividades, mensajes de error, transacciones y otra información relevante sobre su funcionamiento. Estos registros son fundamentales para el diagnóstico de fallos, el monitoreo del rendimiento y, en el ámbito forense, para la reconstrucción de eventos y la identificación de actividades sospechosas. En los sistemas Linux, la gestión de logs ha evolucionado significativamente con la adopción de systemd y su servicio journald. Tradicionalmente, los logs se almacenaban en archivos de texto plano, sin embargo, a partir de la implementación de systemd (Linux 11), los logs pasan a ser gestionados por systemd-journald, que los almacena en un formato binario estructurado e indexado.

Orden de volatilidad (pág. 31): "Es el orden en el cual la evidencia es más susceptible al cambio, es decir, recolectar en primer lugar los datos que tienen mayor probabilidad de ser cambiados, modificados o perdidos." Este es el principio rector que establece la secuencia prioritaria para la recolección de evidencias digitales, determinando que los datos con mayor probabilidad de ser alterados, modificados o perdidos deben ser adquiridos en primer lugar. Este orden no es estático y debe ser evaluado por el perito en función de las circunstancias del caso y la arquitectura del sistema.

Origen (pág. 31): "Lugar de donde procede una persona o cosa".

Peritaje (pág. 32): "Conjunto de procedimientos que permiten obtener información de interés criminalístico, a través del análisis de evidencias físicas o digitales, con la finalidad de aportar a la investigación, los datos necesarios para el esclarecimiento del hecho delictivo que, de manera activa o pasiva, guardan relación con éste".

Perito (pág. 32): "Los o las peritos deberán poseer título en la materia relativa al asunto sobre el cual dictaminarán, siempre que la ciencia, el arte u oficio estén reglamentados. En caso contrario, deberán designarse a personas de reconocida experiencia en la materia. Los o las peritos serán designados o designadas y juramentados o juramentadas por el Juez o Jueza, previa petición del Ministerio Público, salvo que se trate de funcionarios adscritos o funcionarias adscritas al órgano de investigación penal, caso en el cual, para el cumplimiento de sus funciones bastará la designación que al efecto le realice su superior inmediato. Serán causales de excusa y recusación para los o las peritos las establecidas en Código Orgánico Procesal Penal. La o el perito deberá guardar reserva de cuanto conozca con motivo de su actuación."

Perito informático de campo (PIC) (pág. 32): "Criminalista, profesional a fin a las áreas de las tecnologías, capacitado en informática forense para actuar como el primer respondedor en la escena de un incidente para la realización inherente a la adquisición de evidencia digitales".

Perito informático de laboratorio (PIL) (pág. 32): "Criminalista, profesional a fin a las áreas de las tecnologías, capacitado en informática forense quien tiene conocimientos especializados, habilidades y capacidades para manejar una amplia gama de análisis de dispositivos digitales, tiene la capacidad para actuar en campo como en el laboratorio."

Probabilidad (pág. 32): "La probabilidad de la ocurrencia de cualquier forma particular de un evento, calcula la relación entre el número de formas o veces que el evento puede producirse en esa forma para el número total de maneras de que podría ocurrir en cualquier forma."

Procedimiento (pág. 32): "Práctica establecida a seguir en la realización de una tarea especificada o bajo circunstancias específicas".

Procesamiento de data o de información: (LECDI): "realización sistemática de operaciones sobre data o sobre información, tales como manejo, fusión, organización o cómputo".

Programa: "LECDI): "plan, rutina o secuencia de instrucciones utilizados para realizar un trabajo en particular o resolver un problema dado a través de un computador".

Prueba (pág. 33): "Es la actividad necesaria que implica demostrar la verdad de un hecho, su existencia o contenido según los medios establecidos por la ley".

Reconocimiento Legal (pág. 33): "Experticia que consiste en la descripción de las evidencias relacionadas con un hecho delictivo, en la cual se deja constancia de sus características, particulares e individualizantes."

Registro (pág. 33): "Acción de registrar. Documento donde se relacionan ciertos acontecimientos o cosas; especialmente aquellos que deben constar permanentemente de forma oficial."

Registro Digital (pág. 33): "Mediante los libros de control interno se asigna un número de entrada a cada muestra siempre y cuando presenten expedientes distintos."

Registro Manual (pág. 33): "Mediante los libros de control interno se asigna un número de entrada a cada muestra siempre y cuando presenten expedientes distintos".

Rotulación (pág. 33): "Acción y efecto de rotular. Poner un rotulo a algo o en alguna parte. Título de un escrito o de una parte suya. Letrero o inscripción con que e indica o da a conocer el contenido, objeto o destino de algo, o la dirección a que se envía".

Seguridad: (LECDI): "Condición que resulta del establecimiento y mantenimiento de medidas de protección que garanticen un estado de inviolabilidad de influencias o de actos hostiles específicos que puedan propiciar el acceso a la data de personas no autorizadas o que afecten la operatividad de las funciones de un sistema de computación".

SIM (Módulo de Identidad del Suscriptor) (pág. 34): "Es una evidencia digital que contiene información crítica que vincula de forma inequívoca al usuario con el dispositivo y la línea telefónica, permitiendo a los peritos establecer la identidad, los contactos, la geolocalización y los registros de comunicación. Es una tarjeta de plástico que posee un chip electrónico adherido, el cual se inserta en teléfonos móviles, tabletas o dispositivos inteligentes, el cual almacena de manera segura datos de un suscriptor, tales como número de teléfono, claves de acceso y datos de la operadora de telefonía."

SimCard Módulo de Identificación de Suscriptor (pág. 34): "es una tarjeta de plástico que posee un chip electrónico adherido, el cual se inserta en teléfonos móviles, tabletas o dispositivos inteligentes, el cual almacena de manera segura datos de un suscriptor, tales como número de teléfono, claves de acceso y datos de la operadora de telefonía."

Sistema: (LECDI) "cualquier arreglo organizado de recursos y procedimientos diseñados para el uso de tecnologías de información, unidos y regulados por interacción o interdependencia para cumplir una serie de funciones específicas, así como la combinación de dos o más componentes interrelacionados, organizados en un paquete funcional, de manera que estén en capacidad de realizar una función operacional o satisfacer un requerimiento dentro de unas especificaciones previstas".

Sistema de Posicionamiento Global (GPS) (pág. 34): "Sistema que permite conocer la posición de un objeto o de una persona gracias a la recepción de señales emitidas por una red de satélites."

Sitio de Suceso digital (pág. 35): "Espacio intangible que se encuentra contenido en un dispositivo digital o una infraestructura tecnológica, relacionado con la perpetración de un presunto hecho punible, cuyo acceso debe hacerse mediante técnicas y herramientas especializadas de informática forense. Los procesos en este sitio sólo pueden ser realizados por el Perito Informático de Laboratorio (PIL)".

Software: (LECDI): "información organizada en forma de programas de computación, procedimientos y documentación asociados, concebidos para realizar la operación de un sistema, de manera que pueda proveer de instrucciones a los computadores, así como de data expresada en cualquier forma, con el objeto de que éstos realicen funciones específicas".

Técnica (pág. 35): "Procedimiento o conjunto de reglas, normas o protocolos, que tienen como objetivo obtener un resultado determinado."

Tecnología de Información (pág. 35): "Rama de la tecnología que se dedica al estudio, aplicación y procesamiento de data, lo cual involucra la obtención, creación, almacenamiento, administración, modificación, manejo, movimiento, control, visualización, distribución, intercambio, transmisión o recepción de información en forma automática, así como el desarrollo y uso del "hardware", "firmware", "software", cualesquiera de sus componentes y todos los procedimientos asociados con el procesamiento de data".

Tecnología Operativa (sistemas operativos) **(pág. 36): "**Es el uso de hardware y software para monitorear y controlar los procesos físicos, los dispositivos y la infraestructura de un entorno industrial (gas, energía, agua, petróleo, entre otros.)"

Tecnologías disruptivas (pág. 36): "Es cualquier innovación tecnológica que cambie drásticamente la forma en que interactúan las personas; operan las empresas y las industrias."

Tecnologías incrementales (pág. 36): "Son cambios graduales y paulatinos que se realiza en un producto o tecnología, los cuales se aprecian en periodos de tiempos."

Texto (pág. 36): "Estos archivos están compuestos de bytes que representan caracteres ordinarios como letras, números y signos de puntuación, codificados en un sistema de escritura que forma una unidad de sentido, mediante caracteres del código estándar de Intercambio de información (American Standard Codefor Information Interchange (ASCII)."

TICs (pág. 36): "Tecnología de la Información y las Comunicaciones, son el conjunto de recursos, herramientas, equipos, programas informáticos, aplicaciones, redes y medios; que permiten la compilación, procesamiento, almacenamiento, transmisión de información como: Voz, datos, texto, videos e imágenes."

Traslado (pág. 36): "Acción de trasladar o trasladarse de lugar. Cambiar de lugar a una persona o una cosa."

Tratamiento (pág. 36): "Proceso o procedimiento por el que se aplica un protocolo de protección a la muestra, indicio o evidencia; Usar o manejar una cosa de la manera que se expresa."

Trazas (pág. 36): "Huella, vestigio o rastro de una cosa o persona."

Video (pág. 37): "Es el conjunto imágenes, audio y otros datos digitales, que representan una escena en movimiento."

Vincular (pág. 37): "Unir o relacionar una persona o cosa con otra".

Virus: (LECDI): "programa o segmento de programa indeseado que se desarrolla incontroladamente y que genera efectos destructivos o perturbadores en un programa o componente del sistema".

Volatilidad: "Propiedad de la información digital que determina su susceptibilidad a alterarse o desaparecer al interrumpirse la energía eléctrica o por la interacción del sistema (ej. Memoria RAM, registros, caché)"

Web (pág. 37): "Constituye la información que se encuentra en una dirección de internet. Página electrónica, página digital o ciber página es un documento digital complejo, que puede integrar y/o contener texto, sonido, vídeo, programas, enlaces, imágenes, hipervínculos y otros elementos, adaptado para la World Wide Web, y que puede ser accedida y visualizada mediante un navegador web."

2.4 Garantías Constitucionales aplicables al proceso forense

El manejo de la evidencia digital en el marco de una investigación penal debe realizarse con estricto apego a las garantías constitucionales que protegen los derechos fundamentales de las personas. La Constitución de la República Bolivariana de Venezuela establece un conjunto de principios y derechos que constituyen el soporte jurídico esencial para la validez y licitud de cualquier actuación forense. Estas son las principales garantías constitucionales que rigen el proceso de obtención, análisis, resguardo y disposición de la evidencia digital:

2.4.1. **Debido proceso y defensa (Artículo 49):** El artículo 49 de la Constitución consagra el debido proceso como un derecho inviolable aplicable a todas las actuaciones judiciales y administrativas. En el ámbito forense, ello implica:

2.4.1.1 **Notificación y defensa:** Toda persona tiene derecho a ser notificada de los cargos por los cuales se le investiga y a disponer del tiempo y medios adecuados para ejercer su defensa. Ello exige que el perito o funcionario que maneje la evidencia digital garantice que la parte investigada tenga acceso a la información pertinente, en la medida que la ley lo permita.

2.4.1.2 **Nulidad de pruebas ilícitas:** Son nulas las pruebas obtenidas mediante violación del debido proceso. Por tanto, cualquier evidencia digital recolectada, adquirida o analizada sin respetar los procedimientos establecidos (cadena de custodia, orden judicial, respeto a la intimidad) carecerá de valor probatorio.

2.4.1.3 **Presunción de inocencia:** Toda persona se presume inocente mientras no se pruebe lo contrario. El perito debe abstenerse de emitir opiniones que prejuzguen la culpabilidad y debe limitarse a exponer los hechos y resultados técnicos de manera objetiva e imparcial.

2.4.2. **Inviolabilidad de las comunicaciones privadas (Artículo 48):** El artículo 48 garantiza el secreto e inviolabilidad de las comunicaciones privadas en todas sus formas. Esto es especialmente relevante para la evidencia digital, ya que:

2.4.2.1 **Interferencia judicial:** Las comunicaciones (correos electrónicos, mensajes de texto, llamadas, datos de aplicaciones) no pueden ser interferidas sino por orden de un tribunal competente, con el cumplimiento de las disposiciones legales y preservando el secreto de lo privado que no guarde relación con el proceso.

2.4.2.2 **Alcance de la orden:** La orden judicial debe ser específica y limitada a la información relevante para la investigación, sin que pueda extenderse a datos no relacionados con el hecho punible. El perito debe ceñirse estrictamente al alcance de la autorización judicial.

2.4.3. **Inviolabilidad del hogar y recintos privados (Artículo 47):** El artículo 47 protege la inviolabilidad del hogar doméstico y todo recinto privado. En el contexto de la obtención de evidencias digitales:

2.4.3.1 **Allanamiento con orden judicial:** No se puede ingresar a un domicilio, oficina o recinto privado para incautar dispositivos digitales sin una orden judicial previa, salvo los casos de flagrancia previstos en la ley.

2.4.3.2 **Respeto a la dignidad:** Aun en los casos de allanamiento, se debe respetar la dignidad de las personas y evitar la divulgación de información privada no relacionada con la investigación.

2.4.4. **Derecho a la protección del honor, vida privada, intimidad, propia imagen, confidencialidad y reputación (Artículo 60):** Este artículo establece que toda persona tiene derecho a la protección de su honor, vida privada, intimidad, propia imagen, confidencialidad y reputación. Además, dispone que la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar. En el proceso forense digital:

2.4.4.1 **Límites al acceso a datos personales:** El perito debe limitar su análisis a la información estrictamente necesaria para la investigación, evitando la intromisión en datos personales no relevantes.

2.4.4.2 **Confidencialidad:** Toda la información obtenida durante el peritaje debe ser manejada con estricta confidencialidad, y su divulgación debe limitarse a las autoridades competentes y a las partes en el proceso.

2.4.4.3 **Protección de datos biométricos y sensibles:** La evidencia digital que contenga datos biométricos, imágenes, grabaciones o información sobre la salud, orientación sexual, creencias, etc., debe ser tratada con especial cuidado para no vulnerar el derecho a la intimidad.

2.4.5. **Derecho a la protección por parte del Estado (Artículo 55):** El artículo 55 consagra el derecho de toda persona a la protección por parte del Estado a través de los órganos de seguridad ciudadana, frente a situaciones que constituyan amenaza, vulnerabilidad o riesgo para la integridad física, las propiedades, el disfrute de sus derechos y el cumplimiento de sus deberes. En el ámbito forense:

2.4.5.1 **Seguridad de los peritos y funcionarios:** El Estado debe garantizar la seguridad de quienes participan en la obtención y manejo de evidencias digitales, especialmente en situaciones de alto riesgo.

2.4.5.2 **Protección de víctimas y testigos:** La información digital que pueda poner en riesgo la integridad de víctimas o testigos debe ser manejada con las medidas de protección necesarias, de conformidad con la ley.

