CONTENIDO

Elaborado por:	Revisado y Aprobado por:	Aprobación Metodológica por:
Nombre: Katherine Suárez Ardila Cargo: Coordinadora del Grupo de Trabajo de Informática Forense y Seguridad Digital.	Nombre: Adriana Cetina Hernández Cargo: Jefe Oficina de Tecnología e Informática	Nombre: Giselle Johanna Castelblanco Muñoz Cargo: Representante de la Dirección para el Sistema de Gestión de Calidad Fecha: 2025 -02-19

1 OBJETIVO

Establecer los lineamientos generales para la atención de solicitudes, la aplicación eficiente del Modelo API (Adquisición, Procesamiento e Investigación), y la custodia segura del material probatorio y/o confidencial en las diversas áreas y dependencias de la Superintendencia de Industria y Comercio (en adelante, **SIC**), garantizando la integridad y confidencialidad de la información a lo largo de todo el proceso.

2 DESTINATARIOS

El instructivo de Informática Forense está dirigido a los funcionarios y/o contratistas que participan, directa o indirectamente, en las actividades del **Grupo de Trabajo de Informática Forense y Seguridad Digital** (en adelante, **GTIFSD**), así como a las áreas o dependencias de la **SIC** que tengan interés en estos procesos.

3 GLOSARIO

ADQUISICIÓN DE COMPUTADORAS: Actividad realizada durante una Visita de Inspección Administrativa, en la que se realiza una copia exacta de los mensajes de datos de los ordenadores con sistemas operativos MAC OS, Windows y/o Linux.

ADQUISICIÓN DE MÓVILES: Recolección de datos de dispositivos móviles como tabletas, celulares, y GPS, utilizando diversos métodos de extracción según el sistema operativo (iOS o Android).

CADENA DE CUSTODIA: Registro que garantiza la autenticidad de las evidencias materia de prueba que han sido recolectadas en el transcurso de la actuación administrativa –averiguación preliminar o investigación- que permite asegurar la integridad y confidencialidad de los elementos probatorios en todas las etapas procesales[1].

CONTENEDOR DE EVIDENCIA DIGITAL: Es el elemento o dispositivo en el que se guardan las evidencias digitales y los mensajes de datos de forma permanente o temporal. Existe variedad importante de contenedores entre los que se encuentran el CD, el DVD. el Blu-ray, el USB y el disco duro. En tanto. la cadena

[1] Tomado del Manual de Cadena de Custodia de la Fiscalía General de la Nación.

de custodia registra la ubicación y los procedimientos hechos a la evidencia que se encuentra en estos contenedores[2].

COPIA DE MENSAJES DE DATOS: Actividad que consiste en realizar una copia espejo de los datos desde un dispositivo origen a un dispositivo de destino, preservando toda la información, incluyendo bloques de archivos eliminados, espacio libre, metadatos, etc.

CREACIÓN DE LISTA DE INVESTIGACIÓN: Documento que identifica a los participantes de una conducta, actividad o tarea investigada, y establece la asociación directa o indirecta sobre la misma.

CUSTODIO: Persona que vigila y guarda con cuidado y responsabilidad un Elemento Material Probatorio (en adelante, EMP) o Evidencia Física (en adelante, EF) o un lugar de los hechos[3].

DESCARGA DE CONTENIDOS EN LA NUBE: Actividad de adquisición de mensajes de datos alojados en cuentas de correo electrónico o sistemas de almacenamiento en la nube.

ELEMENTO MATERIAL PROBATORIO: Es cualquier objeto que demuestre una conducta en contra de la ley. Según el literal g del artículo 275 de la Ley 906 de 2004, un mensaje de datos puede ser considerado un elemento material probatorio una vez haya sido aportado a un proceso legal, y debe estar protegido garantizando su integridad, confidencialidad y disponibilidad, es decir, que el mensaje de datos recolectado en campo es el mismo mensaje de datos presentado ante una autoridad legal. Adicionalmente, debe haber un registro en el cual se evidencie quién ha sido responsable de custodiar y transportar el mensaje de datos o el contenedor donde éste se encuentre, y así mismo quién o quiénes han sido los investigadores y han tenido contacto con el mismo[4].

EMBALAR: Es el procedimiento técnico utilizado para empacar, preservar y proteger los Elementos Materiales Probatorios y Elementos Físicos en el contenedor adecuado con el fin de ser enviados para análisis o almacenamiento[5].

ESTRUCTURA DE CARPETAS: Parámetros a seguir para la organización de las carpetas (estructura de directorios) en donde se albergan los mensajes de datos adquiridos durante la Visita de Inspección Administrativa.

[2] B, Prieto (2017). El uso de los métodos deductivo e inductivo para aumentar la eficiencia del procesamiento de adquisición de evidencias digitales.
[3] Tomado del Manual de Cadena de Custodia de la Fiscalía General de la Nación.
4 Ley 906 de 2004, Artículo 275
5 Tomado del Manual de Cadena de Custodia de la Fiscalía General de la Nación.

ETIQUETA: Agrupación de un conjunto de datos que comparten un criterio específico.

EVIDENCIA DIGITAL: Cualquier información que, sujeta a una intervención humana u otra semejante, ha sido extraída de un medio informático. Es decir, cualquier registro generado por o almacenado en un sistema computacional que puede ser utilizado como evidencia en un proceso legal[6].

EXTRACCIÓN FÍSICA: Método que algunos casos requiere la manipulación del dispositivo móvil. Este realiza una copia bit a bit de todo el contenido de la memoria flash, incluyendo el espacio sin asignar, lo que permite recuperar información eliminada recientemente. Aunque proporciona un mayor número de datos extraídos, es el menos soportado por los dispositivos[7].

EXTRACCIÓN LÓGICA: Método soportado por la mayoría de los dispositivos móviles, en el que se utilizan las API (Application Programming Interface) disponibles desde la fabricación del dispositivo. El software forense envía comandos al teléfono, que a su vez envía datos desde su memoria. Los datos típicamente adquiridos incluyen SMS, MMS, contactos, registros de llamadas y calendarios[8].

EXTRACCIÓN DE SISTEMAS DE ARCHIVOS: Método que proporciona un volumen intermedio de datos, extrayendo los archivos de sistema del dispositivo móvil, datos del usuario, aplicaciones y algunos archivos ocultos o protegidos. Este tipo de extracción puede recuperar información no visible en una extracción lógica[9].

FIJAR: Registrar o determinar mediante diferentes métodos (fotografía, video, topografía, descriptiva, entre otros), las características y ubicación geográfica de los EMP y EF, así como su relación con el lugar de los hechos[10].

FORMATO DE METODOLOGÍA INVESTIGACIÓN: Documento que facilita la reconstrucción de los hechos, permitiendo identificar personas y generar hipótesis más congruentes del caso investigado.

FUNCIÓN HASH: Una función criptográfica hash, comúnmente conocida como "hash", es un algoritmo matemático que transforma un bloque arbitrario de datos

[6] Tomado de HB:171 2003 GuideLines for the Management of IT Evidence.
[7] Tomado de Investigación forense de dispositivos móviles: metodologías y herramientas - Ondata International
[8] Ibidem
[9] Ibidem
[10] Tomado del Manual de Cadena de Custodia de la Fiscalía General de la Nación.

en una cadena de caracteres de longitud fija. Esta salida permite verificar la confiabilidad, integridad y autenticidad de los datos, lo que a su vez facilita su admisibilidad y fuerza probatoria como evidencia en un proceso legal[11].

IMAGEN FORENSE: Es una copia bit a bit de la información que se encuentra en un dispositivo. Sus dos principales características son (i) que tiene una función hash única que garantiza su integridad desde la creación de la imagen, y (ii) que no modifica la información o los mensajes de datos a los cuales se les realiza este procedimiento[12].

IMAGEN FORENSE COMPLETA: Es una copia bit a bit de todos los sectores de un dispositivo o equipo. Estas imágenes pueden ser (i) **físicas:** que corresponden a la superficie del dispositivo, y (ii) **lógicas:** que corresponden a las particiones lógicas del mismo.

IMAGEN FORENSE PARCIAL: Es una copia bit a bit de solo uno o varios mensajes de datos que están contenidos dentro del dispositivo o equipo, y que se ubican en un sector particular. Ejemplo: una imagen forense del archivo de correo electrónico de Outlook (.pst) que está ubicado en el escritorio del sistema operativo.

INFORMÁTICA FORENSE: Aplicación de la ciencia para la identificación, recolección, examen y análisis de los datos, preservando correctamente su integridad, llevando a cabo a su vez una estricta cadena de custodia de la información[13].

INSTRUCTIVO DE VISITA: Documento dirigido a los funcionarios y/o contratistas encargados de realizar la Visita de Inspección Administrativa, en el cual se encuentra la información necesaria para la identificación del caso, los hechos que en los que se fundamenta la actuación y, entre otros aspectos como la información a recaudar durante la visita mediante los medios de prueba contemplados en la Ley.

LÍNEA DE TIEMPO: Relación cronológica de hechos, eventos e incidentes investigados para visualizar y contextualizar la reconstrucción del caso.

[11] Tomado de Karspesky Latam - https://latam.kaspersky.com/blog/que-es-un-hash-y-como-funciona/2806/.
[12] B, Prieto (2017). El uso de los métodos deductivo e inductivo para aumentar la eficiencia del procesamiento de adquisición de evidencias digitales.
[13] Tomado de la Guía de Evidencia Digital del Ministerio de la Tecnologías de la Información y las Comunicaciones - MINTIC.

MEMORIA VOLÁTIL: Es aquella memoria cuya información se pierde al interrumpirse el flujo eléctrico. Dicha información reposa en las memorias de acceso aleatorio conocidas como memorias RAM.

MENSAJE DE DATOS: La información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el Intercambio Electrónico de Datos (EDI), Internet, el correo electrónico, el telegrama, el télex o el telefax[14].

MODELO API: Buenas prácticas para la adquisición, procesamiento e investigación de la evidencia digital, basado en el modelo EDRM.

- ADQUISICIÓN: La fase de adquisición se refiere a la identificación, preservación y recolección de las evidencias digitales. Para esto, se obtienen imágenes forenses o copias bit a bit para garantizar la integridad de la información, es decir, asegurar que la información adquirida es exactamente igual a la que se almacena en el dispositivo de origen.

- PROCESAMIENTO: El procesamiento se refiere a la reducción del volumen de información electrónicamente almacenada (ESI, por sus siglas en inglés) y, cuando es necesario, a su conversión a formatos más adecuados para su revisión y análisis. También, incluye la transferencia de la información recolectada desde los dispositivos de destino hacia el expediente o soporte documental del caso, así como la extracción y recuperación de datos contenidos en las evidencias digitales, entre otros aspectos.

  Además, en esta etapa se pone a disposición de los expertos en la materia —quienes pueden tener una formación profesional distinta a la de un analista forense— los casos procesados para su análisis, revisión o cualquier otra acción que consideren pertinente.

- INVESTIGACIÓN: Esta etapa se centra en el análisis y revisión de los mensajes de datos con base en el propósito u objetivo de cada caso. Durante esta fase, se evalúan minuciosamente los mensajes de datos para determinar su relevancia y si cumplen con los criterios necesarios para ser considerados como elementos materiales probatorios.

MODELO EDRM: El Modelo de referencia de descubrimiento electrónico, también conocido como EDRM o el diagrama de EDRM, describe los procesos y etapas clave del proceso de descubrimiento electrónico en forma de nueve fases

[14] Definición de acuerdo con Ley 527 de 1999 Artículo 2º

interrelacionadas: Gobernanza de la información, identificación, conservación, recolección, procesamiento, revisión, análisis, Producción y presentación. Cada fase representa una etapa central del proceso de descubrimiento electrónico. Al dividir el proceso de descubrimiento electrónico en fases, los profesionales pueden aprovechar los recursos básicos (es decir, personas, tecnología y procesos) de una manera más organizada para lograr los resultados deseados[15].

PRINCIPIO DEL ORDEN DE VOLATILIDAD: El orden de volatilidad hace referencia al período de tiempo en el que está accesible cierta información. Es por ello que se debe recolectar en primer lugar aquella información que vaya a estar disponible durante el menor período de tiempo, es decir, aquella cuya volatilidad sea mayor[16].

De acuerdo con esta escala se puede crear la siguiente lista en orden de mayor a menor volatilidad:

- Registros y contenido de la caché.
- Tabla de enrutamiento, caché ARP, tabla de procesos, estadísticas del kernel, memoria.
- Información temporal del sistema.
- Disco
- Logs del sistema.
- Configuración física y topología de la red.
- Documentos.

PERSONAS DE INTERÉS: Son todas las personas naturales o jurídicas que surgen como agentes relevantes en el caso y que facilita la reconstrucción de los hechos en el mismo.

PRIMER RESPONSABLE: Es el particular o el servidor público que, por razón de su trabajo o por el cumplimiento de las funciones propias de su cargo, entran en contacto con EMP y EF, y que, por tanto, son responsables por su recolección, preservación y entrega a la autoridad competente[17].

REGISTRO DE CADENA DE CUSTODIA: Es la documentación de cada traspaso y traslado del EMP y EF, durante el desarrollo del proceso de cadena de custodia. Es decir, es la actuación mediante la cual se documenta de manera física y virtual,

[15] Tomado de https://edrm.net/wiki/edrm-model/
[16] Tomado de RFC 3227 - Directrices para la recopilación de evidencias y su almacenamiento
[17] Tomado del Manual de Cadena de Custodia de la Fiscalía General de la Nación.

la información de los EMP y EF y los actores que intervinieron en el sistema de cadena de custodia[18].

RÓTULO: Formato diligenciado que se adhiere al contenedor con fines de identificación del EMP y EF[19].

SUITE DE LOS FABRICANTES DE DISPOSITIVOS MÓVILES: Software específico de los fabricantes de dispositivos móviles que permite la sincronización y administración de dispositivos desde un equipo de cómputo.

TRASPASAR: Es el acto por el cual un custodio entrega la guarda y responsabilidad del lugar de los hechos y los Elementos Materiales Probatorios y Evidencia Física a otro custodio[20].

TRASLADAR: Es el movimiento que se hace de los Elementos Materiales Probatorios y Evidencia Física, de un sitio a otro[21].

UNIFICACIÓN: Actividad por medio del cual se reúne la información adquirida de uno o varios contenedores de evidencia digital de origen a uno o varios contenedores de evidencia digital destino en donde reposará la información de manera integral. Esta actividad se encuentra respaldada por distintos informes técnicos.

VERIFICACIÓN IMAGEN FORENSE: Comprobación del estado de la imagen forense para garantizar la exactitud y validez de la copia adquirida mediante una función hash.

VISITA DE INSPECCIÓN ADMINISTRATIVA: Es aquel medio de prueba dirigido a la verificación o esclarecimiento de los hechos materia de la actuación – averiguación preliminar o investigación - que hace un funcionario de un lugar, una cosa o un documento.

4 GENERALIDADES

Este instructivo describe las actividades de apoyo basado en el Modelo API. Por lo tanto, el **GTIFSD**, es el encargado de atender las solicitudes de cada una de las áreas o dependencias de la **SIC** relacionadas con el servicio de apoyo en las técnicas de Adquisición, Procesamiento e Investigación de mensajes de datos y/o

[18] Ibidem
[19] Ibidem
[20] Ibidem
[21] Ibidem

evidencias digitales, garantizando el valor probatorio de la información mediante herramientas de hardware y software especializado, descrito en el *GS04-P01 Procedimiento de Acompañamiento de Visitas y Solicitudes de Informática Forense*.

4.1 MODELO DE ADQUISICIÓN, PROCESAMIENTO E INVESTIGACIÓN (API)

Este modelo surge de la flexibilidad y versatilidad del modelo EDRM, manteniendo su objetivo principal a pesar de las modificaciones o alteraciones que puedan hacerse a su estructura base.

Debido a su simplicidad, el Modelo API es más accesible, especialmente para quienes no están directamente relacionados con esta área del conocimiento. Además, en Colombia, este modelo es ampliamente reconocido y avalado por distintos entes judiciales, administrativos y afines.

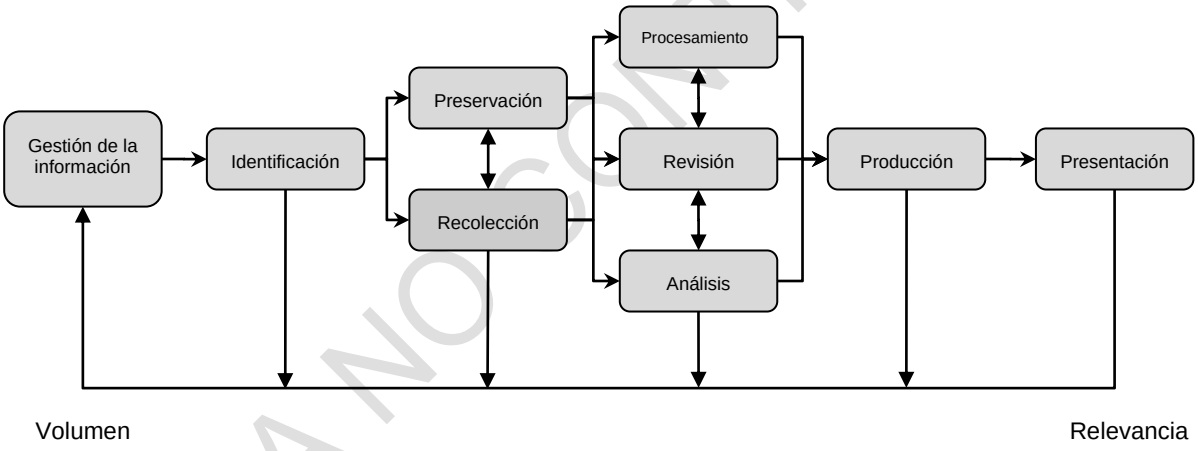

Ilustración 1. Modelo EDRM (Electronic Discovery Reference Model). Ilustración Propia.

A continuación, se presenta la aplicación del nuevo modelo y la explicación de cada una de sus etapas:

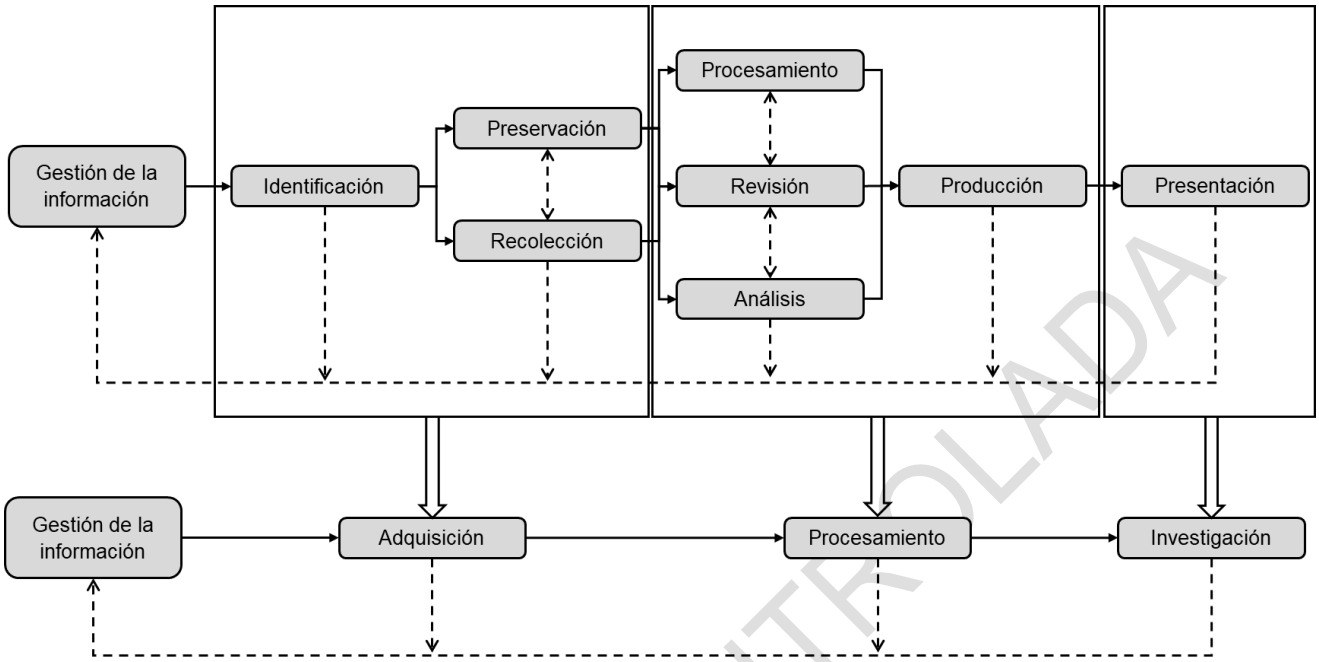

Ilustración 2. Adaptación del Modelo EDRM al Modelo API (Adquisición, Procesamiento e Investigación). Ilustración Propia.

Como se ha mencionado anteriormente, el Modelo API tiene una flexibilidad equivalente al modelo EDRM, permitiendo no solo el entendimiento total a partir de la simplificación de su esquema, sino también la posibilidad de realizar las iteraciones necesarias y regresar a una fase anterior si así se requiere.

4.1.1 ADQUISICIÓN

En esta etapa se integran las fases de identificación, preservación y recolección del modelo EDRM. Esto implica que, durante esta fase, se lleva a cabo la identificación y adquisición de información relevante para cualquier proceso administrativo o judicial. Asimismo, es fundamental garantizar que la recolección de los mensajes de datos de acuerdo con los criterios establecidos por el Artículo 11 de la Ley 527 de 1999.

Así las cosas, resulta eficiente considerar que debe presentarse un equilibrio entre la cantidad de información y su relevancia, ya que un gran volumen de información no implica una mayor cantidad de hallazgos útiles para la investigación. Por lo tanto, el equipo a cargo de esta etapa tiene la responsabilidad de realizar una inspección minuciosa de toda la información disponible, con el objetivo de identificar elementos que puedan ser realmente valiosos.

4.1.2 PROCESAMIENTO

Esta etapa agrupa las fases de procesamiento, revisión y análisis del modelo EDRM. En el contexto del modelo API, el procesamiento implica, entre otras cosas que la información adquirida en la etapa anterior sea transferida a un contenedor donde pueda ser preservada según las políticas internas y/o las exigencias legales.

Asimismo, se llevan a cabo las acciones necesarias para revisar y analizar la información, lo cual incluye la reconstrucción de archivos dañados, recuperación de elementos eliminados, expansión de archivos compuestos, conversión de archivos a formatos más accesibles, indexación de mensajes de datos, y extracción de texto de imágenes mediante herramientas de reconocimiento de caracteres, entre otras tareas. El nivel de procesamiento varía según las necesidades del caso; en algunas situaciones, se sigue un estándar que adapta esta fase a la cantidad y naturaleza de los mensajes de datos, lo que determina la duración del proceso.

Además, una vez procesados, los mensajes de datos se ponen a disposición a través de herramientas especializadas que permiten visualizarlos sin riesgo de modificación o alteración, garantizando así su integridad.

Es importante que las herramientas utilizadas en esta fase sean intuitivas y fáciles de usar, ya que no siempre son expertos forenses quienes las manejan. A menudo, se utilizan soluciones del mismo fabricante para ambas etapas, ya que estas suelen estar diseñadas para cubrir todas las necesidades del modelo EDRM en una misma suite de aplicaciones.

4.1.3 INVESTIGACIÓN

Esta etapa final del proceso implica la identificación y análisis de los mensajes de datos para cumplir con su propósito dentro de la actuación en curso. Según su relevancia, estos pueden ser categorizados como Elementos Materiales Probatorios.

4.2 CONTROLES DE ACCESO

Conjunto de políticas, procedimientos, y mecanismos tanto físicos como digitales, diseñados para regular y restringir el acceso a recursos, sistemas e información dentro de la Entidad. Estos controles aseguran que solo personas autorizadas (funcionarios y/o contratistas), de acuerdo con sus roles y responsabilidades,

puedan acceder a ciertos datos o sistemas, protegiendo así la confidencialidad, integridad y disponibilidad de los recursos organizacionales.

4.2.1 ACCESO A LA INFORMACIÓN

El acceso a la información digital ya sea mediante dispositivos de almacenamiento físico o almacenamiento en la nube, requerirá la autorización previa del Coordinador del **GTIFSD**, o del Coordinador del grupo custodio de la información. Bajo ninguna circunstancia se permitirá el acceso a funcionarios y/o contratistas sin la correspondiente autorización. Es importante mencionar que, el acceso estará restringido exclusivamente a la ejecución de las funciones del funcionario y/o contratista, siempre que dichas actividades lo requieran.

En situaciones que lo ameriten, ya sea por solicitud formal o por disposición legal, se podrá conceder acceso a terceros. Esta autorización deberá ser otorgada por el Coordinador del grupo custodio de la información y/o el Coordinador del **GTIFSD**. Todas estas solicitudes deberán ser gestionadas a través del sistema oficial de trámites y registradas formalmente ante la SIC.

4.3 CONFIDENCIALIDAD

Todo funcionario y/o contratista que, en el ejercicio de sus funciones, tenga acceso a información o evidencia digital, ya sea para su recolección, almacenamiento, análisis, observación o cualquier tipo de interacción, está comprometido, desde su vinculación con la SIC, a salvaguardar la confidencialidad de dicha información. Por lo tanto, está estrictamente prohibida la copia o distribución de esta información, a menos que sea necesario para el desarrollo de sus funciones y cuente con la autorización explícita de su supervisor, jefe inmediato o el custodio de la evidencia.

A continuación, se cita un ejemplo de cláusulas de confidencialidad en los contratos de los funcionarios y/o contratistas:

> "(…) *6 Dar cumplimiento al procedimiento de Administración de Bienes devolutivos y de consumo de la CONTRATANTE, velar por el buen uso de los bienes y elementos entregados por la Contratante, para el ejercicio de las actividades relacionadas con a la ejecución del objeto contractual. Abstenerse de utilizarlos para fines y lugares diferentes a los convenidos, y entregarlos a la finalización del vencimiento del plazo pactado.*
>
> *7 Mantener y garantizar total confidencialidad sobre la información que le sea entregada para el cumplimiento del objeto del contrato, durante la ejecución*

del mismo y con posterioridad a su finalización, la cual no será compartida o divulgada a terceras personas no relacionadas con el desarrollo de las labores encomendadas por la CONTRATANTE. Cualquier información que sea requerida sólo será suministrada previa autorización escrita y expresa dada por la CONTRATANTE. Así mismo, deberá cumplir lo estipulado en el documento: Acuerdo de seguridad y privacidad para Contratistas, publicado en el Sistema Integral de Gestión Institucional – SIGI, el cual se entiende conocido y aceptado con la suscripción del presente contrato. (…)"

5 DESCRIPCIÓN DE ACTIVIDADES

5.1 ATENDER SOLICITUD - VISITA DE INSPECCIÓN ADMINISTRATIVA

El siguiente procedimiento, de forma resumida, describe los pasos para atender una solicitud de acompañamiento por parte de un Ingeniero Forense del **Laboratorio de Informática Forense** en una Visita de Inspección Administrativa:

- Los Jefes o Coordinadores de las distintas áreas o dependencias de la **SIC** generan la solicitud de acompañamiento para las Visitas de Inspección Administrativa, junto con los dispositivos forenses necesarios.

- El Coordinador del **GTIFSD** recibe la solicitud y la asigna a un funcionario y/o contratista del grupo para su gestión y cumplimiento.