2.4.6. **El proceso como instrumento fundamental para la realización de la justicia (Artículo 257):** El artículo 257 establece que el proceso es un instrumento fundamental para la realización de la justicia. Las leyes procesales deben propender a la simplificación, uniformidad y eficacia de los trámites, adoptando un procedimiento breve, oral y público, sin sacrificar la justicia por la omisión de formalidades no esenciales. Esto implica:

2.4.6.1 **Eficacia y celeridad:** El perito debe actuar con la diligencia necesaria para evitar dilaciones indebidas en el análisis de la evidencia digital, siempre que ello no comprometa la calidad técnica del peritaje.

2.4.6.2 **Formalidades esenciales:** La cadena de custodia y la documentación del proceso son formalidades esenciales que garantizan la licitud de la prueba y no pueden ser omitidas bajo el pretexto de simplificación.

2.4.7. **Derecho de acceso a la información y a los archivos administrativos (Artículo 143):** Este artículo garantiza a los ciudadanos el derecho a ser informados oportuna y verazmente por la Administración Pública sobre el estado de las actuaciones en que estén directamente interesados, y a conocer las resoluciones definitivas que se adopten, así como a acceder a los archivos y registros administrativos, con las limitaciones propias de la investigación criminal y la intimidad de la vida privada. En el proceso forense:

2.4.7.1 **Acceso a la evidencia:** Las partes en el proceso tienen derecho a conocer la evidencia digital que se les imputa, en los términos que establezca la ley, sin que ello implique una vulneración de la investigación.

2.4.7.2 **Limitaciones:** El acceso puede ser restringido en los casos de información clasificada como secreta o confidencial por razones de seguridad nacional o de investigación criminal, siempre que dicha restricción sea proporcional y esté legalmente justificada.

2.4.8. **Tutela judicial efectiva (Artículo 26):** El artículo 26 garantiza el derecho de toda persona a acceder a los órganos de administración de justicia para hacer valer sus derechos e intereses, a la tutela efectiva y a obtener con prontitud la decisión correspondiente. Ello implica que:

2.4.8.1 **La evidencia digital debe ser admisible y útil:** El perito debe asegurar que la evidencia que presenta cumpla con todos los requisitos técnicos y legales para ser valorada por el juez.

2.4.8.2 **El juez debe controlar la legalidad de la prueba:** El órgano jurisdiccional tiene el deber de verificar que la evidencia digital ha sido obtenida y analizada respetando las garantías constitucionales.

Las garantías constitucionales antes señaladas constituyen el pilar fundamental sobre el cual debe edificarse todo el proceso forense digital. Su observancia no solo asegura la validez jurídica de la prueba, sino que también protege los derechos fundamentales de las personas involucradas en la investigación, contribuyendo a la realización de una justicia efectiva y al fortalecimiento del Estado democrático y social de Derecho. Por ello, el perito, el funcionario y el abogado deben conocer y aplicar estos principios en cada una de las fases del tratamiento de la evidencia digital, desde la obtención hasta la disposición final.

2.5 Garantías procesales

Los(as) peritos (as), forenses, expertos (as), criminalistas, investigadores (as) penales y especialistas del Ministerio Público, al igual que los (as) adscritos (as) a los órganos con competencia en materia de investigación penal en los procesos y procedimientos criminalísticos, técnicos, científicos y forenses, deben de mantener la mayor objetividad e imparcialidad en todo el proceso investigativo forense para garantizar los derechos de la(s) personas investigada(s) de conformidad al Art. 49 de la Constitución de la República Bolivariana de Venezuela. Toda persona investigada se le debe garantizar sus derechos constitucionales a cabalidad.

Valencia Estado Carabobo, Venezuela — Julio 2026

Toda prueba obtenida durante el proceso investigativo que se desvíe de las garantías técnicas recogidas en las buenas prácticas forense, de la Constitución, de la Gaceta Oficial 6.644, Compendio de Protocolos de Actuación para el Fortalecimiento de la Investigación Penal, del Manual Único de Cadena de Custodia de Evidencia Forense carecerá de valor jurídico conforme a la Constitución.

2.6 Evidencias digitales

Tomando en consideración los criterios y principios que rigen al Manual Único de Cadena de Custodia de Evidencias Físicas y, para los efectos de este protocolo, se fundamenta la clasificación de las evidencias digitales de acuerdo a lo descrito en el Compendio de Protocolos de Actuación para el Fortalecimiento de la Investigación Penal en Venezuela, las cuales son susceptibles de peritajes, en consonancia con los aspectos científicos, forenses, criminalísticos y jurídicos contemplados en la legislación penal y leyes especiales vigentes que rigen la materia de la forma siguiente:

Según su naturaleza y estado en:

1. Según su capacidad de aprehensión:

a) Tangibles: Son todas aquellas evidencias físicas sensibles al sentido del tacto.
b) Intangibles: Son todas aquellas evidencias físicas que no son sensibles al sentido del tacto.

2. Según su naturaleza y peritaje a realizar:

Evidencias de Tecnologías de Información, Comunicaciones y Operativas (TICS y OT)

La tecnología de información es cualquier dato o información digital y el equipo tecnológico que lo contiene, susceptible de peritaje forense, que pueda ser admitido como prueba en un proceso legal.

Las evidencias de Tecnologías de Información, Comunicaciones y Operativas se clasifican por su naturaleza en:

1. Evidencias en Dispositivo Digital (EvDD): Referido a un equipo electrónico de naturaleza (tangible), que puede ser utilizado para procesar, almacenar y transmitir datos o información digital que se encuentra inmerso en un hecho punible.

2. Evidencias Digitales (EvSSD): Referido a datos o información digital (intangible), almacenada o transmitida en binario, en un medio tecnológico de acceso directo, estos son: texto, audio, vídeo, imagen y datos híbridos; donde se cometió el hecho delictivo.

Tecnologías susceptibles de análisis forenses:

La tecnología de información es cualquier dato o información digital y el equipo tecnológico que lo contiene, susceptible de peritaje forense, que pueda ser admitido como prueba en un proceso legal.

1. Dispositivos computacionales portátiles o no (Servidor, PC, notebook/netbook, tabletas, raspberryetc).

2. Sistemas de telefonía y comunicaciones móviles (arquitectura GSM Sistema Global para las comunicaciones Móviles) La telefonía IP (telefonía por protocolo de Internet) y accesorios (tarjetas de memoria, tarjetas SIM, eSIM entre otros.).

3. Dispositivos de sistema satelital de navegación global (GNSS), sistema de posicionamiento global (GPS, Glonass, BeiDou, Galileo, entre otros).

4. Vehículos aéreos pilotados a distancia conocidos como dron o drones (RPAS).

5. Dispositivos de almacenamiento (memorias flash, discos externos, etc.), dispositivos ópticos (DVD, CD, Blu-ray).

6. Dispositivos seguridad de redes: enrutador, detector de intruso, corta fuego (Firewall), distribuidor inteligente (Switch) y cualquier otro equipo que genere sus propios logs.

7. Sistemas de vigilancia y reconocimiento: Sistema de circuito cerrado de televisión (DVR, NVR, cámara ip), todo dispositivo de vigilancia que sea utilizado para almacenar o transmitir video.

8. Dispositivo de internet de las cosas (Internet Of Things) sistemas interconectados con aplicaciones que permite ejecutar acciones como la activación o desactivación del equipo. (relojes inteligentes, televisores inteligentes, ciudades inteligentes, electrodomésticos, entre otros).

9. Tecnología de cadena de bloques (Blockchain).

10. Tecnologías de realidad aumentada.

11. Inteligencia artificial-aprendizaje automático (Machine Learning).

12. Computación en la nube (computer and servicescloud), contemplar todo almacenamiento en la nube bien sea creado por proveedor de servicio o por el usuario.

13. Computación cuántica.

14. Robótica.

15. Cualquier otro tipo de tecnología existente dentro de las gamas de la Tecnología de Información y Comunicación.

Otras tecnologías

1. Redes sociales.
2. Portal Web.

3. Correo Electrónico.

Tecnologías Operativas

Las infraestructuras críticas también conocidas como estratégicas, son aquellas que proporcionan servicios esenciales y cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre tales servicios, lo podemos observar en el servicio eléctrico, transporte masivo, gas, petróleo y defensa.

Cabe destacar, que la tecnología de información, comunicación y operativa antes mencionada no son limitativas, permitiendo incorporar aquellas tendencias incrementales y disruptivas que se vayan desarrollando con el avance tecnológico.

3. Proceso Forense para las evidencias de naturaleza tecnológica de la información, comunicación y operacional.

Basado en los protocolos del compendio, el tratamiento de la evidencia digital se estructura en las siguientes fases:

3.1. Fase de Obtención Técnica
- **3.1.1. Protección Física**
  - 3.1.1.1. En el Sitio Físico
  - 3.1.1.2. En el Dispositivo Digital (EvDD)
- **3.1.2. Observación y Búsqueda**
- **3.1.3. Fijación**
  - 3.1.3.1. Fotográfica/Videográfica
- **3.1.4. Colección y Adquisición**
  - 3.1.4.1. Dispositivos Apagados
  - 3.1.4.2. Dispositivos Encendidos
- **3.1.5. Embalaje, Rotulación y Traslado**
  - 3.1.5.1. Embalaje
  - 3.1.5.2. Rotulación
  - 3.1.5.3. Registro de Cadena de Custodia
  - 3.1.5.4. Traslado

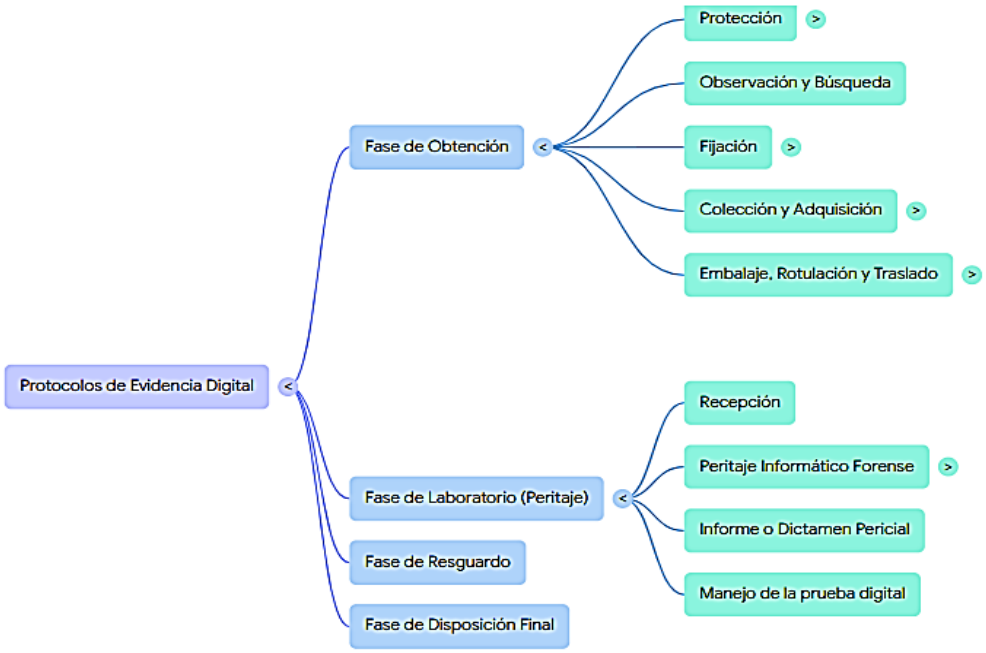
3.2. Fase de Laboratorio (Peritaje)
- **3.2.1. Recepción**
- **3.2.2. Peritaje Informático Forense**
  - 3.2.2.1. Adquisición Forense
  - 3.2.2.2. Análisis de la Evidencia Digital
  - 3.2.2.3. Análisis de la Nube
  - 3.2.2.4. Adquisición por Derivación

3.2.3. Informe o Dictamen Pericial

3.2.3.2 Manejo de la prueba digital para proteger su admisibilidad

3.3. Fase de Resguardo
3.4. Fase de Disposición Final
4. Obtención por Consignación
5. Obtención por aseguramiento (flagrancia)
6. Obtención por Derivación

7. Flujograma del Proceso Forense Digital



A continuación, se desarrollan cada una de las fases:

3.1. Obtención Técnica

Base Normativa
ISO/IEC 27037:2016 §6.1 y Compendio de Protocolos (sección de sitio de suceso digital)

Objetivo de la Fase
Detectar, reconocer y documentar la existencia de posibles fuentes de evidencia del sitio de suceso digital o en el entorno investigado, sin alterar su estado original. El Personal Forense de respuesta

inmediata debe describir adecuadamente los procedimientos que se siguieron y explicar los pasos tomados para la adquisición del material digital considerado delictivo.

De igual forma, de conformidad con la ISO/IEC 27037-2016 el personal forense de respuesta inmediata debe poder justificar todas las acciones y metodologías empleadas en el manejo de dispositivos digitales obtenidas durante la investigación. Dicha justificación debe ser demostrada que el método empleado era la mejor opción al momento de incautar el material digital objeto de la investigación.[3]. Deben validarse las herramientas forenses a utilizar para que no alteren los datos.

La Obtención Técnica constituye el procedimiento científico, criminalístico y forense destinado al levantamiento de evidencias en el sitio del suceso. Este proceso no se ejecuta de forma autónoma, sino que se encuentra subordinado a la dirección y supervisión del Ministerio Público y de los órganos jurisdiccionales competentes, siendo materializado por los cuerpos de investigación penal, en el marco del debido proceso y la cadena de custodia.

3.1.1. Protección:

Se trata de proceder a asegurar y delimitar el perímetro del área a ser investigado y permitir la entrada, exclusivamente de personal forense autorizado.

Actividades a realizar:

3.1.1.1. En el Sitio Físico:

3.1.1.1.1 Identificación del funcionario como requisito previo al ingreso: El primer paso en el procedimiento de obtención técnica es la identificación plena del funcionario o funcionaria actuante, quien deberá acreditar su condición mediante la presentación de su credencial oficial y, de ser necesario, la orden judicial que lo faculta para ingresar al sitio del suceso. Esta identificación, que debe realizarse antes de cualquier otra diligencia, garantiza la transparencia de la actuación, el respeto a los derechos de las personas presentes y la validez de todas las actuaciones posteriores, en estricto cumplimiento del debido proceso y la normativa legal vigente.

3.1.1.1.2 Retirar al usuario(a) que esté trabajando en el equipo, a fin de evitar cualquier alteración o pérdida de la información contenida en el dispositivo digital. (Si estas personas manejan el equipo a ser incautado, se le debe solicitar las claves de acceso, así como cualquier otra información que permita el acceso al material digital.[4]

3.1.1.1.3 Deshabilitar las entradas y salidas de señales de comunicación (alámbricas o inalámbricas) que puedan contaminar, destruir o modificar la evidencia que se encuentre en el sitio del suceso. (Wi-Fi, Bluetooth o cualquier otro tipo de señal digital o telemática)

[3] ISO/IEC 27037-2012 sección 5.3.5.

[4] Compendio de Protocolo de Investigación Penal a la pág. 67.

y, en dispositivos móviles, utilizar inhibidores de señales para evitar acceso remoto a los instrumentos digitales o telemáticos).

3.1.1.1.4 Establecer mecanismos para proteger la información sensitiva o crítica de los sistemas. (Proteger los sistemas, redes y su capacidad, para que estos sigan funcionando, sin afectar su operatividad.)

3.1.1.2. Abordaje del Sitio del Suceso en Situaciones de Alto Riesgo

3.1.1.2.1 El procedimiento estándar de protección del sitio del suceso presupone un escenario controlado y sin amenaza activa. Sin embargo, cuando existe un riesgo inminente de pérdida de vida o posibilidad de enfrentamientos armados, la preservación de la vida humana es la prioridad absoluta, por encima de cualquier diligencia de recolección de evidencia digital.En estos casos, el abordaje debe estructurarse en las siguientes fases:

3.1.1.2.1 Evaluación dinámica de riesgos: El funcionario debe mantener distancia segura, observar desde cobertura, identificar la fuente del peligro y solicitar apoyo de unidades especializadas (tácticas, negociadores, servicios médicos) antes de proceder.

3.1.1.2.2 Aseguramiento del perímetro y neutralización de la amenaza: Se debe establecer un perímetro de seguridad amplio y, si hay enfrentamiento activo, actuar para neutralizar la amenaza aplicando el uso progresivo y diferenciado de la fuerza. No se debe intentar acceder al equipo digital mientras persista el peligro.

3.1.1.2.3 Estabilización del escenario y atención a víctimas: Una vez controlada la amenaza, se debe proteger a los ciudadanos, evacuar el área si es necesario y atender las emergencias médicas de inmediato.

3.1.1.2.4 Abordaje forense del sitio (post-amenaza): Solo cuando el escenario sea declarado seguro, se procederá con el abordaje forense estándar (observación, fijación, colección, embalaje y traslado de evidencias). La solicitud de claves de acceso al usuario solo debe realizarse una vez que la situación esté completamente controlada y el usuario se encuentre bajo custodia.

3.1.1.2.5 Documentación del incidente: En el acta policial se dejará constancia de la naturaleza de la amenaza, las acciones tomadas, cualquier alteración de la evidencia derivada del enfrentamiento y la cadena de custodia de los dispositivos recuperados.

3.1.1.2.6 Se recomienda para la seguridad del perito o funcionario, el uso de chaleco y casco balístico en situaciones de riesgo.

3.1.1.3. En el Dispositivo Digital (EvDD):

3.1.1.3.1 Realizar protección permanente sobre la evidencia de dispositivos digitales para evitar el acceso de terceros.

3.1.1.3.2 Retirar al usuario(a) que esté trabajando en el equipo, a fin de evitar cualquier alteración o pérdida de la información contenida en el dispositivo digital.

3.1.1.3.3 Evaluar las diferentes técnicas preventivas establecidas en la MUCCEF para impedir el acceso de terceros con intenciones maliciosa a dispositivos digitales conectados de forma alámbrica o inalámbrica.

3.1.1.3.4 Mantener encendido el dispositivo (lectores o copiadores, computación personal, comunicacionales y portables de posicionamiento, vigilancia y reconocimiento), para realizar el proceso de observación y fijación de la actividad. (Si están prendidos (On), no se deben de apagar. Si están en la posición de apagados (off) no se deben de prender.)

3.1.1.3.5 Utilizar dispositivos digitales externos previamente acondicionados para el proceso de adquisición a fin de no alterar la metadata o el contenido de las evidencias digitales.

3.1.1.3.6 Si hay sistema de baterías o de energía de *backup* para los sistemas, se debe de evaluar el nivel de autonomía de la batería correspondiente a los dispositivos portátiles, antes de realizar el *triage* (análisis en vivo) a fin de evitar el apagado durante el análisis o el traslado.[5]

3.1.1.3.7 Estudiar los elementos que conforman el entorno informático, con la finalidad de aplicar medidas para la protección del sitio digital y la evidencia en sí.

3.1.1.3.8. Cualquier otro medio necesario para garantizar la debida protección.

3.1.2. Observación y búsqueda:

Objetivo de la Fase

La fase de observación preliminar en la informática forense constituye el reconocimiento técnico inicial del entorno digital y físico objeto de investigación o de la escena de suceso digital. Su objetivo primordial es la identificación exhaustiva de activos informáticos, la determinación del estado de volatilidad de los datos en memoria y la delimitación del perímetro de seguridad lógica. Es considerada la etapa crítica para garantizar la integridad de la cadena de custodia, permitiendo la documentación sistemática del estado operativo de los sistemas y la planificación estratégica de las técnicas de adquisición de evidencias posteriores.

Cualquier desvío de los pasos aquí establecidos pudiera violar garantías constitucionales y procesales en el ámbito jurídico y administrativo.

Actividades a realizar:

3.1.2.1 Realizar una exploración en el sitio a través de método de escaneo con el internet de las cosas, así como la verificación de ranuras, puertos USB, unidad de ópticos, entre otros; que permita la búsqueda de evidencias tecnológicas en dispositivos digitales relacionados con el hecho delictivo.

3.1.2.2 Identificar todos los dispositivos electrónicos (ordenadores, móviles, terminales, impresoras, máquinas de escaneos, máquinas de clonación, discos duros, CD, DVD, artículos de almacenamiento digital y todo equipo cuya definición se encuentre en la normativa vigente, encendidos y apagados.)

3.1.2.3 Evaluar la configuración horaria de los sistemas (CCTV, bases de datos) y compararla con la hora oficial.

3.1.2.4 Se debe señalizar todo el equipo en la escena. La señalización del mismo constituye la demarcación o distinción, relacionada con un objeto, actividad o situación determinada

[5] *Ibidem*.

que suministra una indicación mediante un diagrama o rótulo, color, señal luminosa, señal acústica, comunicación verbal o señal gestual. Se puede realizar con los siguientes materiales: Alfanuméricos (utilización de números y letras), cuerdas, adhesivos, conos, banderines, flechas (se usan para señalar específicamente la evidencia que se requiere fijar).

3.1.2.5 Todos los métodos de almacenamiento empleados deben de estar debidamente esterilizados previo a la transferencia de información digital.[6]

3.1.3. Fijación

Objetivo de la Fase

Consiste en un conjunto de métodos y técnicas que se utilizan para dejar constancia de cómo se encuentra el lugar y las evidencias al momento del abordaje, plasmándose las características generales, particulares y de detalle.

La importancia de este procedimiento radica en registrar de manera escrita, fotográfica, planimétrica, videográfica e imagenológica, entre otras; las condiciones y características que presenten los lugares y las evidencias físicas, a fin de facilitar la comprensión futura del trabajo realizado, lograr la evaluación y análisis correcto de los hechos, así como fundamentar hipótesis en la investigación.

Se realiza antes, durante y después del abordaje, incluso se deberá cumplir si no se localiza alguna evidencia.

Dentro de los tipos de fijación del lugar de interés criminalístico y de sus evidencias, serán de cumplimiento obligatorio, la fijación escrita, la fijación videográfica, la fotográfica, y la fijación planimétrica, cuando corresponda según el tipo de evidencia.

Siempre se debe consultar el Manual Único de Cadena de Custodia de Evidencias Físicas a la página 27 (MUCCEF).

Actividades a realizar:

3.1.3.1. Fotográfica/Videográfica:

3.1.3.1.1 Georreferenciar cada dispositivo in situ, ya sea fotográficamente o mediante vídeo la pantalla del dispositivo de la actividad en ejecución, sin intervenir en su funcionalidad.

3.1.3.1.2 Fijar fotográficamente o mediante video los dispositivos conectados externamente, inserciones, conexiones alámbricas, para dejar constancia de su relación.

3.1.3.1.3 En caso de equipos móviles identificar e individualizar (imei, numero de SimCard, número eSIM, la identificación del modelo, número de serie, color y marca)

3.1.3.1.4 Si se puede, realizar un diagrama que contenga las posiciones de los sistemas, los cables, en sus posiciones originales, que estaban conectados a ellos (con etiquetas si en lo posible

[6] *Ibidem*.

con colores) y en los portales o terminales que estaban conectados y hacía donde terminaban para que se puedan reproducir en el laboratorio.[7]

3.1.3.1.5 Si el Perito Forense de Campo (PFC) encuentra que el sistema está conectado a una nube, debe hacer un mapa de todo el sistema para saber dónde buscar, quién tiene acceso y cómo extraer los datos sin contaminarlos ni perderse nada importante, identificando si la información se encuentra en una nube pública o privada. El PFC debe de reconocer que no todos los sitios de almacenamiento de información digital (nube, NAS y SA) van a poder ser inmediatamente identificables. Por lo que debe asumir que las mismas existen.[8].

3.1.3.1.6 Si las personas que hubieran estado presente durante el operativo hubieran provisto de la información de acceso a la nube, de forma voluntaria el PFC debe documentar el proceso de adquisición de dicho acceso, indicando: La ubicación física de los datos, si está en territorio nacional o extranjero, si los datos están en posesión de un proveedor de servicios de Internet (ISP), o solo el usuario tiene control o ambos lo tienen.

3.1.3.1.7 Verificar y documentar la evidencia digital adquirida que esté relacionada con la información básica asociada con la cuenta o proveedor de servicio en la nube.

3.1.3.1.8 Si el dispositivo no está sincronizado con la nube, se deberá de realizar la sincronización, copia de seguridad y/o respaldo necesario para almacenarlo localmente o procesarla por un dispositivo tecnológico donde sea resguardada en un proveedor que brinda servicio de almacenamiento en la nube para su adquisición y preservación.

3.1.4. Colección y Adquisición

Objetivo de la Fase

El objetivo principal de esta fase es obtener y preservar de manera segura la evidencia digital, garantizando su integridad y autenticidad. Para ello, se extraen los datos de interés (archivos activos, eliminados, metadatos y datos volátiles) y se crean copias exactas o imágenes forenses de los dispositivos, asegurando que la evidencia original no sea alterada.

Además, esta fase busca mantener la cadena de custodia y la admisibilidad legal de la evidencia. Se documenta meticulosamente cada acción, se calculan funciones hash para verificar la integridad de los datos y se implementan medidas como el uso de inhibidores de señales para evitar alteraciones remotas, garantizando que la evidencia sea confiable y válida en un proceso judicial.

En este tipo de escenario pueden intervenir criminalistas de campo previamente capacitados(as) en la colección de evidencias digitales, especialista en informática forense, perito(a) informático de campo y perito informático de laboratorio, o cualquier otro funcionario(a) con habilidades, destrezas y conocimiento específico del área.

[7] ISO/IEC-27037-2016. 6.2.1.

[8] *Ibidem* a la sección 5.4.2.

Actividades a realizar:

3.1.4.1. Antes de tocar cualquier dato, el PFC debe calcular su "huella digital" a través del cálculo del valor hash y anotarla en la planilla de Registro de cadena de Custodia. Una vez copiada la evidencia, debe calcular esa huella nuevamente. Si ambas coinciden, queda demostrado que los datos no fueron alterados durante el proceso. Si no coinciden, algo falló y el procedimiento debe repetirse. Todo queda registrado con fecha, hora y herramienta utilizada, garantizando que lo que el tribunal o juzgado, en su momento, pueda analizar es exactamente lo mismo que se encontró en la escena digital durante su fase de intervención.[9]

3.1.4.1.1 La selección del algoritmo hash para la verificación de integridad de la evidencia digital será determinada por el funcionario o perito actuante, conforme a los criterios técnicos y protocolos establecidos por su laboratorio. La elección del método (SHA-256, SHA-512 u otros) dependerá de la naturaleza del caso y de las políticas internas de la unidad forense, garantizando siempre la fiabilidad, auditabilidad y reproducibilidad de la cadena de custodia.

3.1.4.1.2 El PFC debe intentar maximizar la cantidad de datos preservados mediante las acciones de recolección y adquisición. Sin embargo, puede ser necesario priorizar los elementos según su volatilidad y/o su relevancia/valor probatorio potencial.[10]

3.1.4.1.3 Evitar exponer el dispositivo digital objeto de estudio, a campos electromagnéticos, temperaturas extremas y golpes que puedan averiarlo u ocasionarle pérdida de los datos que contiene.

3.1.4.1.4 **Adquisición Digital:** Proceso por el cual se obtiene una copia exacta o imagen forense de un sitio de suceso digital o directamente de las evidencias contenidas en él, aplicando para ello, técnicas especializadas de copiado y checksum que permitan verificar su integridad. Se debe realizar una **imagen forense** (copia bit a bit) de los medios de almacenamiento.[11]

3.1.4.1.5 Nunca se debe de trabajar sobre el original del equipo a clonar. Esto puede afectar la integridad de la pieza digital y ser impugnada en el proceso judicial.

3.1.4.2 Dispositivos Apagados

Si los tipos de dispositivos digitales se encuentran apagados, aplicar los lineamientos que establece el Manual Único de Cadena de Custodia de Evidencias Físicas, considerando:

3.1.4.2.1 Identificar y documentar las características del dispositivo. (imei, numero de SimCard, número eSIM, datos de laptop, computador, disco duro, marca, modelo, tipo de cargador, ranura USB, entre otros).

3.1.4.2.2 Verificar y documentar la ubicación de los dispositivos de almacenamiento externo encontrados.

3.1.4.2.3 No encenderlo para evitar la ejecución de programas de autoprotección.

[9] Compendio de Protocolo de Investigación Penal op cit. a la pág. 68.
[10] *Op cit* a 6.8.

[11] *Ibidem* a la pág. 27.

3.1.4.2.4 Extraer el dispositivo de almacenamiento externo, si aplica.

3.1.4.2.5 Asegurar que el dispositivo digital este realmente apagado. En caso de estar en modo de espera o suspensión remitirlo al laboratorio en ese estado o contactar al perito, experto, especialista, forense o técnico en el área.

3.1.4.2.6 Utilizar herramientas antiestáticas (brazalete, alfombrilla) que proteja al dispositivo para así disminuir la descarga electroestática.

3.1.4.2.7 Levantar la evidencia de dispositivos digital por los laterales de ésta.

3.1.4.2.8 Hacer desconexión física de los dispositivos digitales, retirando primero el extremo conectado al dispositivo digital y luego al extremo conectado a la toma eléctrica.

3.1.4.2.9 Etiquetar los puertos para que el sistema pueda reconstruirse en una etapa posterior.

3.1.4.2.10 Inmovilizar el interruptor con cinta adhesiva para evitar que cambie de estado.

3.1.4.2.11 Documentar el acceso. Obtener la contraseña (código, pin, usuario, patrón de desbloqueo, etc.) de los dispositivos digitales que lo requieran.

3.1.4.2.12 La práctica de desconectar la batería de una computadora portátil durante el proceso de adquisición forense debe ser evaluada con especial cuidado. Existe la creencia errónea de que la NVRAM (memoria no volátil) requiere energía de la batería para mantener los datos, pero la tecnología actual (celdas de estado sólido, como memoria Flash, FeRAM, MRAM) no requiere corriente eléctrica en reposo, ya que utilizan transistores de compuerta flotante que atrapan cargas eléctricas permanentes, o materiales ferroeléctricos que polarizan sus átomos para retener la información. Por lo tanto, la NVRAM moderna no pierde sus datos al retirar la batería. Sin embargo, el verdadero riesgo de desconectar la batería radica en la pérdida de datos volátiles almacenados en la memoria RAM, así como en la posible corrupción de archivos abiertos o en proceso de escritura, y en la pérdida de información de caché o de archivos temporales que no han sido escritos en el disco. Además, algunos sistemas pueden bloquear el acceso al disco o requerir claves de cifrado que se pierden al cortar la energía bruscamente.