- Se realiza el alistamiento de los equipos y documentos requeridos para la visita administrativa.

- Los funcionarios y/o contratistas designados para acompañar las Visitas de Inspección Administrativa se encargan de adquirir y/o recolectar los mensajes de datos relevantes para la actuación administrativa, asegurar la evidencia digital mediante los mecanismos forenses adecuados, incluyendo el diligenciamiento de la cadena de custodia, y transportar los contenedores de evidencia digital al **Laboratorio de Informática Forense**.

Adicional, los funcionarios y/o contratistas tienen a su cargo las siguientes actividades complementarias relacionadas con las Visitas de Inspección Administrativas:

- Procesamiento de las evidencias digitales, gestión y soporte en la creación de usuarios, asignación de permisos y uso de herramientas de investigación web.

- Apoyo en las investigaciones desarrolladas por las distintas áreas o dependencias de la **SIC** mediante la búsqueda de información a través de vectores de búsqueda y el análisis de la misma.

- Gestión de solicitudes adicionales, tales como: copia de evidencia digital, preservación de páginas web, elaboración de informes técnicos forenses, traslado de evidencia digital, depuración de mensajes de datos, exportación de elementos de evidencias digitales, entre otros.

5.2 LINEAMIENTOS INICIALES

5.2.1 PREPARACIÓN

El funcionario y/o contratista debe preparar cuidadosamente los recursos necesarios (software, hardware y documentación) para la adquisición y/o recolección de las evidencias digitales, basándose en un análisis exhaustivo del caso.

ID TAREA	NOMBRE DE LA TAREA	DESCRIPCIÓN	ARTEFACTOS/FORMATOS/ EVIDENCIAS
1	Reunión de Visita	Asistir a reunión previa a la visita para conocer detalles del caso	
2	Verificar los detalles del caso	Determinar la información a recolectar y el equipo necesario para realizar una adquisición y/o recolección adecuada, minimizando la pérdida o alteración de los mensajes de datos. Esto se logrará a través de la revisión exhaustiva del instructivo de visita correspondiente al caso.	Instructivo de visita del caso
3	Preparar paquete de visita	Preparar los elementos necesarios para la adquisición y documentación de mensajes de datos.	• Computador Portátil (1) • Maletín UFED con su respectiva Dongle en caso de ser necesario (1) • Disco Duro (2) • Bloqueadora de Escritura (1) • Dongle Digital Collector (MacQuisition) (1) • Grabadora (1) • Cámara Fotográfica con tarjeta de memoria (1) • Batería de repuesto para grabadora (1) • Lectora de DVD/Blu-ray (1) • Hub (1) • *GS04-F02 Formato de Adquisición de Imágenes Forenses* (20) • *GS04-F01 Registro Cadena de Custodia* (5) • DVD con funda (1)

ID TAREA	NOMBRE DE LA TAREA	DESCRIPCIÓN	ARTEFACTOS/FORMATOS/ EVIDENCIAS
			● Sellos (5) ● Testigos Métricos ● Señaladores Numéricos ● GS04-F03 Rotulo Elemento Materia de Prueba o Evidencia Física (5) Todo lo anterior según instructivo de preparación de paquetes de visita
4	Revisión de los elementos	Revisar rigurosamente el funcionamiento y estado de los elementos para la adquisición y documentación de mensajes de datos.	● Grabadora: Pilas con carga suficiente y sin grabaciones en la memoria. ● Cámara Fotográfica: Sin fotografías en la memoria, con pila y funcionando. ● Dongle UFED: Funcionando con el software UFED 4PC y UFED Physical Analyzer. ● Kit UFED: cables completos. ● Discos Duros: Revisión de estado y funcionamiento con software Crystal Disk. Todo lo anterior según instructivo de preparación de paquetes de visita
5	Preparar software forense	Asegurarse de contar con las herramientas de software actualizadas. Estas herramientas deben ser almacenadas en los dispositivos magnéticos (USB de Visita) designados por el **Laboratorio de Informática Forense** para tal fin.	● USB de Visita ● FTK Imager ● UFED 4PC ● UFED Physical Analyzer ● Digital Collector ● Winaudit ● CrystalDisk ● Bat inventario redes ● Bat inventario PC ● MAC OS X ● MD5 Summer ● Evidence Collector ● Easy Robocopy ● Encase ● Fastcopy ● TreeSize ● VSO Inspector ● CD Burner ● Xinorbis ● Suite de los fabricantes de dispositivos móviles. ● Otros

Tabla 1. Lineamientos iniciales

Gestión y Supervisión de Equipos para la Visita de Inspección Administrativa

El Coordinador del **GTIFSD** solicitará al funcionario y/o contratista encargado de la administración y supervisión del inventario físico que prepare y entregue al personal asignado para la Visita de Inspección Administrativa los equipos y

herramientas necesarios para cumplir con la solicitud. Estas herramientas formarán parte del inventario físico del **GTIFSD**, el cual será verificado periódicamente o según las solicitudes del Coordinador. Para esta tarea se llevará un control detallado del inventario y del préstamo de equipos a través de la plantilla "*INVENTARIO DEL LIF*".

El uso de los equipos proporcionados por la Entidad para el **GTIFSD** estará limitado exclusivamente a las funciones del grupo, y no se permitirá su uso para fines personales o privados por ningún miembro del **GTIFSD** ni por otro funcionario y/o contratista de la Entidad.

Cada Ingeniero Forense, al recibir los equipos, los revisará y registrará su salida en el "*Control de Inventario de Equipos y Elementos del LIF*" como soporte de la entrega.

Al finalizar la Visita de Inspección Administrativa, cada Ingeniero Forense será responsable de devolver los equipos completos y en buen estado. La persona encargada de recibirlos verificará su estado y registrará su retorno en la planilla de Control de Inventario. En caso de faltantes o daños, notificará de inmediato al Coordinador del **GTIFSD** y al Ingeniero Forense correspondiente mediante correo electrónico.

Solicitud de Permiso para el Retiro de Activos del GTIFSD

Será necesario que tanto el Coordinador del **GTIFSD** como el funcionario y/o contratista designado para la administración y custodia del inventario físico, soliciten periódicamente (anualmente) al área de recursos físicos de la Entidad, a través de la plataforma habilitada para tal fin, el permiso correspondiente para el retiro de activos. En dicha solicitud, deberán relacionar uno a uno los activos que requieran ser retirados de la Entidad para la ejecución de las diversas obligaciones del **GTIFSD**.

Esta medida garantizará que los vigilantes del edificio y el área de recursos físicos estén informados sobre qué equipos serán utilizados en actividades dentro y fuera de la Entidad, permitiendo su retiro sin contratiempos.

Póliza Todo Riesgo por Daño Material

La **SIC** cuenta con una póliza de todo riesgo por daño material, la cual cubre todos los equipos en uso ante siniestros como hurto, daños y pérdidas. En el caso del **Laboratorio de Informática Forense**, esta póliza cubre todos los equipos en caso de que ocurra algún imprevisto. Para reportar y hacer la reclamación

correspondiente, se deberá seguir lo estipulado en el documento *GA02-I01 Instructivo para la Reclamación en Caso de Siniestro*.

Es importante señalar que la póliza solo será efectiva ante situaciones imprevistas, por lo que no se podrán realizar reclamaciones si el siniestro ocurre debido a mal uso, descuido o irresponsabilidad por parte de la persona que tenga asignado el equipo.

5.3 ADQUISICIÓN

5.3.1 AISLAMIENTO DE LA ESCENA O UBICACIÓN

Una vez que los funcionarios y/o contratistas designados para la Visita de Inspección Administrativa lleguen al lugar de la diligencia, deberán proceder a aislar la escena para evitar cualquier alteración o contaminación de los dispositivos.

ID TAREA	NOMBRE DE LA TAREA	DESCRIPCIÓN	ARTEFACTOS/FORMATOS / EVIDENCIAS
1	Aislar la escena o ubicación en donde se encuentra el dispositivo del cual se recaudará las evidencias digitales.	● Retirar el personal de la organización objeto de inspección el cual no esté involucrado con el método realizado. ● Solicitar acompañamiento del personal encargado de Tecnología en la organización.	

Tabla 2. Aislar escena

Sellamiento y apertura de la Escena

El funcionario y/o contratista de las áreas o dependencias de la Entidad que lidere la Visita de Inspección Administrativa, firmará los sellos junto con la persona designada por la persona jurídica o natural objeto de la visita.

El profesional del **GTIFSD** será responsable de capturar el registro fotográfico o en video del procedimiento de sellado realizado por el funcionario y/o contratista que esté liderando la visita. Esta evidencia multimedia se almacenará en el contenedor de evidencia digital correspondiente y dicho registro deberá mostrar el momento exacto en que se sellan las puertas de acceso al lugar de los hechos, indicando fecha, hora y lugar, y describiendo el procedimiento de sellado.

Es esencial que se sellen todas las posibles puertas de acceso a la oficina, sala o área relevante, y se tomará un registro fotográfico o en video de cada acceso sellado.

Cuando sea necesario abrir la sala o área aislada, el funcionario y/o Contratista líder de la visita, acompañado por el representante de la entidad o empresa inspeccionada, procederá a verificar el estado de los sellos antes de retirarlos. Es importante que este procedimiento también sea documentado mediante fotografías o videos.

Una vez realizados los registros multimedia tanto del sellado como de la apertura, se procederá a realizar su respectiva imagen forense y se documentarán en el Acta de Visita elaborada por el responsable de la diligencia.

5.3.2 CREACIÓN DE LA ESTRUCTURA DE CARPETAS Y NOMBRAR IMÁGENES

Los Funcionarios y/o Contratistas deben seguir el estándar presentado a continuación para nombrar las evidencias digitales.

ID TAREA	NOMBRE DE LA TAREA	DESCRIPCIÓN	ARTEFACTOS/FORMATOS/ EVIDENCIAS
1	Enumeración Única	El número de identificador de hallazgo deberá ser el mismo que se relaciona en *GS04-F02 Formato de Adquisición de Imágenes Forenses*, en el control de evidencias, así como para el nombre que se le dará a la imagen de la evidencia	Hallazgo 01 Hallazgo 02
2	Utilizar las siglas para nombrar a las empresas	Es necesario utilizar siglas que resuman el nombre de la empresa.	En vez de indicar el nombre completo de la empresa “Superintendencia de Industria y

ID TAREA	NOMBRE DE LA TAREA	DESCRIPCIÓN	ARTEFACTOS/FORMATOS/ EVIDENCIAS
			Comercio" utilizar la sigla "SIC"
3	Utilizar convenciones	Utilizar las siguientes convenciones para nombrar las imágenes especificando el tipo de adquisición.	PC: Computador de escritorio o portátil. CEL: Dispositivo móvil celular. MAIL: Correo Electrónico. WEB: Almacenamiento en la nube y páginas web. DEC: Declaraciones y/o Testimonios. REQ: Requerimientos de información. SERV: Servidores. BD: Base de datos. DD: Discos Duros. USB: Memoria tipo USB. CD: Disco Compacto - Compact Disc. DVD: Disco Versátil Digital - Digital Versatile Disc. BR: Disco Blu-ray – Blu-ray Disc. MULT: Archivos multimedia, fotos y/o videos. INFO: Información tomada de las tareas en ejecución. De los demás dispositivos no relacionados se deberá colocar su abreviatura.
4	Utilizar el nombre y apellido del titular de la evidencia	Utilizar el primer nombre y el primer apellido del titular de la evidencia en mayúscula para nombrarla, separándolos con un guion intermedio. Si se considera necesario también puede incluirse el cargo.	NOMBRE-APELLIDO NOMBRE-APELLIDO-CARGO
5	Nombrar evidencias	Utilizar la numeración única. Usar un guion intermedio entre la enumeración única y la convención de tipo de dispositivo. Utilizar la convención de tipo de dispositivo. Usar un guion bajo entre la convención de tipo de dispositivo y el nombre del titular de la evidencia. Utilizar el nombre y apellido del titular de la evidencia.	01-PC_NOMBRE-APELLIDO 02-WEB_NOMBRE-APELLIDO 03-CEL_NOMBRE-APELLIDO. . . .
6	Enumerar Declaraciones / Testimonios	Las declaraciones/testimonios tienen una numeración independiente y secuencial iniciando desde el número uno.	01-DEC_NOMBRE-APELLIDO 02-DEC_NOMBRE-APELLIDO 03-DEC_NOMBRE-APELLIDO

ID TAREA	NOMBRE DE LA TAREA	DESCRIPCIÓN	ARTEFACTOS/FORMATOS/ EVIDENCIAS
7	Enumerar Inspecciones Oculares	Las inspecciones oculares tienen una numeración independiente y secuencial iniciando desde el número uno.	01-INSP_DESCRIP_CORTA 02-INSP_DESCRIP_CORTA 03-INSP_DESCRIP_CORTA
8	Enumerar información de anexos	Los anexos tienen una numeración relacionada con la evidencia a la que pertenecen.	01-PC_MULT_NOMBRE_APELLIDO 01-PC_INFO_NOMBRE_APELLIDO 02-PC_MULT_NOMBRE_APELLIDO 02-PC_INFO_NOMBRE_APELLIDO
9	Estructurar carpetas de computadores	Cuando se adquiere la información de computadores la carpeta principal debe nombrarse igual que la imagen forense. Esta puede tener hasta 4 subcarpetas, dependiendo del tipo de adquisición y del sistema operativo del computador: 1. Almacena la imagen forense, 2. Almacena la información técnica del dispositivo junto con su respectiva imagen forense. 3. Almacena el registro fotográfico y/o fílmico realizado al dispositivo con su respectiva imagen forense, 4. Almacena la información de la memoria volátil junto con su respectiva imagen forense y pagefile.sys.	01-PC_ NOMBRE-APELLIDO ● IMG_PARC (Imagen forense del computador) ● INFORMACION DATOS HASH ● MULTIMEDIA DATOS HASH ● MV
10	Estructurar carpetas de celulares	Cuando se adquiere la información de celulares la carpeta principal debe nombrarse igual que la imagen forense. Esta carpeta puede tener 3 subcarpetas: 1. Almacena las adquisiciones generadas por la herramienta para la extracción de dispositivos móviles 2. Almacena la imagen forense, 3. Almacena el registro fotográfico y/o fílmico realizado al dispositivo con su respectiva imagen forense.	01-CEL_ NOMBRE-APELLIDO ● IMG_CEL (Imagen forense de las adquisiciones obtenidas) ● EXTRACCION (Extracciones obtenidas por medio de la herramienta) ● MULTIMEDIA
11	Estructurar carpetas de requerimientos	Cuando se adquiere la información de requerimientos la carpeta principal debe nombrarse igual que la imagen forense. Esta carpeta puede tener 2 subcarpetas: 1. Almacena la imagen forense, 2. Almacena el registro fotográfico y/o fílmico realizado al dispositivo con su respectiva imagen forense	01-REQ ● HASH (imagen forense del dispositivo) ● MULTIMEDIA (registro fotográfico al dispositivo entregado o al dispositivo que contiene el requerimiento de información)

ID TAREA	NOMBRE DE LA TAREA	DESCRIPCIÓN	ARTEFACTOS/FORMATOS/ EVIDENCIAS
12	Estructurar carpetas de declaraciones	Cuando se graban audios o videos de testimonios, es necesario crear una carpeta con el nombre “DECLARACIONES” y dentro de ella, se genera una carpeta con el primer nombre y primer apellido de la persona que fue requerida dentro de la diligencia. Generalmente, la carpeta es nombrada con el mismo nombre que la imagen forense. Cada una de las carpetas asociadas a una declaración/testimonio pueden tener 2 subcarpetas: 1. Almacena la imagen forense, 2. Almacena el archivo de audio y/o el video generado.	DECLARACIONES ● 01-DEC_ NOMBRE-APELLIDO GRABACIÓN HASH ● 02-DEC_ NOMBRE-APELLIDO GRABACIÓN HASH
13	Estructurar carpetas de Inspecciones Oculares	Cuando tengan imágenes, fotos o videos de inspecciones oculares realizas durante la visita, es necesario crear una carpeta con el nombre “INSPECCIONES_OCULARES” y dentro de ella, se genera una carpeta con la abreviatura seguida de una descripción corta del procedimiento que se desea preservar. Generalmente, la carpeta es nombrada con el mismo nombre que la imagen forense. Cada una de las carpetas asociadas a una declaración/testimonio pueden tener 2 subcarpetas: 1. Almacena la imagen forense, 2. Almacena el registro multimedia generado.	INSPECCIONES OCULARES ● 01-INSP_DESCRIP_CORTA MULTIMEDIA HASH ● 02-INSP_DESCRIP_CORTA MULTIMEDIA HASH
14	Estructurar otras carpetas	Para los otros tipos de adquisiciones se crea la carpeta con el nombre de la imagen forense y dos subcarpetas, la primera en donde se almacena la imagen forense de la información, y otra en donde se almacena la información primaria.	● 01-WEB_ NOMBRE-APELLIDO DATOS HASH ● 02-MAIL_ NOMBRE-APELLIDO DATOS HASH

Tabla 3. Estructurar Carpetas y Nombrar Evidencias

5.3.3 IDENTIFICACIÓN DE LAS FUENTES DE INFORMACIÓN

El Funcionario y/o Contratista en sitio deberá identificar todas las posibles fuentes de información digital que almacenen mensajes de datos relevantes para la investigación.

Una vez obtenida la autorización del propietario de la información, procederá a verificar la autenticidad y el estado de los dispositivos que contienen los mensajes de datos. Luego, hará una correcta fijación de estos dispositivos mediante fotografías o videos para preservar la integridad de la evidencia.

ID TAREA	NOMBRE DE LA TAREA	DESCRIPCIÓN	ARTEFACTOS/FORMATOS/ EVIDENCIAS
1	Identificar fuentes de información	Identificar si la fuente de información es un dispositivo óptico	CD, DVD, Blu-Ray
		Identificar si la fuente de información es un dispositivo magnético	Disco Duro (HDD), Disquete
		Identificar si la fuente de información es un dispositivo electrónico	Computadores, USB, Disco Duro (SSD), tabletas, celulares, entre otros.
2	Identificar fuentes de información en la nube	Identificar servidor de correo electrónico	Yahoo!, Gmail, Outlook, Office365, Zimbra, GoDaddy, entre otros.
		Identificar servidor de almacenamiento en la nube	Dropbox, Google Drive, OneDrive, entre otros.
3	Identificar fuentes de información de respaldo	Identificar si existen copias de seguridad de la información contenida en estos dispositivos y si estos tienen conexiones externas	Cintas, unidades de red, redes de área de almacenamiento (SAN), almacenamiento conectado a red (NAS), entre otros.
4	Realizar el registro fotográfico de la fuente de información	Realizar un registro fotográfico completo del dispositivo que será sometido a imagen forense. Para ello, se tomarán al menos tres fotografías desde diferentes ángulos, asegurando una correcta identificación del dispositivo: • Fotografía frontal del dispositivo. • Fotografía trasera del dispositivo. • Fotografía lateral del dispositivo.	• Dispositivo electrónico con cámara fotográfica • Testigo métrico • Señalador numérico

Tabla 4. Identificar Fuentes de información

5.3.4 PLANIFICACIÓN DEL ORDEN DE ADQUISICIÓN

El Funcionario y/o Contratista deberá planificar el orden de adquisición de los dispositivos identificados previamente, que almacenan los mensajes de datos relevantes. Es fundamental seguir el principio de **orden de volatilidad**, donde los datos más volátiles (aquellos que pueden cambiar o desaparecer rápidamente, como la información en memoria RAM) deben ser adquiridos primero. Esto para

evitar la pérdida de información valiosa y asegurar que se capture de manera íntegra.

La planificación de la adquisición debe considerar la naturaleza de la investigación, pudiendo haber variaciones en el proceso según las características de los dispositivos y la evidencia a recolectar.

ID TAREA	NOMBRE DE LA TAREA	DESCRIPCIÓN
1	Estimar tiempos de adquisición de imagen forense	Realizar un estimado del tiempo de adquisición de la imagen forense dependiendo del tamaño de la evidencia digital
2	Adquirir información de las tareas en ejecución	Las tareas en ejecución, como procesos de sistemas operativos, uso de memoria RAM, y conexiones de red activas, son altamente volátiles, ya que desaparecen o cambian con el reinicio o cierre de aplicaciones.
3	Adquirir información de dispositivos móviles	Los dispositivos móviles almacenan información que puede variar con rapidez, como mensajes de texto, registros de llamadas, aplicaciones de mensajería instantánea (WhatsApp, Telegram), y datos de navegación. Su volatilidad depende del uso constante y la actualización en tiempo real, por eso es importante poner el dispositivo en modo avión o en una bolsa de Faraday.
4	Adquirir publicaciones en redes sociales	Las publicaciones, interacciones y mensajes en plataformas de redes sociales, como Facebook, Twitter, o Instagram, pueden ser eliminadas, modificadas o cambiadas rápidamente, lo anterior implica que deba adquirirse esta información lo más pronto posible.
5	Adquirir correos electrónicos	Los correos electrónicos, aunque más estables que otras formas de datos, pueden ser eliminados o modificados en los servidores de correo, por ello es importante realizar la adquisición con prontitud.
6	Adquirir información de páginas web y servidores en la nube	Las páginas web, aplicaciones móviles y servidores en la nube pueden almacenar datos como bases de datos o contenido multimedia que pueden ser modificados o eliminados rápidamente. Es importante extraer esta información con rapidez, ya que puede estar sujeta a cambios.
7	Adquirir registros de sistemas operativos	Los registros del sistema (logs) son menos volátiles que las tareas en ejecución, pero siguen cambiando con el tiempo. Estos registros incluyen actividades como el historial de accesos, el uso de aplicaciones y errores del sistema.
8	Adquirir información de computadores, discos duros y memorias USB	La información de computadores, como archivos almacenados en discos duros, es menos volátil que la memoria y las tareas en ejecución. Sin embargo, sigue siendo crucial extraerla con prontitud, ya que los archivos pueden ser borrados o modificados. Aquí también se incluyen discos duros externos y memorias USB, ya que contienen datos más estables, pero aún susceptibles de eliminación o alteración
9	Adquirir información de bases de datos	Las bases de datos en servidores locales o en la nube son relativamente estables, pero pueden ser alteradas por usuarios con acceso. Es importante adquirir esta información con autenticidad y completar su extracción de forma segura.
10	Adquirir testimonios / declaraciones	Los testimonios/declaraciones realizadas durante la visita o desde las instalaciones de la SIC, deben ser adquiridos de manera precisa y registrados formalmente. Estos suelen ser de baja volatilidad, pero críticos para la investigación.

Tabla 5. Planificar orden de adquisición

5.3.5 IDENTIFICACIÓN DE LAS TAREAS O PROCESOS EN EJECUCIÓN Y DETALLES TÉCNICOS

El Funcionario y/o Contratista procederá a identificar los procesos o tareas en ejecución en los dispositivos inspeccionados, con el fin de determinar si alguno de ellos puede destruir, alterar o modificar los mensajes de datos que se deban recolectar. Además, se examinarán de forma lógica las características técnicas de los dispositivos, incluyendo identificadores únicos (como el número de serie físico), la marca, el modelo, y los componentes de hardware y software del equipo. Esta actividad podrá variar según el tipo de dispositivo que contenga los mensajes de datos a adquirir.

ID TAREA	NOMBRE DE LA TAREA	DESCRIPCIÓN	ARTEFACTOS/FORMATOS/ EVIDENCIAS
1	Captura de la memoria volátil	Capturar el contenido de la memoria RAM del computador, con el fin de identificar las tareas que se encuentran en ejecución.	FTK Imager
2	Captura de la información de la red	Recolectar información de la red	Bat inventario redes
3	Captura de la información del computador	Recolectar información del estado de los discos duros. Realizar inventario de las características de hardware y software del Computador. Obtener los identificadores únicos del equipo.	• Crystal Disk • Winaudit • Bat inventario PC • Herramientas similares

Tabla 6. Examinar tareas en ejecución

5.3.6 ADQUISICIÓN DE LA INFORMACIÓN DIGITAL

Se procederá realizar a la adquisición de los mensajes de datos almacenados en los dispositivos previamente identificados, teniendo en cuenta su tipo y características. Las actividades detalladas a continuación podrán variar en función del método de adquisición, el tamaño de los mensajes de datos, el nivel de seguridad implementado en cada dispositivo, entre otras particularidades.

Asimismo, es fundamental que el experto forense determine qué tipo de información es relevante para el objetivo de la Visita Administrativa, ya que puede encontrarse en ubicaciones no visibles a simple vista o fuera de las habituales. De igual manera, el experto definirá el tipo de imagen forense más adecuado para cada caso procurado no exceder la duración total del acto administrativo.

5.3.6.1 Adquisición de Evidencia Digital de Computadores con Sistema Operativo Windows

La adquisición de evidencia de computadores con sistema operativo Windows puede realizarse mediante diversos métodos y técnicas, que varían según las características del caso. El experto forense podrá realizar una imagen lógica completa, una imagen lógica parcial o una imagen física completa, dependiendo de las particularidades de la situación, esto significa que, durante la adquisición, se podría obtener información de una sola carpeta, de un perfil de usuario específico o de una unidad lógica de disco, entre otras posibilidades.

ID TAREA	NOMBRE DE LA TAREA	DESCRIPCIÓN	ARTEFACTOS/FORMATOS/ EVIDENCIAS
1	Preparar software forense de creación de Imágenes	Incluir el ejecutable de la herramienta forense que permite realizar la adquisición de imágenes forenses	USB de Visita
2	Iniciar el proceso de adquisición de información	Conectar el dispositivo de almacenamiento externo (p.e. memoria tipo USB) al computador que fue entregado e identificado como relevante.	USB de Visita
3	Abrir software para la creación de imágenes de datos.	Ejecutar software forense de creación de imágenes.	FTK Imager
4	Seleccionar la(s) ruta(s) de origen	Identificar las rutas o carpetas fuentes de la información primaria.	FTK Imager
5	Completar información de la imagen forense	Completar la información para la identificación de la imagen forense y utilizar estándar para nombrar imágenes forenses	FTK Imager
6	Seleccionar la ruta destino	Elegir la ubicación en donde se almacenará la imagen forense.	FTK Imager
7	Generar la imagen forense	Completar la parametrización de la herramienta de acuerdo con los lineamientos del **Laboratorio de Informática Forense** de la **SIC** e iniciar con la creación de la imagen forense.	FTK Imager
8	Verificar la Imagen Forense	Comprobar que la imagen forense haya terminado satisfactoriamente y que los hashes tanto de la adquisición como de la verificación hayan coincidido.	.TXT generado por FTK Imager

Tabla 7. Adquisición de computadores con sistema operativo Windows.

5.3.6.2 Adquisición de Evidencia Digital de Computadoras con Sistema Operativo MacOS.

El experto forense podrá realizar una imagen lógica completa, una imagen lógica parcial o una imagen física completa, dependiendo de las particularidades de la situación. Para proceder con la adquisición de este tipo de dispositivos, se tendrán dos alternativas.

Método 1: Este método necesitará contar con el software Digital Collector (MacQuisition) o una herramienta similar.