3.1.4.2.13 Como los datos volátiles se pueden perder al apagar el equipo, se debe recopilar la información rápidamente y en el orden correcto: primero conexiones de red y sesiones activas (cambian rápido), luego configuración de red (más estable). Se puede usar un script automatizado desde un CD para hacerlo de forma consistente y guardar los datos en un USB o unidad de red.[12]

3.1.4.2.14 Debe estar consciente que al apagar el sistema no solo afecta la capacidad de realizar imágenes de flujo de bits y muchas copias de seguridad lógicas, sino que también puede cambiar qué datos del sistema operativo se conservan.

3.1.4.2.15 **Métodos para apagar el sistema**: Para evitar que esa información se pierda o se altere al apagar, existen dos métodos:

3.1.4.2.15.1 **Apagado ordenado del Sistema Operativo (SO):** Casi todos los sistemas operativos ofrecen una opción de apagado normal. Este proceso hace que el SO realice tareas de limpieza antes de cerrarse: cerrar archivos abiertos, eliminar archivos temporales y posiblemente borrar el archivo de intercambio. Sin embargo, un apagado ordenado puede eliminar evidencia maliciosa, como *rootkits* en memoria o rastros de troyanos. Normalmente se ejecuta desde la cuenta del administrador o del usuario activo con privilegios suficientes.

[12] NIST SP 800-86 sección 5.2.1.3.

3.1.4.2.15.2 Depende del SO se podrían corromper datos, como archivos abiertos o archivos a los que se estaba accediendo en ese momento, si se produce una pérdida de energía. En estos casos, un apagado ordenado es generalmente lo más recomendable, a menos que los archivos de intercambio o los archivos de datos temporales sean de particular interés, o que el sistema pueda contener rootkits, troyanos u otros programas maliciosos que podrían activarse durante un apagado ordenado.

3.1.4.2.15.3 Retirar portales o entradas energéticos: Desconectar el cable de alimentación de la parte trasera del equipo o las baterías en las portátiles u otros dispositivos similares puede mantener intacto los archivos del sistema.

3.1.4.2.15.4 Algunos dispositivos pueden perder la información contenida de en ellos si se remueven las baterías. Este es el caso de los móviles y algunas tabletas o cualquier dispositivo portátil[13].

3.1.4.2.16 **Considerar los siguientes aspectos en dispositivos IOT (Internet de las cosas)**, preferiblemente debe ser valorado por un PIC o criminalista de campo capacitado:

3.1.4.2.16.1 Evaluar la función y capacidad del dispositivo en el Internet de las cosas (IOT) para valorar la potencialidad de la evidencia digital.

3.1.4.2.16.2 Evaluar si el dispositivo en el Internet de las cosas (IOT) conduce a datos almacenados en otros sitios como proveedor de servicio en la nube, computadora personal, dispositivos móviles u otro de IOT.

3.1.4.2.16.3 Los dispositivos digitales de IOT deben estar aislados de su(s) red(es), un método a utilizar es desconectar la alimentación del dispositivo o quitar la alimentación de la batería.

3.1.4.2.16.4 Utilizar un método de aislamiento de red en caso que el dispositivo no se puede apagar.

3.1.4.2.16.5 Extraer la batería en los casos donde lo permita para aislar el dispositivo, este debe estar embalado en un contenedor diferente al dispositivo digital para evitar que se habilite el sistema conexión.

3.1.4.2.16.6 Evaluar la seguridad del dispositivo, considerando el diseño de seguridad (tecnología diseñada para invocar la seguridad relacionada con los datos almacenados localmente, las conexiones de red o ad hoc y la transmisión de datos).

3.1.4.3. Dispositivos Encendidos

En estos escenarios digitales las técnicas son variadas, puede ser una captura de pantalla de un sitio web, copia instantánea (Snapshots) en la nube, una réplica de información digital o una imagen forense; en este sentido, queda a criterio del experto, perito, especialista o forense las técnicas y herramientas a usar en dependencia del caso:

[13] *Ibidem* sección 5.2.2

3.1.4.8.1 Evaluar el nivel de autonomía de la batería correspondiente a los dispositivos portátiles, antes de realizar el triaje (análisis en vivo) a fin de evitar el apagado durante el análisis o durante el traslado. Desconectar y documentar las redes alámbricas o inalámbricas.

3.1.4.3.2 Documentar el acceso: Obtener credenciales de acceso (contraseñas, patrones de desbloqueo) si es posible.

3.1.4.3.3 Adquirir los elementos de interés criminalístico de manera inmediata en el dispositivo digital que se encuentren encendido y que su carga no permita mantenerlo activo hasta su traslado al laboratorio.

3.1.4.3.4 Verificación de Integridad: Calcular y registrar el valor hash (ej. SHA-256, SHA-512) de las evidencias adquiridas.

3.1.4.3.5 **Adquisición en Vivo:** Si la carga es insuficiente o es un sistema crítico, se debe priorizar una adquisición en vivo de los datos volátiles (memoria RAM, procesos activos, conexiones de red, particiones y archivos de intercambio (swap), procesos de red y del sistema operativo en ejecución; información de los sistemas de ficheros y datos contenidos en los sectores de los dispositivos por bloque de interés criminalístico de manera inmediata en el dispositivo digital que se encuentren encendido.

3.1.4.3.5.1 Evaluar los métodos e interfaz de conexión (remoto o local) a utilizar para la adquisición de la evidencia digital.

3.1.4.3.5.2 En los casos de infraestructura o servicios críticos, se debe aplicar la adquisición en vivo manteniendo la continuidad del servicio.

3.1.4.3.5.3 Emplear medios esterilizados de almacenamiento que permita la transferencia y depósito de la información a objeto de realizar el tratamiento de evidencia digital.

3.1.4.3.5.4 Adquirir la evidencia digital con programas y dispositivos especializados en dicha tarea.

3.1.4.3.5.5 Aplicar métodos de verificación de la integridad de la evidencia adquirida, para asegurar que la evidencia digital no fue alterada y que la copia obtenida sea idéntica al contenido de la evidencia en dispositivos digitales de origen.

3.1.4.3.5.6 En relación al análisis en vivo, este también se aplicará a sistemas de vigilancia y otros sistemas que causen afectación a terceros si son ininterrumpidos o apagados.

3.1.4.3.6 **Dispositivos encendidos que no ameritan adquisición en sitio:**

3.1.4.3.6.1 Apagar el dispositivo de posicionamiento global (GPS) y no encenderlo, para evitar que registre la ruta de traslado al laboratorio.

3.1.4.3.6.2 En caso de aeronaves pilotadas a distancia, verificar si se encuentran encendido revisando las conexiones remotas, vinculaciones con otros dispositivos (móvil o de nube) y realizar la adquisición in situ antes de proceder a apagarlo.

3.1.4.3.7 **Adquisición por Selección:** Adquirir la evidencia por selección cuando se encuentre en los siguientes casos:

3.1.4.3.7.1 Aplicar a sistemas de grandes volúmenes o por restricciones legales que limiten el alcance de la solicitud. Se realiza una copia lógica de las carpetas o archivos identificados.

3.1.4.3.7.2 Sistema crítico para ser apagado.

3.1.4.3.7.3 Por restricción legal que sólo permita adquirir lo que está definido en el alcance de la solicitud.

3.1.4.3.7.4 Cualquier otro dispositivo digital en el cual se considere que se debe aplica este método.

3.1.4.3.7.5 Documentar la adquisición por selección de la evidencia digital incluyendo lo siguiente:

3.1.4.3.7.6 Identificar carpeta (s), archivo (s) y toda la información relevante disponibles a ser adquirida.

3.1.4.3.7.7 Realizar una adquisición lógica de todos los datos identificados.

3.1.4.3.7.8 Obtener las credenciales de acceso a los sistemas y aplicaciones que serán objeto de la adquisición (base de datos, correos electrónicos, redes sociales, entre otros).

3.1.4.3.7.9 Gestionar ante el tribunal correspondiente la autorización del acceso a los sistemas y aplicaciones que serán objeto de la adquisición (base de datos, correos electrónicos, redes sociales, entre otros), cumpliendo con la normativa legal vigente.

3.1.4.3.7.10 Ubicar, identificar y documentar diagramas de red relacionados con los sistemas y aplicaciones que serán objeto de la adquisición sin exponer la seguridad de la red (sistemas CCTV, bases de datos, comercio electrónico (E-comerce), etc.).

3.1.4.3.8 **Dentro del proceso de adquisición de evidencia digital en entornos de nube**, el PFRI debe verificar la existencia de copias instantáneas del sistema (*snapshots*) con fecha anterior al suceso investigado.

3.1.4.3.8.1 Estas copias, generadas de forma automática o programada por el proveedor de servicios en la nube, constituyen una representación fiel del estado del sistema en un momento determinado, preservando la configuración, los archivos y los datos tal como existían antes de que se produjera de la incautación.

3.1.4.3.8.2 El experto(a), perito(a), especialista o forense debe considerar la determinación del tipo de nube donde se realizará la adquisición de la evidencia digital (privada, comunitaria, pública, híbrida), así como el modelo de servicios utilizado (IaaS, SaaS, Paas, entre otros), con los consecuentes niveles de control de datos asignados al proveedor del servicio de internet (ISP), al usuario(a), arquitectura y topología física y lógica de la nube; y los posibles lugares de almacenamiento de la evidencia o tecnologías utilizadas por los dichos proveedores de servicio (herramientas de auditoría, formatos de metadatos, cifrados, etc.).

3.1.4.3.8.3 El perito debe considerar que la nube puede contener datos de redes sociales, correos electrónicos, y documentos compartidos. La adquisición debe centrarse en la información de la cuenta, y, si es posible, solicitar al proveedor (por vía judicial) los registros de conexión (dirección IP, fechas y horas, dispositivos utilizados) para geolocalizar al usuario

3.1.4.3.8.4 El experto(a), perito, especialista o forense debe seleccionar las acciones apropiadas en función de los recursos disponibles, su conocimiento y comprensión del caso investigado para la adquisición u obtención de la evidencia digital.

3.1.4.3.8.5 Verificar y documentar la evidencia digital adquirida que esté relacionada con la información básica asociada con la cuenta o proveedor de servicio en la nube.

3.1.4.3.8.6 Verificar y constatar las credenciales de acceso de la cuenta o estación de trabajo donde se almacenan evidencia digital (usuario, cuenta de correo electrónico y contraseña), con el objeto de obtener la evidencia correctamente al ingresar los datos por parte la interesada.

3.1.4.3.8.7 Usar algún método a través de API que se pueda obtener desde un dispositivo en investigación que utiliza los servicios en la nube u otros métodos alternativos, en los casos de no ser posible el acceso con las credenciales obtenidas.

3.1.4.3.8.8 Documentar el proceso de adquisición, métodos utilizados, cómo se obtienen los datos, tomar fotografías, capturas de pantalla, registros de facturación o en algunos casos realizar una grabación de la sesión de manera que permita a otro experto, perito, especialista o forense identificar que se ha hecho y evaluar los resultados.

3.1.4.3.8.9 Verificar si existe copias (snapshots) con fecha anterior al suceso que pueda servir para esclarecer el caso investigado.

3.1.4.3.8.10 En los casos que el dispositivo no esté sincronizado con la nube, el experto(a), perito(a), especialista o forense deberá realizar la sincronización, copia de seguridad y/o respaldo necesario para almacenarlo localmente o procesarla por un dispositivo tecnológico donde sea resguardada en un proveedor que brinda servicio de almacenamiento en la nube para su adquisición y preservación.

3.1.4.3.8.11 En los casos que surjan problemas para la obtención o adquisición de datos a través de métodos planificados, el experto(a), perito(a), especialista o forense deberá intentar métodos alternativos y documentarlos mediante capturas de pantalla o fotografías de los datos relevantes.

3.1.4.3.8.12 Calcular y registrar valores hash antes de después de los datos adquiridos.

3.1.5. Embalaje, Rotulación y Traslado

Objetivo de la Fase

El objetivo principal de esta fase es proteger la integridad física y lógica de la evidencia digital desde el momento de su colección hasta su llegada al laboratorio o tribunal. Esto implica aislar los dispositivos de cualquier factor que pueda alterarlos, como campos electromagnéticos, golpes, temperaturas extremas o, en el caso de dispositivos móviles, señales de comunicación remotas que podrían borrar o modificar los datos.

Además, esta fase busca garantizar la cadena de custodia y la identificación inequívoca de la evidencia. Mediante el etiquetado detallado, el registro en la planilla de custodia (incluyendo valores hash y características del dispositivo) y el traslado seguro, se asegura que la evidencia pueda ser rastreada y reconocida en todo momento, manteniendo su autenticidad y validez probatoria para el proceso judicial.

Actividades a realizar:

3.1.5.1. Embalaje

3.1.5.1.1 Aplicar los procedimientos establecidos en el MUCCEF, a fin de proteger las condiciones físicas y estáticas de las evidencias de acuerdo a su naturaleza.

3.1.5.1.2 Empaquetar en dispositivos de almacenamiento (discos externos, CD, DVD) la evidencia digital adquirida en el sitio de suceso digital.

3.1.5.1.3 Identificar las carpetas digitales contenedoras con la información referida a la evidencia digital, siempre aplicando los criterios establecidos en el MUCCEF.

3.1.5.1.4 Embalar los dispositivos móviles utilizando inhibidores de señales.

3.1.5.1.4.1 **Bolsa Faraday**: No se debe introducir el dispositivo encendido en una bolsa Faraday sin antes ponerlo en modo avión, ya que el dispositivo, al no poder comunicarse, puede aumentar la potencia de su señal y generar daños térmicos. La práctica recomendada es: Modo Avión -> Bolsa Faraday.

3.1.5.1.4.2 **Pintura Faraday (habitación)**: Tiene fibra de aluminio y cobre unidad e impide las comunicaciones.

3.1.5.1.4.3 **Lata contra incendios:** Es la versión casera de una bolsa de Faraday, puede usarse para transporte. No se pude manipular el teléfono cuando está adentro.

3.1.5.1.4.4 **Papel aluminio:** Es la versión casera de un aislamiento de la red, puede requerir dos o tres capas para ser eficaz.

3.1.5.1.4.5 **Modo avión:** Utilice este modo para cortar las comunicaciones de WIFi y las comunicaciones celulares al dispositivo.

3.1.5.1.4.6 Para otros dispositivos, embalaje estándar con protección antiestática y acolchado.

3.1.5.2. Rotulación

3.1.5.2.1 Etiquetar el embalaje con los datos de identificación del caso, el dispositivo y el responsable.

3.1.5.3. Registro de Cadena de Custodia

3.1.5.3.1 Incluir los datos del dispositivo (marca, modelo, serial y componentes anexos).

3.1.5.3.2 Incluir el resultado del valor hash en la planilla de cadena de custodia en caso de tratarse de una sola evidencia digital.