ID TAREA	NOMBRE DE LA TAREA	DESCRIPCIÓN	ARTEFACTOS/FORMATOS/ EVIDENCIAS
1	Preparar software forense de creación de Imágenes	Incluir dentro de los dispositivos para realizar la visita el dongle de Digital Collector (MacQuisition).	• Digital Collector (MacQuisition) • Herramientas similares
2	Iniciar el proceso de adquisición de información	Conectar el dongle al computador que fue entregado e identificado como relevante.	• Digital Collector (MacQuisition) • Herramientas similares
3	Abrir software para la creación de imágenes de datos.	Ejecutar software forense de creación de imágenes.	• Digital Collector (MacQuisition) • Herramientas similares
4	Completar información de la imagen forense	Completar la información para la identificación de la imagen forense y utilizar estándar para nombrar imágenes forenses	• Digital Collector (MacQuisition) • Herramientas similares
5	Seleccionar la(s) ruta(s) de origen o información relevante del usuario del sistema	Identificar las rutas o carpetas fuentes de la información primaria.	• Digital Collector (MacQuisition) • Herramientas similares
6	Seleccionar la ruta destino	Elegir la ubicación en donde se almacenará la imagen forense.	• Digital Collector (MacQuisition) • Herramientas similares
7	Generar la imagen forense	Completar la parametrización de la herramienta de acuerdo con los lineamientos del **Laboratorio de Informática Forense** de la **SIC** e iniciar con la creación de la imagen forense.	• Digital Collector (MacQuisition) • Herramientas similares
8	Verificar la Imagen Forense	Comprobar que la imagen forense haya terminado satisfactoriamente y sin errores.	.TXT y log de errores generado por la herramienta forense

Tabla 8. Adquisición de computadores con sistema operativo MacOS – Método 1.

Método 2: Este método requerirá la ejecución de comandos a través de la línea de comandos (Terminal) disponible en computadoras con el sistema operativo MacOS. Es importante destacar que el uso de FTK Imager en distribuciones con sistemas operativos MacOS o Linux permite realizar únicamente imágenes forenses completas en los formatos EnCase (E01) o Smart (S01).

ID TAREA	NOMBRE DE LA TAREA	DESCRIPCIÓN	ARTEFACTOS/FORMATOS/ EVIDENCIAS
1	Preparar software forense de creación de Imágenes	Incluir el archivo comprimido de la herramienta forense que permite realizar la adquisición de imágenes forenses	USB de Visita
2	Iniciar el proceso de adquisición de información	Conectar el dongle al computador que fue entregado e identificado como relevante.	USB de Visita

ID TAREA	NOMBRE DE LA TAREA	DESCRIPCIÓN	ARTEFACTOS/FORMATOS/ EVIDENCIAS
3	Abrir la Terminal	Hacer clic en el ícono de Launchpad en el Dock, escribir Terminal en el campo de búsqueda y haz clic en Terminal. En el Finder, abrir la carpeta /Aplicaciones/Utilidades, y haz doble clic en Terminal.	
4	Verificar el disco de origen y de destino	Identificar plenamente la unidad desde donde se va a realizar la imagen forense y la unidad donde se va a almacenar la imagen forense.	Terminal
5	Acceder a la ubicación del archivo de creación de imágenes forense y descomprimirlo	Navegar hasta la ubicación del archivo en la memoria USB y descomprimirlo allí.	Terminal
6	Generar la imagen forense	Completar la parametrización de la herramienta de acuerdo con los lineamientos del **Laboratorio de Informática Forense** de la **SIC** e iniciar con la creación de la imagen forense. 1. Seleccionar el dispositivo de origen. 2. Seleccionar el dispositivo de destino seguido del nombre de la imagen forense. 3. Elegir el formato de la imagen forense 4. Elegir el tamaño para la fragmentación de cada parte de la imagen 5. Elegir el nivel de compresión de la imagen. 6. Completar la información de la imagen forense, tales como, numero de caso, numero de evidencia, descripción, investigador, etc. 7. Incluir la verificación de la imagen forense.	FTK Imager
7	Verificar la Imagen Forense	Comprobar que la imagen forense haya terminado satisfactoriamente y que los hashes tanto de la adquisición como de la verificación hayan coincidido.	.TXT generado por FTK Imager

Tabla 9. Adquisición de computadores con sistema operativo MacOS – Método 2.

5.3.6.3 Adquisición de Evidencia Digital Desde Dispositivos Móviles con Sistema Operativo Android o iOS

La extracción de información de dispositivos móviles dependerá del software forense utilizado y de sus capacidades para recuperar los datos. No siempre será posible obtener toda la información deseada; por ello, el experto forense seleccionará el método de extracción más adecuado según el caso, ya sea

extracción física, extracción lógica, extracción del sistema de archivos, entre otros, para maximizar la cantidad de información recolectada.

Es importante destacar que los procedimientos forenses no borran ni eliminan información de los dispositivos móviles, solo en casos extremos y específicos, podría ocurrir el borrado de aplicaciones o incluso del dispositivo completo.

ID TAREA	NOMBRE DE LA TAREA	DESCRIPCIÓN	ARTEFACTOS/FORMATOS/ EVIDENCIAS
1	Identificar Fabricante del dispositivo móvil	Conectar el dispositivo al computador portátil asignado y seleccionar de acuerdo con el modelo y el sistema operativo del dispositivo móvil el tipo de extracción a realizar	
2	Realizar los ajustes necesarios para iniciar con la extracción de la información	Seguir los pasos previos a la extracción o ajustes que indica la herramienta para preparar el dispositivo móvil, con el fin de evitar errores en el proceso.	• Dispositivo Móvil • UFED 4PC (herramientas similares)
3	Verificar si la copia de respaldo está encriptada	Si el dispositivo cuenta con sistema operativo iOS, verificar mediante la herramienta iTunes que la copia de respaldo no se encuentre encriptada. En caso de estarlo, es necesario deshabilitar esta opción, para ellos es necesario solicitar la contraseña al dueño del dispositivo.	iTunes
4	Ejecutar el método de extracción de la información	Iniciar el procedimiento de extracción de la información del dispositivo móvil. En caso de que la herramienta solicite asignar una contraseña para cifrar la copia de respaldo asigne la que se especifica por defecto.	UFED 4PC (herramientas similares)
5	Verificar Extracción en Physical Analyzer	Abrir mediante la herramienta la(s) extracción(es) para verificar que no cuente(n) con ningún tipo de cifrado y para validar si se extrajo satisfactoriamente la información del dispositivo móvil.	Physical Analyzer (herramienta similar)
6	Solicitar contraseña de cifrado de dispositivo móvil	En caso de que la información del dispositivo móvil se encuentre cifrada es necesario solicitar al dueño del dispositivo dicha contraseña.	
7	Documentar en el Acta de Visita	Especificar en la documentación del acta lo ocurrido con el cifrado de la información, indicando si la contraseña de descifrado fue entregada o no lo fue.	Acta de Visita
8	Seleccionar la(s) ruta(s) de origen	Identificar las rutas o carpetas fuentes de la información primaria.	FTK Imager
9	Completar información de la imagen forense	Completar la información para la identificación de la imagen forense y utilizar estándar para nombrar imágenes forenses	FTK Imager
10	Seleccionar la	Elegir la ubicación en donde se almacenará la	FTK Imager

ID TAREA	NOMBRE DE LA TAREA	DESCRIPCIÓN	ARTEFACTOS/FORMATOS/ EVIDENCIAS
	ruta destino	imagen forense.	
11	Generar la imagen forense	Completar la parametrización de la herramienta de acuerdo con los lineamientos del **Laboratorio de Informática Forense** de la **SIC** e iniciar con la creación de la imagen forense.	FTK Imager
12	Verificar la Imagen Forense	Comprobar que la imagen forense haya terminado satisfactoriamente y que los hashes tanto de la adquisición como de la verificación hayan coincidido.	.TXT generado por FTK Imager

Tabla 10. Adquisición Dispositivos móviles

5.3.6.4 Adquisición de Evidencia Digital de Correos Electrónicos

Las adquisiciones de correos electrónicos se podrán realizar en sitio y de forma particular, en el **Laboratorio de Informática Forense**. Esto para atender las solicitudes hechas por las distintas áreas o dependencias de la SIC, dando cumplimento a descrito en los estándares nacionales e internacionales para la identificación, recopilación, adquisición y preservación de evidencia digital.

ID TAREA	NOMBRE DE LA TAREA	DESCRIPCIÓN	ARTEFACTOS/FORMATOS/ EVIDENCIAS
1	Instalar o preparar el software especializado	Instalar de herramientas para la adquisición de correos electrónicos.	• Aid4Mail (herramientas similares) • Outlook • Thunderbird
2	Identificar el origen de la información (*Caso 1. Dispositivo* o *Caso 2. Nube*)	Identificar las cuentas de correo electrónico que tienen información de carácter laboral o mixto (entiéndase, como laboral y personal), que fueron motivadas en declaraciones juramentadas.	
3	Verificar condiciones para realizar la adquisición **en sitio** o **remota**	Antes de iniciar las actividades de adquisición de la información se debe verificar si la descarga se puede realizarse en sitio; de lo contrario, o en condiciones que le impidan al forense desplazarse al sitio, se realizaran de forma remota.	
EN SITIO			
4	Diligenciar el consentimiento informado.	Diligenciar el consentimiento informado para la realización de la actividad de descarga del correo electrónico.	*GS04-F02 Formato Adquisición Imágenes Forenses*
5	Fijar fotográficamente y describir el dispositivo origen	Realizar la fijación fotográfica del dispositivo que contiene la información de correo electrónico.	• Dispositivo electrónico con cámara fotográfica • Testigo métrico • Señalador numérico
6	**Caso 1. En el Dispositivo**		
6a	Realizar imagen forense parcial	En caso de que el correo se encuentre sincronizado en el computador de escritorio o portátil de la persona dueña de la información, hacer la imagen forense directamente desde el	

ID TAREA	NOMBRE DE LA TAREA	DESCRIPCIÓN	ARTEFACTOS/FORMATOS/ EVIDENCIAS
		dispositivo.	
6b	Seleccionar la(s) ruta(s) de origen	Identificar las rutas o carpetas fuentes de la información primaria.	FTK Imager
6c	Completar información de la imagen forense	Completar la información para la identificación de la imagen forense y utilizar estándar para nombrar imágenes forenses	FTK Imager
6d	Seleccionar la ruta destino	Elegir la ubicación en donde se almacenará la imagen forense.	FTK Imager
6e	Generar la imagen forense	Completar la parametrización de la herramienta de acuerdo con los lineamientos del **Laboratorio de Informática Forense** de la **SIC** e iniciar con la creación de la imagen forense.	FTK Imager
6f	Verificar la Imagen Forense	Comprobar que la imagen forense haya terminado satisfactoriamente y que los hashes tanto de la adquisición como de la verificación hayan coincidido.	.TXT generado por FTK Imager
6	**Caso 2. En la Nube**		
6a	Realizar las configuraciones técnicas.	Verificar junto con el personal del TI de la compañía y/o de la persona dueña de la información, que se puedan realizar las configuraciones necesarias para continuar con la descarga del correo.	
6b	Diligenciar las credenciales de acceso	Parametrizar los datos necesarios para que inicie la descarga (usuario y contraseña).	• Aid4Mail (herramientas similares) • Outlook • Thunderbird
6c	Iniciar y validar la descarga	Comenzar la descarga y validar que la información del correo electrónicos se esté descargando correctamente Hacer las recomendaciones al dueño de la información de no interrumpir el procedimiento, no modificar la contraseña y/o modificar o eliminar la información contenida en el buzón de correo.	• Aid4Mail (herramientas similares) • Outlook • Thunderbird
6d	Realizar la imagen forense parcial del archivo .pst o .ost	Generar la imagen forense parcial una vez se termine el proceso de descarga del correo electrónico.	FTK Imager
6e	Seleccionar la(s) ruta(s) de origen	Identificar las rutas o carpetas fuentes de la información primaria.	FTK Imager
6f	Completar información de la imagen forense	Completar la información para la identificación de la imagen forense y utilizar estándar para nombrar imágenes forenses	FTK Imager
6g	Seleccionar la ruta destino	Elegir la ubicación en donde se almacenará la imagen forense.	FTK Imager
6h	Generar la imagen forense	Completar la parametrización de la herramienta de acuerdo con los lineamientos del **Laboratorio de Informática Forense** de la **SIC** e iniciar con la creación de la imagen forense.	FTK Imager

ID TAREA	NOMBRE DE LA TAREA	DESCRIPCIÓN	ARTEFACTOS/FORMATOS/ EVIDENCIAS
6f	Verificar la Imagen Forense	Comprobar que la imagen forense haya terminado satisfactoriamente y que los hashes tanto de la adquisición como de la verificación hayan coincidido.	.TXT generado por FTK Imager
6e	Borrado seguro de la información	Si se efectuó la descarga en algún equipo diferente al usuario titular de la evidencia, realizar borrado seguro y/o desvinculación de la cuenta de correo. Dejar evidencias del proceso en el contendor de evidencia digital.	Eraser (herramientas similares)
7	Documentar en el Acta	Consignar en el Acta las herramientas que usadas para el procedimiento y los reportes tanto de la herramienta como el informe técnico de la herramienta forense para creación de imágenes forense.	Acta de Visita
REMOTA			
4	Diligenciar el consentimiento informado	Diligenciar el consentimiento informado para la realización de la actividad de descarga del correo electrónico.	*GS04-F02 Formato Adquisición Imágenes Forenses*
5	Realizar las configuraciones técnicas.	El profesional en sitio junto con el personal del TI de la compañía y/o de la persona dueña de la información deben gestionar o realizar las configuraciones necesarias para continuar con la descarga del correo. En caso de que ningún profesional se encuentre en sitio, el profesional designado para la descarga remota hará lo descrito en el formulario de información técnica.	
6	**Caso 2. En la Nube**		
6a	Iniciar y validar la descarga de la información del buzón de correo.	Comenzar y validar que la información del correo electrónicos se esté descargando correctamente.	• Aid4Mail (herramientas similares) • Outlook • Thunderbird
6b	Realizar la imagen forense parcial del archivo .pst o .ost	Generar la imagen forense parcial una vez se termine el proceso de descarga del correo electrónico.	FTK Imager
6c	Seleccionar la(s) ruta(s) de origen	Identificar las rutas o carpetas fuentes de la información primaria.	FTK Imager
6d	Completar información de la imagen forense	Completar la información para la identificación de la imagen forense y utilizar estándar para nombrar imágenes forenses	FTK Imager
6e	Seleccionar la ruta destino	Elegir la ubicación en donde se almacenará la imagen forense.	FTK Imager
6f	Generar la imagen forense	Completar la parametrización de la herramienta de acuerdo con los lineamientos del **Laboratorio de Informática Forense** de la **SIC** e iniciar con la creación de la imagen forense.	FTK Imager
6g	Verificar la Imagen Forense	Comprobar que la imagen forense haya terminado satisfactoriamente y que los hashes tanto de la adquisición como de la verificación	.TXT generado por FTK Imager

ID TAREA	NOMBRE DE LA TAREA	DESCRIPCIÓN	ARTEFACTOS/FORMATOS/ EVIDENCIAS
		hayan coincidido.	
6h	Borrado seguro de la información	Realizar borrado seguro y/o desvinculación de la cuenta de correo. También del borrado de los datos sensibles de la persona dueña de la información. Incluir las evidencias del proceso en el contendor de evidencia digital.	Eraser (herramientas similares)
7	Enviar correo electrónico con notificación de finalización de descarga de correo	Al finalizar la descarga se debe informar mediante un mensaje de correo electrónico enviado desde la cuenta del lifsic@sic.gov.co, a la persona dueña de la información o los interesados, que la descarga finalizó correctamente y como evidencia de este proceso se debe adjuntar el archivo con los hashes creados. En todos los casos se recomienda el cambio de credenciales.	Correo electrónico
8	Documentar en el Acta de Copia de Buzón de Correo Electrónico y Creación de Imagen Forense	Documentar dentro del Acta las herramientas usadas, el procedimiento y los reportes tanto de la herramienta como el informe técnico de la herramienta forense para creación de imágenes forense.	Acta de Copia de Buzón de Correo Electrónico y Creación de Imagen Forense

Tabla 11. Adquisición de información de correos electrónicos

5.3.6.5 Adquisición de Evidencia Digital desde Páginas Web

La adquisición de evidencia digital desde páginas web dependerá de las herramientas forenses empleadas y de su capacidad para capturar la información de manera íntegra y confiable, ya que la estructura y el contenido de las páginas web pueden variar considerablemente, no siempre será posible obtener toda la información deseada. Por esta razón, el experto forense seleccionará el o los métodos de adquisición más adecuados para cada caso. Estos pueden varias desde la captura de contenido estático, captura en vivo de interacciones, o bien, la extracción de elementos específicos como imágenes, scripts o registros de actividad, con el fin de obtener la mayor cantidad de información relevante posible.

ID TAREA	NOMBRE DE LA TAREA	DESCRIPCIÓN	ARTEFACTOS/FORMATOS/ EVIDENCIAS
1	Instalar o preparar el Software especializado	Instalación de las herramientas de preservación	• FAW - Forensics Acquisition of Websites • HTTrack Website Copier • Otros
2	Realizar las configuraciones del software	Configurar en el software el servidor NTP indicado para que la adquisición quede con la estampa de tiempo correcta.	

ID TAREA	NOMBRE DE LA TAREA	DESCRIPCIÓN	ARTEFACTOS/FORMATOS/ EVIDENCIAS
3	Generar la captura de pantalla completa del sitio web	Tomar una captura completa del sitio web, donde se puede ver con claridad la información que compone toda la página web.	• Capturas de pantalla de Windows • FireShot
4	Generar un vídeo del sitio web	Verificar que el software cuente con la opción de grabar video del sitio web, en caso contrario, elegir la herramienta de preferencia para capturar en forma de vídeo de la evidencia que certifique la existencia del sitio web.	• Barra de Juegos de Windows • Otros
5	Generar un informe de modificaciones y guardar el sitio web	Si es necesario, capturar la página web tal como aparece en el instante de la adquisición para usarla como una cita confiable en el futuro.	https://web.archive.org/
6	Iniciar descarga sitio Web	Descargar sitio web mediante herramienta de preservación	• FAW - Forensics Acquisition of Websites • HTTrack Website Copier • Otros
7	Validar requerimiento	Dependiendo de la solicitud se verifican y documentan los puntos del requerimiento.	
8	Consultar Herramientas web: ● Borderware – Talos intelligence https://talosintelligence.com/ ● Symantec ● RUES ● Ultratools - DomainToools - https://whois.domaintools.com/ ● Virus total ● SSL Checker	● Incluir geolocalización. ● Categoría del sitio web. ● Reputación. ● RUES de la empresa responsable. ● Información del dominio. ● Revisión del virus. ● Revisión de seguridad, verificar certificados	Navegador web
9	Descargar otros elementos vinculados al sitio web	Descargar los documentos, imágenes, capturas de pantalla, vídeos, etc., que se encuentren vinculados al sitio web.	Navegador web
10	Análisis de vulnerabilidades	Verificar el estado en general de las vulnerabilidades de un sitio web	• OWASP ZAP • Nessus
11	Revisión de Cookies	Verificar las cookies usadas por el sitio web	• Cookiebot • Herramientas similares
12	Realizar la Adquisición de las evidencias digitales	Generar imagen forense de la preservación web realizada.	FTK Imager
13	Seleccionar la(s) ruta(s) de origen	Identificar las rutas o carpetas fuentes de la información primaria.	FTK Imager
14	Completar información de la imagen forense	Completar la información para la identificación de la imagen forense y utilizar estándar para nombrar imágenes forenses	FTK Imager

ID TAREA	NOMBRE DE LA TAREA	DESCRIPCIÓN	ARTEFACTOS/FORMATOS/ EVIDENCIAS
15	Seleccionar la ruta destino	Elegir la ubicación en donde se almacenará la imagen forense.	FTK Imager

Tabla 12. Preservación de páginas web.

5.3.6.6 Adquisición de Evidencia Digital de Aplicaciones Móviles

La adquisición adecuada de evidencia digital de aplicaciones móviles requiere un proceso meticuloso que incluye la preparación y configuración de herramientas especializadas, como emuladores y software de preservación forense, para asegurar una captura precisa y detallada de los datos contenidas en las mismas.

ID TAREA	NOMBRE DE LA TAREA	DESCRIPCIÓN	ARTEFACTOS/FORMATOS/ EVIDENCIAS
1	Instalar o preparar el Software especializado	Instalación de las herramientas de preservación	• Genymotion • Celular • Otros
2	Realizar las configuraciones del software	Configurar en el software el servidor NTP indicado para que la adquisición quede con la estampa de tiempo correcta.	Navegador del dispositivo
3	Generar la captura de pantalla completa del sitio web	Tomar una captura completa del sitio web, donde se puede ver con claridad la información que compone toda la página web.	Capturas de pantalla del software de emulación o del teléfono
4	Generar un vídeo del sitio web	Verificar que el software cuente con la opción de grabar video del sitio web, en caso contrario, elegir la herramienta de preferencia para capturar en forma de vídeo de la evidencia que certifique la existencia del sitio web.	• Capturas de pantalla del software de emulación • Otros
5	Iniciar descarga Aplicación móvil	Descargar sitio web mediante herramienta de preservación	Aplicaciones para descargar la APK en Android
6	Validar requerimiento	Dependiendo de la solicitud se verifican y documentan los puntos del requerimiento.	
7	Consultar Herramientas web: ● Virus total ● Mobsf - https://mobsf.live/ ● Exodus - https://reports.exodus-privacy.eu.org/es/	● Revisión del virus. ● Revisión de permisos a los que accede la app.	Navegador web
8	Descargar otros elementos	Descargar los documentos, imágenes, capturas de pantalla, vídeos, etc., que se	Navegador web

ID TAREA	NOMBRE DE LA TAREA	DESCRIPCIÓN	ARTEFACTOS/FORMATOS/ EVIDENCIAS
	vinculados al sitio web	encuentren vinculados al sitio web.	
9	Realizar la Adquisición de las evidencias digitales	Generar imagen forense de la preservación web realizada.	FTK Imager
10	Seleccionar la(s) ruta(s) de origen	Identificar las rutas o carpetas fuentes de la información primaria.	FTK Imager
11	Completar información de la imagen forense	Completar la información para la identificación de la imagen forense y utilizar estándar para nombrar imágenes forenses	FTK Imager
12	Seleccionar la ruta destino	Elegir la ubicación en donde se almacenará la imagen forense.	FTK Imager
13	Generar la imagen forense	Completar la parametrización de la herramienta de acuerdo con los lineamientos del **Laboratorio de Informática Forense** de la **SIC** e iniciar con la creación de la imagen forense.	FTK Imager
14	Verificar la Imagen Forense	Comprobar que la imagen forense haya terminado satisfactoriamente y que los hashes tanto de la adquisición como de la verificación hayan coincidido.	.TXT generado por FTK Imager

Tabla 13. Adquisición de aplicaciones móviles.

5.3.6.7 Adquisición de Evidencia Digital de Requerimientos de Información

Se generará una imagen forense de la información contenida en los dispositivos entregados durante la Visita Administrativa. El experto forense será responsable de seleccionar el tipo de imagen forense más adecuado para cada caso y actuará como custodio temporal si el dispositivo es recolectado, ya que cuenta con el conocimiento y habilidades técnicas para asegurar la información de manera correcta. Al llegar al **Laboratorio de Informática Forense**, la custodia de la evidencia se transferirá formalmente al Laboratorio, que cuenta con las medidas de seguridad necesarias para garantizar que la información mantenga su integridad, originalidad y autenticidad desde el momento de su recolección hasta su disposición final.

ID TAREA	NOMBRE DE LA TAREA	DESCRIPCIÓN	ARTEFACTOS/FORMATOS/ EVIDENCIAS
1	Identificar el dispositivo entregado	Realizar una correcta identificación del dispositivo de evidencia digital que contiene los mensajes de datos solicitados durante el transcurso de la Visita Administrativa y hacer la fijación fotográfica del mismo.	
2	Conectar el dispositivo entregado (Si aplica)	De acuerdo con el tipo de dispositivo entregado, el experto forense debe usar las herramientas necesarias tanto de software como de hardware para evitar que los datos de los dispositivos entregados sufran	• Computador portátil • Bloqueadora de escritura

ID TAREA	NOMBRE DE LA TAREA	DESCRIPCIÓN	ARTEFACTOS/FORMATOS/ EVIDENCIAS
		modificaciones.	
3	Abrir software para la creación de imágenes de datos.	Ejecutar software forense de creación de imágenes.	FTK Imager
4	Seleccionar la(s) ruta(s) de origen	Identificar las rutas o carpetas fuentes de la información primaria.	FTK Imager
5	Completar información de la imagen forense	Completar la información para la identificación de la imagen forense y utilizar estándar para nombrar imágenes forenses	FTK Imager
6	Seleccionar la ruta destino	Elegir la ubicación en donde se almacenará la imagen forense.	FTK Imager
7	Generar la imagen forense	Completar la parametrización de la herramienta de acuerdo con los lineamientos del **Laboratorio de Informática Forense** de la **SIC** e iniciar con la creación de la imagen forense.	FTK Imager
8	Verificar la Imagen Forense	Comprobar que la imagen forense haya terminado satisfactoriamente y que los hashes tanto de la adquisición como de la verificación hayan coincidido.	.TXT generado por FTK Imager
9*	Embalar el dispositivo electrónico	Proceder a embalar el dispositivo electrónico que funciona como contenedor de la evidencia digital entregada por la parte, asegurando que se utilicen materiales adecuados para proteger el dispositivo contra cualquier daño físico durante el transporte.	• Bolsas antiestáticas • Bolsa abullonada • Felpas • Otros

Nota: solo aplica si el dispositivo es recolectado para su transporte al **Laboratorio de Informática Forense.*

Tabla 14. Adquisición de información entregada como requerimiento de información.

5.3.6.8 Adquisición de elementos técnicos y anexos

Se procederá a generar la imagen forense de elementos complementarios que puedan apoyar las actividades técnicas realizadas. Esto incluye información técnica relevante, registros de tareas en ejecución, archivos multimedia como fotografías y videos, y cualquier otro dato que respalde o contextualice la adquisición de evidencia.

ID TAREA	NOMBRE DE LA TAREA	DESCRIPCIÓN	ARTEFACTOS/FORMATOS/ EVIDENCIAS
1	Abrir software para la creación de imágenes de datos.	Ejecutar software forense de creación de imágenes.	FTK Imager
2	Seleccionar la(s) ruta(s) de origen	Identificar las rutas o carpetas fuentes de la información primaria.	FTK Imager
3	Completar información de la imagen forense	Completar la información para la identificación de la imagen forense y utilizar estándar para nombrar imágenes forenses	FTK Imager

ID TAREA	NOMBRE DE LA TAREA	DESCRIPCIÓN	ARTEFACTOS/FORMATOS/ EVIDENCIAS
4	Seleccionar la ruta destino	Elegir la ubicación en donde se almacenará la imagen forense.	FTK Imager
5	Generar la imagen forense	Completar la parametrización de la herramienta de acuerdo con los lineamientos del **Laboratorio de Informática Forense** de la **SIC** e iniciar con la creación de la imagen forense.	FTK Imager
6	Verificar la Imagen Forense	Comprobar que la imagen forense haya terminado satisfactoriamente y que los hashes tanto de la adquisición como de la verificación hayan coincidido.	.TXT generado por FTK Imager

Tabla 15. Adquisición de Anexos

5.3.6.9 Documentar y diligenciar Acta de Visita, Formatos de Adquisición, Rótulos y Cadenas de Custodia

En cada proceso de adquisición de evidencia digital, será imprescindible completar y diligenciar la documentación correspondiente, cumpliendo con los estándares nacionales e internacionales para la identificación, recolección, adquisición y preservación de la evidencia digital, lo cual asegura un manejo riguroso, transparente y confiable de los elementos adquiridos o recolectados, preservando su integridad y garantizando su validez en todas las etapas del proceso forense.