3.1.5.3.3 Incluir el nombre, el tamaño y el hash de la imagen forense realizada a contenedores digitales de grandes cantidades de evidencias adquiridas (en el caso del hash), solo si se realiza en el sitio de colección al tratarse de evidencia que no puede ser colectada ni trasladada.

3.1.5.4. Traslado

3.1.5.4.1 Proceso de traslado: Se debe seguir los parámetros según el Manual Único de Cadena de Custodia de Evidencia Físicas (MUCCEF).

3.1.5.4.2 El transporte de la evidencia del lugar de la obtención al laboratorio debe estar garantizada por el manejo correcto y seguro para evitar alteraciones. Se debe evitar, en lo posible, el traslado de las evidencias en vehículos particulares.

3.1.5.4.3 Se debe documentar fehacientemente a todas las personas presentes en el lugar de la obtención, así como al responsable del traslado de la evidencia y los métodos empleados en su transportación. La custodia legal e inmediata del transporte recae de manera exclusiva sobre el experto técnico que ejecutó físicamente el precintado e inició la firma en la planilla de Registro de Cadena de Custodia y es quien debe hacer la entrega de las evidencias colectadas hasta el laboratorio forense, debiendo garantizar en todo momento su integridad e inalterabilidad, y dejando constancia en la Planilla de Registro de Cadena de Custodia de la persona a quien entrega en el Laboratorio.

3.2. Fase de Laboratorio (Peritaje)

Objetivo de la Fase

El objetivo principal de la Fase de Laboratorio (Peritaje) es analizar técnicamente la evidencia digital para extraer, procesar y evaluar la información de interés criminalístico contenida en los dispositivos o archivos adquiridos. Esto se realiza aplicando métodos científicos y forenses que permitan descubrir datos relevantes, como archivos eliminados, metadatos, conexiones de red, mensajes, registros de actividad y cualquier otra huella digital que pueda vincularse con el hecho punible, todo ello sin alterar la evidencia original.

El investigador debe examinar, identificar y extraer la información relevante. Esto puede incluir superar obstáculos como cifrado, compresión o controles de acceso que ocultan datos. El conocimiento de la información en los archivos permitirá al investigador identificar aquellos archivos que requieran investigación más detallada y documentada para propósitos de la investigación.

Actividades a realizar:

3.2.1. Recepción

3.2.1.1 Una vez recibida la prueba de su lugar de obtención, el laboratorio deberá corroborar que la prueba depositada en su localidad es comparable a la bitácora creada en la recuperación u obtención de la misma y al número de investigación que se la ha asignado, así como la identidad del dispositivo (EvDD), es decir se debe verificar la integridad del embalaje (sello de seguridad) antes de la apertura.

3.2.1.2 Verificar la funcionalidad del dispositivo y registrar la fecha, hora y datos existentes en el mismo. En caso de dispositivo bloqueado, dejar constancia de este hecho en la planilla de cadena de custodia.

3.2.1.3 Para evidencias digitales (EvSSD): verificar la integridad de los archivos o imágenes recibidas mediante el cálculo de hashes.

3.2.1.4 Se debe corroborar que los datos de la persona que hace entrega de la evidencia recopilada correspondan con la que aparece en la Planilla de Registro de Cadena de Custodia (PRCC).

3.2.1.5 Constatar que la información plasmada en el documento de solicitud de pericia corresponda con las características de la evidencia física entregada y con la descripción de la misma en la PRCC.

3.2.2. Peritaje Informático Forense

El perito informático de laboratorio (PIL) aplicará los siguientes procesos:

3.2.2.1. Adquisición Forense

3.2.2.1.1 Si no se realizó en campo, se procederá a crear una imagen forense bit a bit del dispositivo o del medio de almacenamiento, utilizando un write-blocker para evitar la modificación del dispositivo original.

3.2.2.1.2 En esta etapa se debe emplear métodos científicos para reconstruir las líneas de tiempo, identificar los autores y las acciones ejecutadas (trazabilidad). Se debe dejar constancia del proceso de calibración y validación de las herramientas forenses empleadas.

3.2.2.1.3 Verificación de Integridad: Calcular y comparar el valor hash (ej. SHA-256, SHA-512) de las evidencias adquiridas con las asentadas en la Planilla de Cadena de Custodia.

3.2.2.1.4 Búsqueda de evidencias digitales: Revisión exhaustiva del contenido del dispositivo (EvDD) para ubicar archivos, metadatos y datos eliminados vinculados con el hecho delictivo.

3.2.2.1.5 Recuperación de archivos eliminados: Procesos para la adquisición de archivos que han sido borrados.

3.2.2.2. Análisis de la Evidencia Digital

3.2.2.2.1 **Análisis Técnico:** Cuando se habla de trazabilidad es la huella indeleble que contiene ese archivo: su origen, líneas de tiempo, el(la)(los) autor(a)(es), su(s) usuario(a)(os)(as), las acciones ejecutadas, y los efectos causados. La trazabilidad es la historia de ese archivo. Nos permite rastrear y recrear el historial completo del documento digital evaluado o investigado; desde su creación, las modificaciones, accesos y aprobaciones, hasta su archivo final o eliminación.[14] En esta etapa, el investigador debe determinar la existencia o no de evidencias digitales contenidas en Web, redes sociales, correos electrónicos o sistemas telemáticos.

3.2.2.2.1.1 Análisis de metadatos: (fechas, autores, geolocalización, etc.).

3.2.2.2.1.2 Análisis de archivos eliminados: (recuperación de datos mediante carving, entre otros).

3.2.2.2.1.3 Análisis de logs: (registros de eventos del sistema, conexiones, etc.).

3.2.2.2.2 **Reconocimiento técnico Informático:** Este análisis permitirá al investigador identificar sujetos, objetos y eventos y podrá determinar cómo estos eventos o elementos se relaciona entre sí para emitir una conclusión.

3.2.2.2.3 Búsqueda en sitio digital: Revisión del contenido de la Web, redes sociales, correos electrónicos o sistemas para ubicar evidencias.

[14] El investigador debe seguir la normativa establecida en la Sección VI del Compendio en su apartado 2 que reza:

> Realizar una revisión exhaustiva al contenido de un dispositivo digital (EvDD), con la finalidad de ubicar texto, audio, video e imagen, vinculados con un hecho delictivo.

3.2.2.2.4 La evidencia digital no debe alterarse. Si hay riesgo de daño, se minimiza y se documenta todo. Cualquier hallazgo inesperado se reporta al superior antes de continuar.[15]

3.2.2.2.5 Cada investigador que trabaje sobre el equipo digital clonado debe llevar, contemporáneamente, notas precisas y detalladas de sus acciones y los resultados de las mismas, además del registro de cadena de custodia.[16].

3.2.2.2.6 Es indispensable verificar las especificaciones y elementos de la evidencia encontrada en el dispositivo digital el cual incluye: su estado, uso, funcionamiento y condiciones.[17]

3.2.2.2.7 Si se puede hacer una copia o clonar el sistema, se examina y trabaja sobre esa copia en un entorno o ambiente lo más parecido posible al original (usando máquinas virtuales o hardware idéntico), asegurándose de que la emulación no distorsione la evidencia.[18] . Cualquier desvío a este proceder, requerirá de la anuencia y aprobación de un superior y debe de ser documentado y explicado

3.2.2.2.8 El investigador debe determinar la correspondencia entre el código fuente o archivos de texto, audio, video e imagen y la evidencia digital adquirida, mediante el análisis comparativo.[19]

3.2.2.3. Análisis de la Nube

3.2.2.3.1 En caso de que el proveedor no coopere, se debe recurrir al procedimiento de consignación o a la orden judicial para obtener los datos. Técnicamente se trata de adquirir los datos de forma local mediante credenciales validadas o el aseguramiento de sesiones activas en caliente, diferenciándose a las solicitudes vía exhorto internacional de proveedores principales como (Google, Microsoft, Meta) los cuales poseen sedes transfronterizas.

3.2.2.3.2 Determinar el tipo de nube (privada, pública, híbrida) y modelo de servicio.

3.2.2.3.3 Gestionar las credenciales de acceso o solicitar información al proveedor.

3.2.2.3.4 Buscar y adquirir datos relevantes, documentando el proceso.

3.2.2.3.5 Calcular y registrar valores hash de los datos adquiridos.

3.2.2.4. Adquisición por Derivación

3.2.2.4.1 Si durante el peritaje se obtienen nuevas evidencias digitales, éstas pueden ser derivadas a otros laboratorios para análisis específicos (ej. análisis de imágenes de homicidio).

3.2.2.5. Análisis de Evidencia en Entornos de Comunicación

3.2.2.5.1 Análisis de Redes Sociales

[15] ISO/IEC 27042-2016 sección 6.2.

[16] *Ibidem* a la sección 6.4.

[17] *Ibidem*.

[18] *Ibidem* 7.2.3.

19 Compendio, *op.cit* a la pág. 103.

Objetivo
El objetivo principal es extraer y documentar la información generada por usuarios en plataformas como WhatsApp, Telegram, Instagram, Facebook, X, etc., que pueda ser vinculada a un hecho punible.

Actividades a realizar:

3.2.2.5.1 Identificación de la plataforma y del perfil: Determinar la aplicación, el usuario (nombre, alias, ID numérico o hash del perfil), y la fecha de creación de la cuenta.

3.2.2.5.2 Extracción de datos:

3.2.2.5.2.1 Mensajes de texto, audios, imágenes y vídeos: Se debe extraer el contenido de las conversaciones, archivos multimedia y cualquier otro dato compartido.

3.2.2.5.2.2 Metadatos de los mensajes: Fecha y hora de envío/recepción, remitente y destinatario, estado de los mensajes (entregado, leído).

3.2.2.5.2.3 Información de perfil: Foto de perfil, biografía, lista de contactos, grupos a los que pertenece.

3.2.2.5.2.4 Registros de actividad (logs de la aplicación): Aunque en la aplicación del usuario no suelen estar disponibles, se debe solicitar a la plataforma (ej. solicitud judicial a Facebook, WhatsApp, etc.) los logs de conexión, dirección IP, y dispositivos utilizados.

3.2.2.5.2.5 Información compartida: Publicaciones, historias, reacciones, comentarios, etc.

3.2.2.5.2.6 Nombrar las Herramientas forenses Utilizadas que permiten extraer y analizar esta información, siempre trabajando sobre la imagen forense del dispositivo.

3.2.2.5.2 Análisis de Portales web

Objetivo
El objetivo principal es examinar la evidencia digital que se encuentra alojada en sitios web, como páginas de contenido, foros, tiendas en línea, blogs, etc.

Actividades a realizar

3.2.2.5.2.1 Identificación del portal web: URL, propietario (domicilio, datos de WHOIS), y fecha de creación.

3.2.2.5.2.2 Documentación del estado actual: Fijación fotográfica (captura de pantalla de la página completa) y grabación de la navegación (con herramientas como OBS Studio).

3.2.2.5.2.3 Extracción de datos:

3.2.2.5.2.3.1 Contenido publicado: Textos, imágenes, vídeos, y cualquier otro elemento visible en el sitio.

3.2.2.5.2.3.2 Código fuente: Para identificar elementos ocultos, redirecciones, o posibles malware.

3.2.2.5.2.3.3 Base de datos: Si el perito tiene acceso (por orden judicial o por consignación), se puede extraer información de los usuarios registrados, publicaciones, comentarios, y actividades.

3.2.2.5.2.3.4 Análisis de tráfico: Se puede solicitar a la empresa de hosting o al ISP los registros de acceso (logs del servidor) para determinar quién y cuándo accedió al sitio, y desde qué dirección IP.

3.2.2.5.2.3.5 Nombrar las Herramientas forenses Utilizadas que permiten extraer y analizar esta información, para analizar el tráfico, bases de datos y plataformas OSINT.

3.2.2.5.3 Análisis de correo electrónico

Objetivo
El objetivo principal es extraer y analizar la información de los correos electrónicos que se encuentren en el dispositivo o en el servidor del proveedor.

Actividades a realizar

3.2.2.5.3.1 Extracción de la bandeja de entrada, salida, y correos eliminados: Se debe recuperar la información del cliente de correo (ej. Outlook, Thunderbird) que se encuentra en el dispositivo, y también solicitar al proveedor (ej. Gmail, Hotmail) los registros de la cuenta (metadatos, cabeceras de los correos, y contenido).

3.2.2.5.3.2 Análisis de cabeceras: El análisis de las cabeceras (headers) es crucial para determinar la ruta del correo, el servidor de origen, la dirección IP, y las fechas de envío y recepción.

3.2.2.5.3.3 Extracción de archivos adjuntos: Documentos, imágenes, vídeos, etc., que deben ser analizados también por separado (metadatos, hashes, posibles malware).

3.2.2.5.3.4 Análisis de la línea de tiempo: Reconstruir los eventos según el flujo de los correos.

3.2.2.5.3.5 Nombrar las Herramientas forenses Utilizadas que permiten extraer y analizar esta información.

3.2.2.6 Análisis de Logs

Objetivo

El objetivo principal es analizar los registros de eventos (logs) generados por sistemas operativos, aplicaciones, dispositivos de red y servicios, con la finalidad de reconstruir la secuencia cronológica de acciones, identificar actividades sospechosas, establecer la trazabilidad de usuarios y determinar posibles vulnerabilidades o incidentes de seguridad vinculados al hecho punible investigado.
Este protocolo aplica a cualquier fuente de logs que pueda ser de interés forense, incluyendo:

- Logs del sistema operativo (Windows Event Log, syslog, journald de Linux).
- Logs de aplicaciones (servidores web, bases de datos, correo electrónico, etc.).

- Logs de dispositivos de red (firewalls, routers, switches, proxies).
- Logs de servicios en la nube (proveedores de servicios, aplicaciones SaaS).
- Logs de dispositivos IoT y de seguridad física (sistemas CCTV, controles de acceso).

3.2.2.6.1 **Consideraciones Previas**: Los logs deben ser adquiridos preservando su integridad, aplicando los principios de cadena de custodia y calculando valores hash de acuerdo a la práctica del laboratorio forense (SHA-256, SHA-512) antes y después de cualquier manipulación.

3.2.2.6.2 El análisis se realizará sobre copias forenses de los archivos de log, nunca sobre los originales.

3.2.2.6.3 Se debe documentar la zona horaria del sistema que generó los logs y contrastarla con la hora oficial del país, para evitar interpretaciones erróneas de las marcas de tiempo.

3.2.2.6.4 Utilizar las herramientas científicas que permitan la adquisición y preservación, extraer línea de tiempo, análisis de logs tanto en Windows como en Linux/Unix, auditoría, correlación y visualización.

3.2.2.6.5 **Procedimiento:** Identificación de Fuentes de Logs: Inventariar todos los dispositivos y sistemas que puedan generar logs relevantes para la investigación (servidores, estaciones de trabajo, dispositivos de red, aplicaciones críticas, sistemas de vigilancia) y determinar la ubicación de los archivos de log en cada sistema (Windows, Linux o MAC.).

3.2.2.6.5.1 Identificar el formato de los logs (texto plano, binario, estructurado como JSON, XML, etc.) y el sistema de registro subyacente.