ID TAREA	NOMBRE DE LA TAREA	DESCRIPCIÓN	ARTEFACTOS/FORMATOS/ EVIDENCIAS
1	Documentar Acta de visita	Registrar el resultado de cada actividad en el acta de la visita realizada durante la diligencia.	Acta de Visita
2	Diligenciar *GS04-F02 Formato de Adquisición de Imágenes Forenses*	Diligenciar el formato *GS04-F02 Formato de Adquisición de Imágenes Forenses* por cada adquisición de evidencia digital, exceptuando declaraciones e inspecciones oculares.	*GS04-F02 Formato de Adquisición de Imágenes Forenses*
3	Abrir *GS04-F01 Registro Cadena de Custodia*	Diligenciar el *GS04-F01 Registro Cadena de Custodia* para cada dispositivo de almacenamiento (contenedor de evidencia digital) y cada requerimiento de información.	*GS04-F01 Registro Cadena de Custodia*
4	Diligenciar rótulo	Diligenciar el rótulo de evidencia para los dispositivos de almacenamiento recolectados en visita y que generalmente, están asociados a los requerimientos de información.	Formato Rótulo de evidencia física

Tabla 16. Soportes de adquisición.

5.3.7 TRANSPORTE EL DISPOSITIVO CONTENEDORES DE EVIDENCIA DIGITAL

Los funcionarios y/o contratistas se comprometerán a trasladar a las instalaciones de la **SIC** el dispositivo de almacenamiento que contiene todos los mensajes de

datos recolectados durante la Visita de Inspección, asegurando en todo momento su integridad y evitando cualquier daño o alteración de la evidencia que pueda afectar la validez de la evidencia en un proceso judicial o investigativo.

El funcionario y/o contratista identificado como primer responsable deberá entregar las evidencias digitales recolectadas a más tardar al día siguiente de finalizada la visita, en casos en que la actividad concluya fuera del horario laboral de la entidad.

Cabe destacar que, en caso de pérdida durante el traslado de la evidencia digital, tanto los equipos de cómputo como los discos duros utilizados por el funcionario y/o contratista del **GTIFSD** están cifrados, lo cual garantiza la protección de la información durante el transporte y resguarda la confidencialidad de la evidencia hasta su entrega final.

5.3.8 ENTREGA DE LA VISITA, LISTADO DE IMÁGENES Y CONTROL DE EVIDENCIAS

En esta etapa, se realizará la entrega formal de las evidencias recolectadas durante la visita de inspección, asegurando que todas las imágenes forenses y demás elementos estén debidamente documentados para que sean entregados al responsable de la siguiente actividad. Esto facilita el rastreo y manejo adecuado de las evidencias digital en etapas posteriores del proceso forense.

ID TAREA	NOMBRE DE LA TAREA	DESCRIPCIÓN	ARTEFACTOS/FORMATOS/ EVIDENCIAS
1	Diligenciar Excel de control de evidencias	Diligenciar Excel para notificar el inventario de evidencias adquiridas durante la visita puesto a disposición.	Excel de control de evidencias
2	Preparar formatos de adquisición, rótulos y *GS04-F01 Registro Cadena de Custodia*	Organizar la documentación generada en la visita en el orden de adquisición de los hallazgos.	• *GS04-F02 Formato de Adquisición de Imágenes Forenses* • *GS04-F01 Registro Cadena de Custodia*
3	Entrega de documentos y contenedores de evidencia digital	Entregar al servidor público o contratista designado para recibir las visitas la documentación obtenida durante la visita y el (los) contenedor(es) de evidencia digital	

Tabla 17. Entrega de Visita.

5.3.9 GESTIÓN DE UNIFICACIONES

La unificación de información tiene como objetivo principal agrupar los datos relacionados con un mismo caso en un único contenedor, esto no solo para optimizar el espacio de almacenamiento, sino para facilitar un mejor control de la

información, al centralizarla en un solo dispositivo o en varios dependiendo del tamaño de la información.

Para iniciar la gestión de la unificación, es fundamental que se haya completado la entrega y revisión de cada visita de inspección realizada por los expertos forenses, ya que, con los datos obtenidos, como el peso de la información, se podrá determinar el tipo de dispositivo de almacenamiento adecuado y su capacidad máxima; tras dicha revisión, el Coordinador del **GTIFSD** asignará las tareas de unificación a los funcionarios y/o contratistas disponibles para llevar a cabo la labor.

5.3.9.1 Gestionar las Unificaciones

Como se ha planteado anteriormente, es necesario realizar las siguientes tareas para esta actividad:

ID TAREA	NOMBRE DE LA TAREA	DESCRIPCIÓN	ARTEFACTOS/FORMATOS/ EVIDENCIAS
1	Asignar servidor público y/o contratista.	Valorar el impacto de la atención del requerimiento con base en la información de la solicitud de servicio. Identificar la disponibilidad de los recursos y las horas de dedicación necesarias para la atención del requerimiento, asegurándose de que los recursos asignados sean adecuados para la magnitud del requerimiento.	Correo electrónico con informe de asignación
2	Verificar documentación y contenedor (es) origen	Verificar que el espacio utilizado en el *GS04-F01 Registro Cadena de Custodia* corresponda al tamaño de la información almacenada en el contenedor de evidencia digital. Verificar el adecuado diligenciamiento de la documentación adjunta al contenedor de evidencia digital. Si lo considera necesario, se deberá realizar sesiones de entendimiento con el funcionario y/o contratista encargado de la Visita.	• *GS04-F01 Registro Cadena de Custodia*. • Rótulo • *GS04-F02 Formato de Adquisición de Imágenes Forenses*.
3	Realizar la unificación en cascada	La unificación en cascada consiste en almacenar la información recolectada de cada empresa visitada bajo un mismo radicado, en un solo contenedor de evidencia digital, para cada una de las empresas, utilizado dentro de la misma. Para realizar la unificación en cascada, es necesario verificar el tamaño de los dispositivos utilizados por cada empresa hasta identificar el que posea mayor tamaño utilizado, lo anterior con el fin de seleccionarlo como el contenedor temporal de destino, el cual albergará la información recolectada. Es indispensable asegurarse de que los datos se hayan transferido correctamente a este	• *GS04-F01 Registro Cadena de Custodia* Origen y Destino. • TreeSize (o similares). • Software LIF. • Informes de Copia • Informes Técnicos de copia. • Software de copia (FastCopy, TeraCopy o similares)

ID TAREA	NOMBRE DE LA TAREA	DESCRIPCIÓN	ARTEFACTOS/FORMATOS/ EVIDENCIAS
		contenedor. Al finalizar esta actividad, toda la información de la visita de inspección administrativa debe encontrarse en el contenedor de destino, para más detalle ver **Realizar Unificación en Cascada**	
4	Copiar información en contenedor	Seleccionar un dispositivo contenedor final de evidencias digitales de acuerdo al estándar propuesto en la sección **Copia de Contenedores de Evidencias Digitales.** Copiar la información del contenedor temporal de destino al contenedor final de evidencias digitales. Asegurarse de que los datos sean copiados correctamente sin alteración alguna. Realizar la documentación técnica de la actividad. Para más detalle ver **Copia de Contenedores de Evidencias Digitales.**	• *GS04-F01 Registro Cadena de Custodia* Origen y Destino. • Software LIF. • TreeSize • Informes de Copia. • Informes Técnicos.
5	Cerrar *GS04-F01 Registro Cadena de Custodia* Origen	Una vez realizadas las actividades de **Borrado Seguro**, es necesario que el encargado de la unificación finalice el *GS04-F01 Registro Cadena de Custodia* de los contenedores Origen. Este cierre certifica que el encargado del método de unificación ha sido el último custodio de la información almacenada en el contenedor de evidencia digital. La finalización del registro debe ser validada por el responsable de la actividad.	*GS04-F01 Registro Cadena de Custodia* Origen
6	Generar registro(s) de la actividad	Realizar la documentación detallada de la forma en la que técnicamente se soportará el proceso de unificación, especificando todos los pasos y herramientas utilizadas en el proceso.	*GS04-F06 Acta de Unificación de Evidencias Digitales*
7	Aprobar registro(s) de la actividad	Validar las actividades realizadas y la documentación técnica, asegurándose de que todo esté conforme con los requisitos establecidos en el procedimiento de unificación.	
8	Firmar registro de unificación	Formalizar la aceptación de la actividad de Unificación.	
9	Archivar información	Clasificar y almacenar la información en archivo físico y/o digital. Determinar si el contenedor se anexa al expediente o si se almacena en el cuarto de evidencias.	

ID TAREA	NOMBRE DE LA TAREA	DESCRIPCIÓN	ARTEFACTOS/FORMATOS/ EVIDENCIAS
		Los contenedores que se almacenan en el expediente pueden ser medios ópticos como CD, DVD, BLU-RAY, mientras que los contenedores que se almacenan en el cuarto de evidencias incluyen discos duros y memorias USB.	
10	Verificar el tipo de contenedor	Considerar la criticidad del tipo de contenedor y las evidencias digitales almacenadas para decidir si debe ser entregado a la dependencia solicitante o si debe ser almacenado en el cuarto de evidencias.	
11	Entregar contenedor y documentación para expediente	Entregar al líder del caso o al encargado por parte de la dependencia solicitante, los contenedores (para el caso en que estos sean medios ópticos) y la documentación correspondiente.	
12	Almacenar contenedor en cuarto de evidencias y entregar documentación	Entregar al encargado del cuarto de evidencias el(los) contenedores(es) de evidencia digital.	
13	Almacenar hoja de recibido para archivo	El documento generado con firma de recibido a cabalidad debe ser entregado al encargado de administrar las Tablas de Retención Documental de **GTIFSD**.	

Tabla 18. Flujo para gestionar las unificaciones.

5.4 PROCESAMIENTO

5.4.1 COPIA EN LOS SERVIDORES

En esta tarea, se realizará una copia exacta de la información desde los contenedores de evidencia digital de destino a los servidores de almacenamiento del **GTIFSD**, ya que, conforme con lo establecido por la comunidad técnico-científica, es necesario contar con al menos dos copias de la evidencia digital y garantizar que no se trabaje directamente sobre la evidencia original, para preservar su integridad.

Durante la actividad de copia de los mensajes de datos a los servidores de almacenamiento, los funcionarios y/o contratistas del **GTIFSD** deberán tener en cuenta las siguientes consideraciones.

ID TAREA	NOMBRE DE LA TAREA	DESCRIPCIÓN	ARTEFACTOS/FORMATOS/ EVIDENCIAS
1	Utilizar una herramienta informática que	Utilizar una herramienta informática que genere un registro de:	• FastCopy • Teracopy • Herramientas similares

ID TAREA	NOMBRE DE LA TAREA	DESCRIPCIÓN	ARTEFACTOS/FORMATOS/ EVIDENCIAS
	genere un registro o log de la copia	• Ruta de origen (información del dispositivo de origen de donde provienen los mensajes de datos). • Ruta de destino (información del dispositivo de destino en donde se conservará la información). • Contenido del disco de origen (Peso, número de carpetas, entre otros). • Fecha y hora en que se iniciada y se terminada la copia de la información.	
2	Verificar si existe la carpeta del caso	Verificar si existe la carpeta del caso, de ser así la información debe ser copiada dentro de ella.	
3	Crear carpeta del caso	Si no existe la carpeta es necesario crear una carpeta con el Radicado y nombre del caso.	

Tabla 19. Flujo de copia en los servidores.

5.4.2 CREACIÓN DE LA LISTA DE PROCESAMIENTO

Una vez que la información recolectada sea almacenada en los servidores de almacenamiento administrados por el **GTIFSD**, los funcionarios y/o contratistas deberán crear, como buena práctica de procesamiento, una lista detallada con la información de las evidencias que deberán ser procesadas. De esta manera, se podrá conocer la cantidad y el tamaño de las evidencias que deberán ser procesadas una vez llegue la solicitud de la Dependencia o Delegatura dueña de la información.

La información que debe contener la lista de procesamiento es la siguiente:

- Entidad o empresa de donde fue tomada la evidencia
- Nombre de la imagen forense
- Ubicación y nombre del caso en donde se encuentra la evidencia
- Tipo de evidencia
- Tamaño de la evidencia

5.4.3 PROCESAMIENTO DE EVIDENCIAS DIGITALES

El procesamiento incluye el traspaso de la información recolectada en los dispositivos de destino que harán parte del expediente o soporte documental que se lleve del caso, además, se llevan a cabo tareas como la recuperación de archivos dañados o eliminados, expansión de archivos compuestos, conversión de formatos, indexación de datos y extracción de texto de imágenes mediante reconocimiento de caracteres, entre otras.

El nivel de procesamiento depende de las necesidades del caso, variando según la cantidad y naturaleza de los datos, lo que afecta la duración del proceso. Por ello, el procesamiento se clasifica en tres tipos:

i. Procesamiento corto: Incluye solo la extracción de mensajes de datos de las muestras, mediante herramientas de software que identifican archivos digitales sin realizar acciones de recuperación.

ii. Procesamiento completo. Aparte de la extracción de mensajes de datos, incluye acciones como la recuperación de datos borrados o perdidos, recuperación de archivos, OCR, expansión de archivos compuestos, y la organización o indexación de los datos adquiridos.

iii. Procesamiento alterno. Similar al procesamiento completo, pero utilizando otras herramientas de software, con el fin de personalizar y agilizar el proceso según las necesidades específicas del negocio.

Para llevar a cabo el procesamiento de los mensajes de datos, es necesario utilizar software especializado. En el caso de la **SIC**, se dispone de herramientas licenciadas para este proceso.