3.2.2.6.5.2 Consultar la política de retención de logs del sistema o del proveedor de servicios para conocer el período disponible.

3.2.2.6.6 **Adquisición de Logs**: Preservar la integridad: Calcular y registrar el valor hash de cada archivo de log original antes de cualquier copia.

3.2.2.6.6.1 Realizar una copia forense bit a bit de los archivos de log o, en su defecto, una copia lógica que mantenga los metadatos (fechas de modificación, permisos, etc.).

3.2.2.6.6.2 Documentar la fecha y hora de la adquisición, las herramientas utilizadas y el responsable.

3.2.2.6.6.3 Si los logs están en la nube o en un proveedor externo, gestionar la solicitud formal (orden judicial, consignación) para obtener los registros de actividad y las copias de seguridad de los mismos.

3.2.2.6.7 **Preservación y Cadena de Custodia**: Registrar en la Planilla de Registro de Cadena de Custodia la recepción de los logs, sus hashes y las transferencias posteriores.

3.2.2.6.7.1 Almacenar los logs originales en un área de resguardo con control de acceso, protegiéndolos de modificaciones, borrados o corrupción.

3.2.2.6.7.2 Trabajar siempre sobre copias de trabajo, manteniendo el original como evidencia inalterable.

3.2.2.6.8 **Análisis de Logs: Normalización y Filtrado:** Unificar el formato de las marcas de tiempo a una zona horaria común (UTC o la del país) y documentar la conversión.

3.2.2.6.8.1 Filtrar eventos irrelevantes (ruido) para reducir el volumen de datos, utilizando criterios como el rango de fechas vinculado al hecho, los usuarios o equipos implicados, o los códigos de evento específicos.

3.2.2.6.8.2 Aplicar expresiones regulares o consultas estructuradas para extraer campos relevantes (fechas, usuarios, direcciones IP, acciones, resultados).

3.2.2.6.9 **Análisis Cronológico y Línea de Tiempo**: Construir una línea de tiempo (timeline) con todos los eventos relevantes extraídos de los logs, ordenados cronológicamente.

3.2.2.6.9.1 Identificar eventos clave que puedan estar relacionados con el incidente (inicios de sesión, accesos a archivos, cambios de configuración, ejecución de comandos, conexiones de red, errores de seguridad, etc.).

3.2.2.6.9.2 Buscar patrones anómalos (por ejemplo, múltiples fallos de autenticación, accesos fuera de horario laboral, cambios en permisos, creación de usuarios, ejecución de scripts sospechosos).

3.2.2.6.10 **Correlación de Eventos:** Relacionar eventos de diferentes fuentes de logs para reconstruir la secuencia completa de una acción (por ejemplo, un acceso a un recurso, una transferencia de datos, una modificación de sistema).

3.2.2.6.10.1 Cruzar información con otras evidencias digitales (metadatos de archivos, registros de conexión, capturas de tráfico de red) para confirmar o descartar hipótesis.

3.2.2.6.10.2 Identificar la fuente de acciones: usuario, dirección IP, dispositivo, proceso, etc.

3.2.2.6.11 **Análisis de Seguridad y Detección de Incidentes:** Buscar indicadores de compromiso (IoC) en los logs, como direcciones IP maliciosas, hashes de malware, patrones de ataque conocidos (por ejemplo, ataques de fuerza bruta, inyecciones SQL, acceso a rutas sensibles).

3.2.2.6.11.1 Detectar actividades de exfiltración de datos o movimientos laterales dentro de la red.

3.2.2.6.11.2 Verificar la integridad de los logs mediante la comparación de hashes o la revisión de posibles alteraciones (por ejemplo, borrado de eventos, modificación de marcas de tiempo).

3.2.2.6.11.3 Documentar las limitaciones del análisis (por ejemplo, logs incompletos, rotación de logs, falta de registros, saltos en la secuencia).

3.2.3. Informe o Dictamen Pericial

3.2.3.1 Se debe emitir un informe técnico o dictamen pericial que contenga la siguiente información:

3.2.3.1.1 El nombre del investigador principal incluyendo sus credenciales y experiencia en el sector de peritaje forense digital;

3.2.3.1.2 La naturaleza del incidente investigado que incluirá el tiempo, duración y lugar del incidente;

3.2.3.1.3 Qué motivó el objetivo de la investigación, los miembros del equipo y sus roles, el tiempo, duración y lugar de la investigación;

3.2.3.1.4 Una lista descriptiva de los hechos o información sobre de la evidencia digital encontrada; cualquier daño a la evidencia observado y su impacto; las limitaciones del análisis realizado; la ruta de ubicación de cada evidencia digital

y su cuantificación y clasificación por tipo (texto, audio, imagen, video), fechas de creación, modificación y acceso de los archivos, valores hash calculados para cada uno de los archivos garantizar la integridad de los mismos, análisis de línea de tiempo (Timeline) de los eventos, una lista de los procesos y herramientas utilizados y las conclusiones basadas en los resultados de los análisis.

3.2.3.1.5 Colocar un apartado sobre la "cadena de custodia electrónica", donde se detallen los hashes y las firmas digitales de los archivos.

3.2.3.1.6 Es permisible que el investigador pueda incluir cuantas interpretaciones de la evidencia puedan ser posibles y conclusiones para cada una de ellas. También puede incluir posibles ángulos investigativos, a posteriori, de surgir nueva data o información.

3.2.3.1.7 El perito debe estar disponible para declarar en el juicio oral, ratificando su dictamen y respondiendo a las preguntas de las partes

3.2.3.2 Manejo de la prueba digital para proteger su admisibilidad

3.2.3.2.1 Como la prueba digital se va a utilizar en un procedimiento judicial, es obligatorio trabajar sobre la copia del medio original. El original se debe guardar bajo llave o medidas de seguridad que impida el acceso no autorizado de la misma y que pueda contaminar su manejo. Todo debe estar documentado en caso de que haya una reclamo legal o impugnación durante el manejo de la prueba digital.

3.2.3.2.2 Es importante que se siga el protocolo establecido en el Manual de Único de Cadena de Custodia de Evidencias Físicas (MUCCEF).

3.2.3.2.3 Debe describir las características de los dispositivos digitales entregados y dejar constancia del estado de los mismos con los signos y señas particulares.

3.2.3.2.4 Es obligatorio que el perito use un bloqueador de escritura (*write-blocker*) homologado, ya que sirve de escudo o protector para que la evidencia original no sea escrita o alterada accidentalmente.[20]

3.2.3.2.5 Toda la evidencia siempre debe ser regresada a su embalaje original y documentar su entrada (hora y fecha) y firmar el mismo para que quede constancia del número de veces que el embalaje fue abierto para ser evaluado y analizado.

3.2.3.2.6 El investigador debe emitir las conclusiones de forma objetiva e imparcial. Su opinión y conclusiones deben estar basados en la ciencia y en los procesos analíticos empleados.

3.2.3.2.7 Al evaluar la evidencia, se debe tener cuidado en distinguir los hechos que han sido encontrados de la información que ha sido inferida.[21]

3.3. Fase de Resguardo

Objetivo de la Fase

[20] NIST op.cit. sección 4.2.2

[21] Op. cit. 27042-2016 sección 8.3

El objetivo principal de la Fase de Resguardo es garantizar la preservación y seguridad de la evidencia digital durante el tiempo que permanece bajo custodia, desde su ingreso al área de resguardo hasta su disposición final. Esto implica mantener la integridad física de los dispositivos (EvDD) protegiéndolos de golpes, temperaturas extremas y campos electromagnéticos, y asegurar la integridad lógica de los datos adquiridos (EvSSD) mediante almacenamiento en dispositivos limpios, copias de seguridad y verificación periódica de los valores hash.

Además, esta fase busca asegurar la cadena de custodia y el control de acceso a la evidencia. Se registra meticulosamente cada ingreso y egreso en las planillas correspondientes, se almacenan los dispositivos en áreas con control de acceso (como la sección de evidencias electrónicas) y se implementan medidas para evitar alteraciones, modificaciones o sustracciones. De esta forma, se garantiza que la evidencia se mantenga inalterada y disponible para futuros análisis, exhibiciones en audiencias o su disposición final, cumpliendo con los estándares legales y científicos requeridos.

Actividades a realizar:

3.3.1 Las evidencias digitales (EvDD) se resguardarán en el Área de Resguardo Ordinario, en la Sección de evidencias electrónicas.
3.3.2 Las evidencias digitales que son producto de la adquisición (EvSSD) se almacenarán en dispositivos de almacenamiento limpios (sonetizados), debidamente etiquetados y con un sistema de hash calculado.
3.3.3 El depósito de la evidencia debe garantizar su preservación. Para las EvDD, se debe mantener la integridad física del dispositivo. Para las EvSSD, se debe preservar la integridad de los datos (copias de seguridad, almacenamiento en discos protegidos).
3.3.3 El egreso de la evidencia para su peritación, exhibición en audiencia o disposición final se realizará bajo estricto control, registrando a la persona responsable de su custodia.

3.4. Fase de Disposición Final

Objetivo de la Fase

El objetivo principal de la Fase de Disposición Final es culminar formalmente el ciclo de vida de la evidencia digital, determinando su destino final de acuerdo con lo establecido por la autoridad competente (juez o fiscal). Esto implica cerrar la cadena de custodia mediante la ejecución de una orden judicial que puede disponer la devolución al propietario legítimo, la entrega a otra autoridad, la destrucción física o lógica de los datos, o el archivo definitivo de la evidencia.

Además, esta fase busca documentar y registrar el cierre del caso, dejando constancia en el Acta de Disposición Final y en la Planilla de Registro de Cadena de Custodia de todos los pasos realizados. Para la evidencia digital, la destrucción implica la inutilización física del dispositivo o el borrado seguro de los datos mediante métodos que imposibiliten su recuperación, mientras que el archivo requiere su

almacenamiento en condiciones que preserven su integridad para futuras consultas, garantizando así que el proceso concluya con total transparencia y validez jurídica.

Actividades a realizar:

3.3.1 El cierre de la cadena de custodia para la evidencia digital se materializa mediante:

3.3.1.1 **Devolución:** Restituir el dispositivo o la información a su propietario legítimo, previa orden judicial.

3.3.1.2 **Entrega**: Otorgar la evidencia procesada a la autoridad competente designada.

3.3.1.3 **Destrucción**: Inutilizar físicamente el dispositivo o borrar de forma segura (destrucción lógica) la información digital que no tenga interés en la investigación, previa orden judicial. Para el caso de datos almacenados, se debe solicitar al proveedor de servicios su eliminación definitiva.

3.3.1.4 **Consumida en peritaje**: Cuando la evidencia digital es procesada y se convierte en una copia de trabajo, la copia original (imagen forense) se archiva y puede ser considerada como evidencia consumida o almacenada.

4. Fase de Obtención por Consignación

La obtención por consignación, aplica en aquellos casos en los que un particular hace entrega de manera directa o indirecta de una determinada evidencia ante un(a) funcionario(a) con competencia en materia de investigación penal en el ejercicio de sus funciones, según sea el caso de la consignación primaria o secundaria.

4.1 **De la obtención por consignación ante instituciones públicas de investigación:**

4.1.1 Evaluar la evidencia y su vinculación con la investigación penal.

4.1.2 Entrevistar al (la) consignatario (a) de la evidencia y dejar constancia mediante acta de las circunstancias de modo, tiempo y lugar en las que la ubicó y las condiciones de la misma.

4.1.3. Manipular la evidencia lo estrictamente necesario.

4.1.4 Clasificar y separar las evidencias según corresponda, en caso de consignación de más de una evidencia.

4.1.5 Garantizar la integridad de la evidencia durante el tiempo en que se encuentre sometida al proceso de recepción.

4.1.6 Elaborar Acta de Obtención por Consignación por parte del(la) operario(a) que recibe la evidencia, la cual estará inserta en el expediente, acompañada de una copia simple del Registro de Planilla de Cadena de Custodia.

4.1.7 Trasladar la evidencia sin dilación, al laboratorio correspondiente para su respectivo análisis.

4.2 **Lineamientos específicos Para la Consignación Primaria**

4.2.1 Elaborar comunicación de forma inmediata dirigida al laboratorio competente solicitando la peritación correspondiente dependiendo de la evidencia y su vinculación con la investigación. En este caso, el (la) operador (a) receptor (a) deberá verificar que la solicitud se ajuste a los análisis que le corresponde a dicha evidencia.

4.2.2 En los casos de evidencia física de tipo digital, el (la) consignatario (a) hace entrega de un dispositivo digital para que se practique la obtención de la información que corresponde.

4.3 **Lineamientos específicos Para la Consignación Indirecta**

4.3.1 Cuando se trate de evidencias digitales remitidas por el (la) consignatario (a) de manera física o digital, el (la) funcionario (a) con competencia en materia de investigación penal, deberá verificar la pertinencia y/o vinculación con la investigación, a fin de proceder con el levantamiento de un Acta de Consignación Indirecta mediante la cual se deje constancia de toda la información referente a la evidencia recibida, tales como lugar, fecha y hora de la recepción y relación con el hecho.

4.3.2 Cuando se trate de la evidencia documental recibida de forma digital, además de los aspectos previamente mencionados, se deberá plasmar el medio empleado para la remisión y recepción de la evidencia. Se empleará herramientas o programas forenses que permitan la autenticidad, integridad, inalterabilidad de la evidencia digital al momento de realizar la verificación, descarga y almacenamiento de esta, con la finalidad de ser remitido a la dependencia correspondiente para su peritación, previo cumplimiento de los lineamientos establecido en el procedimiento de obtención por consignación.

4.3.3 En los casos de consignación de dispositivos digitales, se aplican los procedimientos establecidos en ese apartado. Esto ocurre en los casos de víctimas que son enviadas para que se le haga la adquisición digital de la información del teléfono u otros dispositivos tecnológicos portables con información de interés criminalístico.

4.4 Obtención por Consignación ante Perito Privado

Consideraciones previas: Marco Legal del Perito Privado en Venezuela

4.4.1**. Fundamento Constitucional:** El artículo 257 de la Constitución de la República Bolivariana de Venezuela establece que “el proceso constituye un instrumento fundamental para la realización de la justicia”, garantizando a las partes el derecho a utilizar los medios de prueba que consideren conducentes para hacer valer sus pretensiones. Este principio constitucional sienta las bases para la admisión de cualquier medio probatorio lícito, incluyendo los dictámenes de peritos privados.

4.4.2. **Base Legal en el Código Orgánico Procesal Penal (Ámbito Penal)**

En materia penal, la figura del perito se encuentra regulada en el artículo 224 del Código Orgánico Procesal Penal (COPP), el cual dispone:

"Los o las peritos deberán poseer título en la materia relativa al asunto sobre el cual dictaminarán, siempre que la ciencia, el arte u oficio estén reglamentados. En caso contrario, deberán designarse a personas de reconocida experiencia en la materia. Los o las peritos serán designados o designadas y juramentados o juramentadas por el Juez o Jueza, previa petición del Ministerio Público, salvo que se trate de funcionarios adscritos o funcionarias adscritas al órgano de investigación penal, caso en el cual, para el cumplimiento de sus funciones bastará la designación que al efecto le realice su superior inmediato".

De esta norma se desprende que la ley penal no prohíbe la participación de peritos privados; simplemente establece un procedimiento distinto para su designación: mientras los peritos oficiales son designados por su superior jerárquico, los peritos privados deben ser designados y juramentados por el Juez, previa petición del Ministerio Público. Esto implica que el perito privado puede ser propuesto por cualquiera de las partes, y su designación formal corresponde al órgano jurisdiccional, garantizando así su imparcialidad y el control judicial sobre su actuación.

El artículo 223 del COPP, por su parte, establece que "el Ministerio Público realizará u ordenará la práctica de experticias cuando para el examen de una persona u objeto, o para descubrir o valorar un elemento de convicción, se requieran conocimientos o habilidades especiales en alguna ciencia, arte u oficio". Esta norma, al referirse al Ministerio Público, no excluye la posibilidad de que las partes promuevan sus propios peritos, lo cual es consistente con el principio de contradicción y el derecho a la defensa.

4.4.3. **El Perito Privado en el Ámbito Civil**

En el proceso civil venezolano, la prueba pericial es un medio de prueba ampliamente reconocido. El artículo 1427 del Código Civil establece que "los Jueces no están obligados a seguir el dictamen de los expertos si su convicción se opone a ellos", lo que confirma que el dictamen pericial, sea de perito oficial o privado, es un medio de prueba que el juez valora libremente, sin estar vinculado de manera absoluta al mismo.

La doctrina señala que "la experticia judicial constituye una prueba de complejidad técnica o científica de los hechos que conforman el supuesto para la aplicación de las normas jurídicas", y los expertos actúan como "figuras auxiliares de carácter técnico para con el juez", sin que exista distinción legal entre peritos oficiales y privados en cuanto a la validez de su dictamen.

4.4.4. **El Perito Privado en el Ámbito Laboral**

En materia laboral, la Ley Orgánica del Trabajo, los Trabajadores y las Trabajadoras (LOTTT) y su normativa procesal, la Ley Orgánica Procesal del Trabajo, también reconocen la prueba pericial como medio de prueba. El principio de oralidad, inmediación y concentración que rige el proceso laboral no impide la participación de peritos privados, quienes pueden ser propuestos por las partes para sustentar sus pretensiones.

4.4.5. **El Principio de la Prueba Libre y la Valoración del Dictamen del Perito Privado**

El sistema probatorio venezolano se rige por el principio de la libre valoración de la prueba o sana crítica, consagrado en el artículo 395 del Código de Procedimiento Civil, que establece que "son medios de prueba admisibles en cualquier juicio aquellos que determina el Código Civil, el presente Código y otras leyes". Este principio implica que el juez debe apreciar las pruebas según su sana crítica, observando las reglas de la lógica, la ciencia y la experiencia.

En este contexto, el dictamen del perito privado es un medio de prueba más, que el juez debe valorar junto con los demás elementos del proceso, sin que exista una jerarquía probatoria que favorezca a los peritos oficiales por encima de los privados. La ley no establece diferencias en cuanto a la validez o el peso probatorio de un dictamen pericial por el solo hecho de haber sido emitido por un perito privado. Su valoración dependerá de la solidez técnica, la fundamentación científica, la imparcialidad y la claridad de las conclusiones.

4.4.6**. El Dictamen del Perito Privado como Prueba Preconstituida en el Ámbito Penal y Civil**

En el proceso penal venezolano, el dictamen del perito privado debe ser considerado como una prueba preconstituida. La doctrina define la prueba preconstituida como "aquella practicada antes del inicio formal del proceso penal o en la propia fase de investigación, observando las garantías constitucionales y legales pertinentes, respecto a diligencias de imposible o muy difícil reproducción".

El dictamen pericial privado, al ser elaborado antes o durante la fase preparatoria, y al poder ser de difícil o imposible reproducción en el juicio oral (por ejemplo, cuando la evidencia digital se ha modificado o destruido), encaja en esta categoría. Su admisibilidad está sujeta a que se hayan observado las garantías del debido proceso y que el perito pueda ser citado a declarar en el juicio oral para ratificar su dictamen y someterlo al contradictorio.

La prueba anticipada, regulada en el COPP, procede "en aquellos casos que sea necesario practicar un reconocimiento, inspección o experticia, que por sus características y naturaleza puedan considerarse como pruebas definitivas de imposible repetición". Este mecanismo permite que el perito privado, previa solicitud al juez, pueda realizar su experticia con las garantías propias del juicio, asegurando así su validez.

4.5.7. Reconocimiento legal del Perito Privado

4.5.7.1 El perito privado tiene pleno reconocimiento legal en el ordenamiento jurídico venezolano, tanto en el ámbito penal (COPP, art. 224) como en el civil, mercantil y laboral.

4.5.7.2 Su dictamen es un medio de prueba admisible, sujeto a las mismas reglas de valoración que el de cualquier perito oficial, basadas en el principio de la sana crítica.

4.5.7.3 En el proceso penal, el dictamen del perito privado constituye una prueba preconstituida, cuya validez depende de que se hayan respetado las garantías del

debido proceso y de que el perito pueda ser citado a juicio para ratificarlo y someterlo al contradictorio.

4.5.7.4 La designación del perito privado en materia penal debe ser formalizada por el Juez, previa petición del Ministerio Público o de las partes, conforme al artículo 224 del COPP.

4.5.7.5 El principio de prueba libre (arts. 395 CPC y 1427 CC) garantiza que el juez valore el dictamen del perito privado con la misma libertad que cualquier otra prueba, sin privilegios para los peritos oficiales.

4.5.7.6 La figura del perito privado es una manifestación del derecho a la defensa y del principio de contradicción, permitiendo a las partes contar con asesoramiento técnico especializado para sustentar sus pretensiones.

4.5.8 Naturaleza de la Consignación Privada: La obtención por consignación ante perito privado aplica en aquellos casos en los que un particular, víctima, imputado, su representante legal o cualquier sujeto procesal, hace entrega de manera voluntaria de una evidencia digital (dispositivo o archivo) a un perito o experto privado, con el objeto de que éste realice el análisis forense correspondiente. En estos supuestos, el perito privado actúa como auxiliar de la administración de justicia, debiendo cumplir con los mismos estándares técnicos, científicos y legales que rigen la actuación de los funcionarios públicos, a fin de garantizar la licitud, integridad, autenticidad y admisibilidad de la prueba ante el tribunal.

4.5.8.1 El perito privado no ejerce funciones de investigación penal ni de autoridad, por lo que su actuación se limita al análisis técnico-científico de la evidencia que le es consignada, sin que ello implique un menoscabo en la rigurosidad del procedimiento. La validez de su dictamen pericial dependerá del estricto cumplimiento de los protocolos de cadena de custodia, documentación y preservación de la evidencia, así como de su capacidad para demostrar la inalterabilidad de los datos desde el momento de la recepción hasta la emisión de su informe.

4.5.9 Deberes del Perito Privado en la Obtención por Consignación

4.5.9.1 El perito privado que recibe una evidencia digital por consignación deberá:

4.5.9.2 Evaluar la evidencia y su vinculación con el caso objeto de peritaje, determinando su pertinencia y utilidad para la investigación.

4.5.9.3 Entrevistar al consignatario de la evidencia, levantando un acta donde se deje constancia de las circunstancias de modo, tiempo y lugar en las que se le entregó el dispositivo o archivo, las condiciones en que se encontraba, su procedencia y cualquier otra información relevante para establecer la cadena de custodia.

4.5.9.4 Verificar la identidad del consignatario y su relación con el caso, documentando dicha información en el acta correspondiente.

4.5.9.5 Manipular la evidencia lo estrictamente necesario, evitando cualquier acción que pueda alterar, modificar o contaminar los datos originales. En ningún caso se deberá acceder al contenido del dispositivo sin antes haber realizado la imagen forense o copia de respaldo.

4.5.9.6 Clasificar y separar las evidencias cuando se trate de la consignación de más de un dispositivo o archivo, asignando una identificación única a cada uno y documentando su recepción por separado.

4.5.9.7 Garantizar la integridad de la evidencia durante todo el tiempo en que se encuentre bajo su custodia, implementando las medidas de seguridad física y lógica necesarias para evitar su deterioro, pérdida o modificación.

4.5.9.8 Elaborar el Acta de Recepción y Salvaguarda de Evidencia Consignada, en la que se detalle toda la información relativa a la recepción de la evidencia, incluyendo fecha, hora, lugar, identificación del consignatario, descripción de la evidencia, estado en que se recibió y cualquier otra circunstancia relevante. Esta acta deberá ser firmada por el perito y por el consignatario, y se adjuntará como anexo al dictamen pericial.

4.5.9.9 Calcular y registrar los valores hash (función hash) de la evidencia recibida en el momento mismo de la recepción, utilizando herramientas forenses que permitan su verificación y que garanticen la inalterabilidad de los datos. Los valores hash obtenidos deberán constar en el Acta de Recepción y Salvaguarda de Evidencia Consignada.

4.5.9.10 El Perito documentará a través de Bitácora que anexará al informe pericial, cada evaluación de la evidencia, desde su recepción hasta su disposición final, incluyendo fecha, hora y responsable del tratamiento de la evidencia.

4.5.10 Procedimiento de Recepción de Evidencias Digitales

4.5.10.1 Recepción de Dispositivos Digitales (EvDD): Cuando el consignatario hace entrega de un dispositivo digital (ordenador, teléfono móvil, tableta, disco duro, memoria USB, etc.), el perito privado deberá:

4.5.10.1.1 Verificar el estado físico del dispositivo, documentando cualquier daño, alteración o modificación visible, mediante fijación fotográfica o videográfica.

4.5.10.1.2 Identificar y registrar las características técnicas del dispositivo: marca, modelo, número de serie, IMEI (en caso de teléfonos móviles), capacidad de almacenamiento, y cualquier otro identificador único.

4.5.10.1.3 Determinar el estado del dispositivo (encendido o apagado). Si está encendido, se debe evaluar la posibilidad de realizar una adquisición en vivo de los datos volátiles (memoria RAM, procesos activos, conexiones de red) antes de proceder con su apagado.

4.5.10.1.4 Calcular y registrar el valor hash de la imagen forense que se generará a partir del dispositivo, una vez que se haya realizado la copia de seguridad. Este hash deberá ser incluido en el Acta de Recepción y Salvaguarda de Evidencia Consignada y en el informe pericial.

4.5.11 Recepción de Evidencias Digitales (EvSSD)

4.5.11.1 Cuando el consignatario hace entrega de archivos o datos digitales (documentos, correos electrónicos, imágenes, vídeos, audios, bases de datos, etc.) a través de medios físicos o electrónicos, el perito privado deberá:

4.5.11.2 Verificar el medio de almacenamiento y la integridad de los archivos recibidos, comprobando que no hayan sido alterados durante la transmisión.

4.5.11.3 Calcular y registrar los valores hash de cada archivo o conjunto de archivos, tanto en el momento de la recepción como después de cualquier proceso de copia o transferencia, para garantizar su integridad.

4.5.11.4 Documentar el medio empleado para la remisión y recepción de la evidencia (correo electrónico, plataforma de intercambio de archivos, dispositivo de almacenamiento físico, etc.), así como la fecha y hora de recepción.

4.5.11.5 Emplear herramientas forenses que permitan la verificación de la autenticidad, integridad e inalterabilidad de la evidencia digital, dejando constancia del proceso en el Acta de Recepción y Salvaguarda de Evidencia Consignada

.

4.5.12 Cadena de Custodia en la Consignación Privada

4.5.12.1 La cadena de custodia en el ámbito privado debe cumplir con los mismos requisitos que en el ámbito público, a fin de garantizar la admisibilidad de la prueba. El perito privado deberá:

4.5.12.1.1 Iniciar el Acta de Recepción y Salvaguarda de Evidencia Consignada al momento de la recepción de la evidencia, consignando los datos del consignatario, la descripción de la evidencia, la fecha y hora de la recepción, y los valores hash calculados.

4.5.12.1.2 Documentar cada evaluación de la evidencia, la entrega a otros peritos (si es necesario), la devolución al consignatario o la disposición final. En cada transferencia, se deberá registrar la fecha, hora, responsables y motivo del traslado.

4.5.12.1.3 Asegurar que la evidencia permanezca bajo custodia de una persona responsable en todo momento, evitando que sea dejada sin supervisión o en lugares no seguros.

4.5.12.1.4 Dejar constancia de cualquier incidencia que pueda afectar la integridad de la evidencia, así como de las medidas adoptadas para subsanarla.

4.5.13 Requisitos de Validez y Licitud

4.5.13.1 Para que el dictamen pericial emitido por un perito privado tenga plena validez y sea inobjetable ante el tribunal, se debe cumplir con los siguientes requisitos:

4.5.13.1.1 Que el perito esté debidamente calificado y acreditado en la materia, y que su experiencia y formación se encuentren documentadas.

4.5.13.1.2 Que el procedimiento de obtención y análisis se ajuste a los estándares científicos y forenses, tal como se establece en el Manual Único de Cadena de Custodia de Evidencias Físicas y en el Compendio de Protocolos de Actuación para el Fortalecimiento de la Investigación Penal en Venezuela.

4.5.13.1.3 Que se haya documentado exhaustivamente el proceso, incluyendo el Acta de Recepción y Salvaguarda de Evidencia Consignada, y cualquier

otro instrumento que permita reconstruir la trazabilidad de la evidencia desde su recepción hasta la emisión del dictamen.

4.5.13.1.4 Que se hayan calculado y registrado los valores hash en todas las fases del proceso, garantizando la integridad e inalterabilidad de la evidencia digital.

4.5.13.1.5 Que el dictamen pericial incluya una descripción clara y detallada de los métodos, herramientas y procedimientos utilizados, así como las conclusiones obtenidas, de manera que sea comprensible para el tribunal y para las partes.

4.5.13.1.6 Que el perito pueda ser citado a declarar en el juicio oral para ratificar su dictamen y responder a las preguntas de las partes y del tribunal, demostrando así la validez de su análisis.

4.5.14 Consideraciones Finales

4.5.14.1 La intervención del perito privado en el proceso penal venezolano es una figura reconocida y valiosa, que permite a las partes contar con asesoramiento técnico especializado y garantiza la contradicción de la prueba. Sin embargo, para que su dictamen tenga el peso probatorio requerido, es imprescindible que el perito actúe con la misma rigurosidad y objetividad que un funcionario público, documentando cada paso de su actuación y demostrando la integridad de la evidencia desde el momento de su recepción.

4.5.14.2 El perito privado deberá estar siempre dispuesto a poner a disposición del tribunal, del Ministerio Público y de las partes, toda la documentación relativa a su actuación, incluyendo la evidencia original (si está bajo su custodia) y los archivos de trabajo, a fin de permitir la verificación de sus conclusiones y la realización de contrainformes periciales si así se solicita.

5. Fase de Obtención por aseguramiento (flagrancia)

5.1. Aplica para situaciones de flagrancia, ante un peligro inminente de pérdida de la evidencia, en caso de situaciones apremiantes y cuando sea imposible cumplir los procedimientos de obtención técnica, se considerará que las evidencias han sido obtenidas por aseguramiento, desarrollando cada uno de los procedimientos establecidos para esta última.

5.2. De la obtención por aseguramiento: Realizar los procedimientos correspondientes a la obtención por aseguramiento, con los funcionarios actuantes en el escenario.

5.3. En este tipo de procedimiento el cumplimiento de la cadena de custodia debe ser aún más rigurosa, ya que la evidencia se obtiene en circunstancias de urgencia.

5.4. Realizar la inspección técnica de los escenarios donde sean obtenidas evidencias vinculadas al suceso, cumpliendo progresivamente con los criterios y principios que rigen el abordaje y tratamiento de la evidencia contenidos en el Manual Único de Cadena de Custodia de Evidencias Físicas.

6. Fase de Obtención por Derivación

6.1 Al derivar la evidencia a otro laboratorio, se debe documentar el envío y la recepción con nuevos valores hash y la firma del responsable.

Valencia Estado Carabobo, Venezuela — Julio 2026

6.2 **Por Selección:** Cuando las evidencias de dispositivos digitales son previamente colectadas, son trasladadas al laboratorio de informática forense y dentro de su procesamiento se obtienen evidencias digitales de interés criminalístico, éstas deben ser enviadas a otros laboratorios para sus respectivos análisis.

6.3 **Procedimiento de búsqueda**: Dentro de la peritación se aplicarán métodos con programas de búsqueda de evidencias digitales vinculadas o conexas al hecho investigado, por ejemplo, casos de videos e imágenes.

6.4 **Procedimiento de Fijación:** El (la) perito (a) informático (a) de laboratorio realizará fijaciones fotográficas o utilizando impresiones de pantallas, en las que se refleje la ruta de la ubicación de la evidencia digital, la fecha de creación, modificación y acceso.

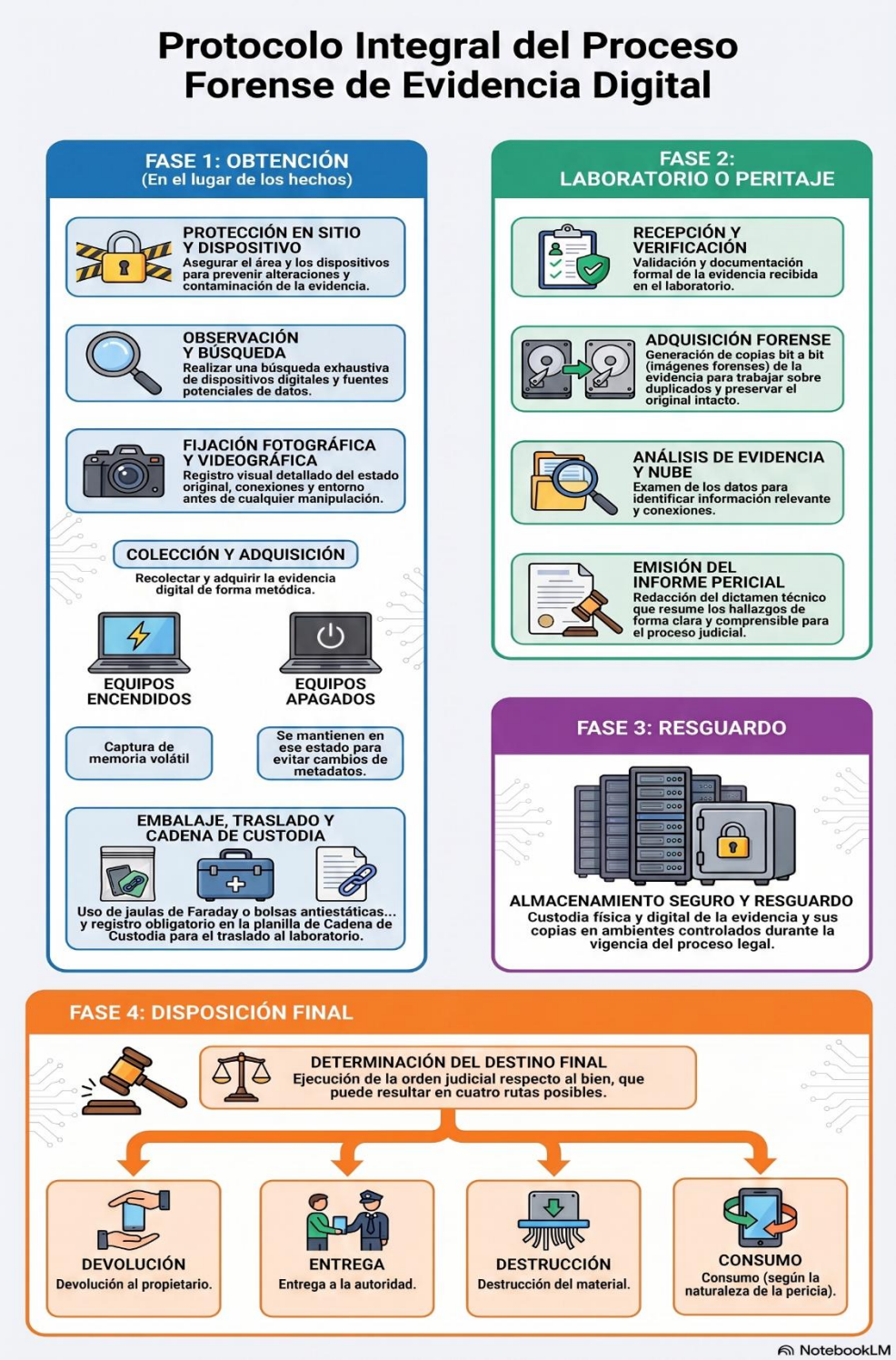
6.5 **Procedimiento de adquisición**: Se aplicarán los programas específicos para la obtención de la evidencia digital.

Tabla Resumen de Actuaciones Clave para la Evidencia Digital

Fase	Acción Principal	Documento / Herramienta
Obtención	Colección / Adquisición	Planilla de Cadena de Custodia, Cámara Fotográfica, Bolsas de Faraday, Herramientas de Adquisición (ej. FTK Imager, dd).
Protección	Inhibición de Señales	Bolsas de Faraday, Modo Avión.
Fijación	Registro Fotográfico	Cámara, Teléfono Móvil, Captura de Pantalla (Screenshot).
Laboratorio	Análisis / Peritaje	Software Forense (EnCase, FTK, X-Ways), HDD Clonador, Calculadora de Hash.
Peritaje	Informe Técnico	Archivo de texto, Tablas, Gráficos (Línea de Tiempo).
Resguardo	Almacenamiento	Área de Resguardo con Control de Acceso, Discos Duros Almacenados.

Fase	Acción Principal	Documento / Herramienta
Disposición Final	Cierre	Acta de Disposición Final, Planilla de Cadena de Custodia sellada.

7. Flujograma del Proceso Forense Digital



Valencia Estado Carabobo, Venezuela — Julio 2026

CLÁUSULA DE INTEGRIDAD

REFERENCIA DE CITACIÓN SUGERIDA

Para citar este manual como fuente de consulta, se recomienda utilizar el siguiente formato:

Álvarez, N. & Seivanne, J. A. R. (2026). Manual de Procedimientos Forenses para el Tratamiento de Evidencias Digitales (1ª actualización). Escritorio Jurídico Lazarus, Álvarez & Asociados, S.C / Centro de Investigación Informática Lazarus, C.A.

ANEXO: MODELO DE ACTA DE RECEPCIÓN Y SALVAGUARDA DE EVIDENCIA CONSIGNADA

ACTA DE RECEPCIÓN Y SALVAGUARDA DE EVIDENCIA CONSIGNADA

Nº [XXXXX]

En la ciudad de [Ciudad], Estado [Estado], a los [día] días del mes de [mes] del año [año], siendo las [hora]:[minutos] horas, se reúnen por una parte, el(la) ciudadano(a) [Nombre y Apellido del Consignatario], venezolano(a), mayor de edad, titular de la cédula de identidad Nº V- [Número de Cédula], actuando en su propio nombre y representación (o en representación de [indicar si actúa como apoderado, representante legal, etc.]), quien en lo sucesivo se denominará **EL(LA) CONSIGNATARIO(A);** y por la otra, el(la) ciudadano(a) [Nombre y Apellido del Perito], venezolano(a), mayor de edad, titular de la cédula de identidad Nº V- [Número de Cédula], [indicar profesión y especialidad] [perito privado / experto forense] actuando en su condición de [Perito Privado/Experto Forense], inscrito(a) en [indicar colegio o institución correspondiente] bajo el Nº [número de matrícula o credencial], en lo sucesivo y a los fines de este acto **EL(LA) PERITO(A).** Ambas partes, hábiles y capaces, convienen en celebrar el presente acto de consignación privada de evidencia digital, el cual se regirá por las siguientes cláusulas:

PRIMERA: OBJETO Y JUSTIFICACIÓN: El(La) Consignatario(a) entrega voluntariamente al Perito(a) un dispositivo digital o conjunto de archivos digitales, a los fines de que éste(a) realice el correspondiente análisis pericial forense. La consignación tiene como fundamento la necesidad de contar con un análisis técnico-científico especializado que permita preservar, analizar y documentar la evidencia digital vinculada al asunto de interés, garantizando su integridad, autenticidad e inalterabilidad.

SEGUNDA: IDENTIFICACIÓN DE LA EVIDENCIA CONSIGNADA: El(La) Consignatario(a) hace entrega al Perito(a) de la siguiente evidencia digital, descrita de manera detallada:

Tipo de Evidencia:
( ) Dispositivo Digital (EvDD):
Marca: _____
Modelo: _____
Número de Serie: _____
IMEI (si aplica): _____
Tipo de dispositivo: ( ) Teléfono móvil ( ) Computador ( ) Tableta ( ) Disco Duro ( ) Memoria USB ( ) Otro: _____
Estado del dispositivo al momento de la entrega: ( ) Encendido ( ) Apagado
Observaciones sobre el estado físico: _____
( ) Archivos o Datos Digitales (EvSSD):
Medio de almacenamiento: ( ) Disco Duro ( ) Memoria USB ( ) CD/DVD ( ) Correo electrónico ( ) Plataforma en la nube ( ) Otro: _____
Cantidad de archivos: _____
Descripción del contenido (si se conoce): _____
Fecha de creación/modificación (si se conoce): _____
Formato del archivo: ( ) Texto ( ) Imagen ( ) Audio ( ) Vídeo ( ) Base de datos ( ) Otro: _____
Observaciones adicionales: _____

TERCERA: DECLARACIÓN DEL(LA) CONSIGNATARIO(A): El(La) Consignatario(a) declara bajo juramento, y en conocimiento de las responsabilidades penales en que puede incurrir por falso testimonio, que:

Origen de la evidencia: La evidencia entregada fue obtenida lícitamente, y proviene de [describir las circunstancias de modo, tiempo y lugar en que la ubicó], y se encuentra en las condiciones en que se describe.

Propiedad y posesión: Es el(la) legítimo(a) propietario(a) o poseedor(a) de la evidencia, o está facultado(a) para disponer de ella, y la entrega de manera voluntaria.

Integridad: A su leal saber y entender, la evidencia no ha sido alterada, modificada, ni manipulada desde el momento de su hallazgo o recepción hasta la fecha de esta consignación.

Finalidad: La entrega se realiza con el objeto de que el(la) Perito(a) practique el análisis forense correspondiente, y se compromete a colaborar con el(la) mismo(a) en lo que sea necesario para el esclarecimiento de los hechos.

CUARTA: OBLIGACIONES DEL(LA) PERITO(A): El(la) Perito(a) acepta la consignación y se compromete a:

Preservar la integridad de la evidencia: Mantener la evidencia en condiciones de seguridad y custodia que impidan su pérdida, daño, alteración o acceso no autorizado.

Aplicar los estándares forenses: Realizar el análisis de la evidencia siguiendo los protocolos técnicos y científicos establecidos en el Manual Único de Cadena de Custodia de Evidencias Físicas, el Compendio de Protocolos de Actuación para el Fortalecimiento de la Investigación Penal, y los estándares internacionales aplicables (ISO/IEC 27037, NIST SP 800-86, etc.).

Calcular y registrar los valores hash: Calcular y registrar los valores hash (SHA-256, SHA-512 u otro) de la evidencia digital recibida, en el momento mismo de su recepción, y dejar constancia de los mismos en la Planilla de Registro de Cadena de Custodia y en la presente acta. Estos valores servirán como "huella digital" para verificar la integridad de la evidencia en cualquier momento futuro.

Realizar el dictamen pericial: Elaborar un informe pericial objetivo, imparcial, y técnicamente fundamentado, que contendrá la descripción del análisis realizado, los métodos y herramientas utilizados, los resultados obtenidos, y las conclusiones a las que se llegue.

Custodia y confidencialidad: Guardar estricta confidencialidad sobre toda la información conocida en el ejercicio de su función, y no divulgarla a terceros no autorizados.

Ponerse a disposición del tribunal: Estar disponible para comparecer a declarar en el juicio oral y ratificar su dictamen, en caso de ser requerido por la autoridad judicial competente.

QUINTA: APLICACIÓN DE LA CADENA DE CUSTODIA: El(la) Perito(a) declara que iniciará la Planilla de Registro de Cadena de Custodia, en la que se documentará cada transferencia de la evidencia, desde su recepción hasta su disposición final, incluyendo fecha, hora, responsables y motivos del traslado. La evidencia será manejada exclusivamente por personal autorizado, y será almacenada en condiciones que garanticen su integridad.

SEXTA: CÁLCULO DE HASH DE LA EVIDENCIA: En el acto de recepción, se procede al cálculo de los valores hash de la evidencia consignada, dejando constancia de los siguientes resultados:

Archivo/Dispositivo: _____
Algoritmo utilizado: ( ) SHA-256 ( ) SHA-512 ( ) Otro: _____
Valor Hash (huella digital): _____
Fecha y hora del cálculo: _____
Herramienta utilizada: _____
Responsable del cálculo: _____

SÉPTIMA: DOCUMENTACIÓN ADJUNTA: Se deja constancia de que, junto con la presente acta, se anexa copia del(los) siguiente(s) documento(s):

( ) Copia del documento de identidad del(la) Consignatario(a).
( ) Copia del documento de identidad del(la) Perito(a).

( ) Registro o credencial del(la) Perito(a).
( ) Planilla de Registro de Cadena de Custodia (inicial).
( ) Descripción detallada de la evidencia.
( ) Fijación fotográfica de la evidencia (si se realizó).
( ) Documento que acredita la representación legal (si aplica).
( ) Otros: _____

OCTAVA: ACEPTACIÓN Y FIRMA: En señal de conformidad con todas y cada una de las cláusulas establecidas en la presente acta, se firma a los [día] días del mes de [mes] del año [año], en [lugar y fecha].

EL(LA) CONSIGNATARIO(A)	**EL(LA) PERITO(A) / EXPERTO(A) FORENSE**
Nombre y Apellido	Nombre y Apellido
Cédula de Identidad N°	Cédula de Identidad N°
Firma	Credencial / Matrícula N°
	Firma
TESTIGO(S)	
Nombre y Apellido	Nombre y Apellido
Cédula de Identidad N°	Cédula de Identidad N°
Firma	Firma