5.4.4 PUESTA A DISPOSICIÓN

Una vez procesados, los datos se ponen a disposición mediante herramientas especializadas que garantizan su integridad al permitir su visualización sin riesgo de alteración. Además, las herramientas utilizadas en esta fase deben son intuitivas, ya que no siempre son operadas por expertos forenses.

En el caso de la **SIC**, la puesta a disposición de los datos procesados permite que los expertos en la materia puedan analizarlos y revisarlos dentro de la etapa de investigativa. Por ellos, el **Laboratorio de Informática Forense** dispone de software especializado y licenciado para facilitar la visualización de los datos procesados, así como, permitir la consulta y análisis exclusivo por personal autorizado dentro de la Entidad:

Clase de software	Nombre	Descripción
Plataforma Web	FTK Central	Consulta para análisis de mensajes de datos adquiridos de dispositivos ópticos, magnéticos y electrónicos, excluyendo dispositivos móviles y computadores con sistema operativo MacOS.
Plataforma Web	Cellebrite Pathfinder Enterprise	Consulta para análisis de mensajes de datos adquiridos de dispositivos móviles y computadores con sistema operativo MacOS
Aplicación	FTK Lab	Procesamiento y consulta para análisis de mensajes de datos adquiridos de dispositivos ópticos, magnéticos y

Clase de software	Nombre	Descripción
		electrónicos, excluyendo dispositivos móviles.
Aplicación	FTK Imager	Consulta para análisis de mensajes de datos adquiridos de dispositivos ópticos, magnéticos y electrónicos, excluyendo dispositivos móviles y computadores con sistema operativo MacOS.
Aplicación	Cellebrite Physical Analyzer Cellebrite Inseyets	Procesamiento y consulta para análisis de mensajes de datos adquiridos de dispositivos móviles
Aplicación	Cellebrite Reader	Consulta para análisis de mensajes de datos adquiridos de dispositivos móviles

Tabla 20. Descripción Herramientas Forenses.

5.4.5 GESTIÓN DE ACCESO A EVIDENCIAS EN PLATAFORMA DE INVESTIGACIÓN

La gestión de acceso a las evidencias digitales en la plataforma de investigación tendrá como objetivo garantizar un control riguroso de los usuarios y grupos con permisos asignados, asegurando la integridad, trazabilidad y registro detallado de todas las consultas realizadas sobre las evidencias.

Las solicitudes de acceso serán canalizadas exclusivamente a través de los coordinadores, delegados, jefes de las áreas y/o Delegaturas responsables de la información. Dichas solicitudes deberán especificar claramente el caso de interés y los niveles de acceso requeridos, permitiendo así un control preciso y seguro a la información.

El administrador de la plataforma tendrá la responsabilidad de gestionar la creación de usuarios y la asignación de permisos sobre los casos que contengan evidencias digitales, además, realizará la depuración periódica de usuarios que ya no estén activos en la entidad, ya sea por desvinculación, vacaciones, licencias u otras razones.

ID TAREA	NOMBRE DE LA TAREA	DESCRIPCIÓN	ARTEFACTOS/FORMATOS / EVIDENCIAS
1	Recepción de la solicitud para creación y/o permisos de usuario	Recibir y registrar la solicitud de creación o asignación de permisos por parte de coordinadores, delegados y/o jefes de área.	Correo electrónico de la solicitud
2	Verificación de autorización	Validar que la solicitud cuenta con la autorización formal de los coordinadores, delegados y/o jefes de área responsables.	
3	Creación y/o asignación de permisos	Crear y/o asignar los permisos correspondientes en la plataforma de investigación, asegurando su correcta configuración.	Evento de creación y/o asignación de permisos

ID TAREA	NOMBRE DE LA TAREA	DESCRIPCIÓN	ARTEFACTOS/FORMATOS / EVIDENCIAS
4	Confirmación al solicitante	Informar al solicitante sobre la finalización de la creación o asignación de los permisos solicitados en la plataforma de forense respectiva.	Correo Electrónico
5	Solicitud de actualización de usuarios	Solicitar a los coordinadores el listado actualizado de funcionarios y contratistas activos para depuración de usuarios.	Correo Electrónico
6	Depuración de usuarios	Realizar la eliminación o derogación de permisos a los usuarios inactivos, según el listado actualizado recibido.	Registro de eliminación / derogación.

Tabla 21. Flujo de Gestión de Acceso en Plataforma de Investigación.

5.5 INVESTIGACIÓN

5.5.1 GESTIONAR LAS INVESTIGACIONES

La gestión de las investigaciones consiste en coordinar y ejecutar las actividades necesarias para analizar y contextualizar los mensajes de datos puestos a disposición, con el objetivo de identificar hallazgos relevantes para el caso. Dichas actividades abarcan desde la selección y análisis de la información, hasta la reconstrucción de hechos y generación de hipótesis, contribuyendo así a la formulación de conclusiones precisas sobre la conducta investigada.

ID TAREA	NOMBRE DE LA TAREA	DESCRIPCIÓN
1	Pre - investigación	Evaluar las interacciones entre los actores involucrados en el caso para identificar relaciones y posibles líneas de investigación.
2	Selección por niveles de relevancia	Identificar y clasificar la información según su importancia y relación directa con los objetivos de la investigación.
3	Selección de técnicas de búsqueda	Determinar las técnicas de búsqueda más adecuadas para optimizar el análisis y facilitar los hallazgos.
4	Selección de mensajes de datos finales	Identificar los mensajes de datos clave que presentan patrones relevantes para convertirse en hallazgos.
5	Revisión del caso	Analizar los antecedentes del caso para identificar posibles actores o contextos relevantes.
6	Identificación de personas de interés	Registrar personas naturales o jurídicas que surgen como agentes clave para la reconstrucción de los hechos..
7	Creación de etiquetas y filtrado de información	Organizar y clasificar los agentes, factores y datos relevantes mediante etiquetas que permitan una segregación y análisis más eficiente.
8	Creación de la lista de investigación	Elaborar un documento que relacione los actores participantes y su vínculo directo o indirecto con los hechos investigados.

ID TAREA	NOMBRE DE LA TAREA	DESCRIPCIÓN
9	Refuerzo de búsquedas	Realizar búsquedas adicionales para identificar posibles terceros o parámetros relevantes que incidan en la investigación.
10	Línea de tiempo	Desarrollar una cronología detallada de los eventos, incidentes y hechos investigados para facilitar la reconstrucción del caso.
11	Revisión y ajuste de etiquetas	Depurar y actualizar las etiquetas creadas previamente en la plataforma investigativa, identificando nuevos parámetros o agentes relevantes.
12	Exportación de la evidencias y creación de imágenes derivada	Extraer los elementos clave de las imágenes forenses recolectadas para identificar conductas contrarias al marco legal colombiano y asegurarlas mediante la creación de imágenes forenses.

Tabla 22. Flujo de Gestionar las Investigaciones.

5.6 ATENDER SOLICITUDES COMPLEMENTARIAS

5.6.1 SOLICITUDES COMPLEMENTARIAS

5.6.1.1 Copia de Contenedores de Evidencias Digitales

El procedimiento para realizar copias de contenedores de evidencias digitales tiene como objetivo preservar la integridad de las pruebas digitales y garantizar la seguridad de la información para que pueda ser utilizada como evidencia en investigaciones legales y judiciales. Dentro del proceso de copia se contemplan una serie de tareas que aseguran que las evidencias sean copiadas de manera segura siguiendo los protocolos establecidos en la normativa nacional e internacional.

ID TAREA	NOMBRE DE LA TAREA	DESCRIPCIÓN	ARTEFACTOS/FORMATOS/ EVIDENCIAS
1	Análisis del contenedor de origen	Ejecutar software especializado para obtener información técnica del dispositivo que contiene la evidencia digital, como tamaño de carpetas, cantidad de archivos y otros datos relevantes.	TreeSize (o herramientas similares)
2	Identificación de información del contenedor de origen	Registrar detalles técnicos como el tamaño de carpetas y subcarpetas, cantidad de archivos, y los seriales lógico y físico del dispositivo.	• TreeSize (o herramientas similares) • Símbolo del sistema o CMD
3	Selección del dispositivo de destino	Gestionar y seleccionar un dispositivo de destino con capacidad suficiente para almacenar la evidencia digital según su tamaño. Para más detalle ver **Selección de Contenedor de Destino**	

ID TAREA	NOMBRE DE LA TAREA	DESCRIPCIÓN	ARTEFACTOS/FORMATOS/ EVIDENCIAS
4	Configuración y ejecución del software LIF	Configurar y ejecutar el software LIF para la copia de los datos. Ajustar la herramienta según que el procedimiento que se desea realizar.	Software LIF
5	Revisar *GS04-F05 Formato de Informe de Copia* generado por el software LIF	Validar que los registros generados por la herramienta no presenten errores.	• Software LIF • *GS04-F05 Formato de Informe de Copia*
6	Ajustes por errores en la copia	En caso de errores, ajustar las configuraciones del software de copia y repetir el proceso. Verificar nuevamente que no existan inconsistencias en los registros generados.	• Software LIF • FastCopy, Teracopy o Herramientas similares
7	Análisis del contenedor de destino	Ejecutar el software que permita obtener información técnica del dispositivo contenedor de evidencia digital	TreeSize (o herramientas similares)
8	Diligenciamiento del rótulo del contenedor	Imprimir y diligenciar el rótulo correspondiente con la información del dispositivo de destino.	*GS04-F03*
9	Diligenciamiento *GS04-F01 Registro Cadena de Custodia* contenedor destino	Imprimir y diligenciar formato de *GS04-F01 Registro Cadena de Custodia* con la información del contenedor destino	*GS04-F01 Registro Cadena de Custodia*
10	Creación de anexo digital	Almacenar la información técnica en un dispositivo óptico sin escritura o en el dispositivo que donde se impida su escritura. Para más detalle ver **Anexo Digital Copia**	
11	Registro de ubicación de contenedores fuera de expediente	Diligenciar el *GS04-F04 Formato Testigo Documental de Contenedor de Evidencia Digital* que especifica la ubicación física de contenedores de evidencia digital almacenados fuera del expediente, como discos duros o memorias USB.	*GS04-F04 Formato testigo documental de contenedor de evidencia digital ubicado fuera de expediente*
12	Elaboración de acta	Documentar en un acta los pasos, herramientas y métodos utilizados en el proceso de copia, asegurando trazabilidad y cumplimiento la normativa.	*GS04-F07 Acta de Copia de Contenedores de Evidencia Digital*

Tabla 23. Flujo de Copiar información en contenedores.

5.6.1.2 Informe Técnico

El Informe Técnico es un documento que detalla la información técnica de las actividades forenses realizadas en el **Laboratorio de Informática Forense** y tiene como propósito principal es registrar, de manera clara y precisa, los procedimientos aplicados, asegurando que se mantenga la integridad de los datos y que las actividades cumplan con los estándares forenses aplicables. Es decir

que, los informes técnicos son clave para respaldar la validez y confiabilidad de los resultados obtenidos, especialmente en contextos legales o administrativos donde la evidencia digital debe ser presentada como prueba.

ID TAREA	NOMBRE DE LA TAREA	DESCRIPCIÓN	ARTEFACTOS/FORMATOS / EVIDENCIAS
1	Análisis del contenedor de origen	Ejecutar un software especializado para obtener información técnica detallada del dispositivo contenedor de evidencia digital, como estructura de carpetas, tamaño y número de archivos.	TreeSize (o herramientas similares)
2	Identificación de información del contenedor de origen	Registrar detalles técnicos como el tamaño de carpetas y subcarpetas, cantidad de archivos, y los seriales lógico y físico del dispositivo.	• TreeSize (o herramientas similares) • Símbolo del sistema o CMD
3	Elaboración de acta	Documentar los pasos realizados, las herramientas utilizadas y los métodos aplicados durante la actividad en un acta oficial que respalde el análisis técnico realizado..	*GS04-F09 Acta de Informe Técnico*

Tabla 24. Flujo de Informe Técnico.

5.6.1.3 Traslado de Contenedores de Evidencias Digitales

El traslado de contenedores de evidencias digitales es el procedimiento mediante el cual se transfiere evidencia de un dispositivo de almacenamiento a otro, ya sea por razones como daños físicos en el dispositivo original, necesidad de minimizar riesgos de pérdida o alteración de datos, o para facilitar el análisis en un entorno controlado.

Además, este procedimiento implica la validación técnica y física tanto del contenedor origen como del destino, la generación de registros detallados, y la documentación de cada paso a través de herramientas y formatos especializados que se basan en estrictos estándares forenses para preservar la autenticidad de los datos y su aceptación como pruebas en procedimientos legales o administrativos.

ID TAREA	NOMBRE DE LA TAREA	DESCRIPCIÓN	ARTEFACTOS/FORMATOS/ EVIDENCIAS
1	Análisis del contenedor de origen	Ejecutar software especializado para obtener información técnica del dispositivo que contiene la evidencia digital, como tamaño de carpetas, cantidad de archivos y otros datos relevantes.	TreeSize (o herramientas similares)
2	Identificación de información del contenedor de origen	Registrar detalles técnicos como el tamaño de carpetas y subcarpetas, cantidad de archivos, y los seriales lógico y físico del dispositivo.	• TreeSize (o herramientas similares) • Símbolo del sistema o CMD

ID TAREA	NOMBRE DE LA TAREA	DESCRIPCIÓN	ARTEFACTOS/FORMATOS/ EVIDENCIAS
3	Selección del dispositivo de destino	Gestionar y seleccionar un dispositivo de destino con capacidad suficiente para almacenar la evidencia digital según su tamaño. Para más detalle ver **Selección de Contenedor de Destino**	
4	Configuración y ejecución del software LIF	Configurar y ejecutar el software LIF para la copia de los datos. Ajustar la herramienta según que el procedimiento que se desea realizar.	Software LIF
5	Revisar *GS04-F05 Formato de Informe de Copia* generado por el software LIF	Validar que los registros generados por la herramienta no presenten errores.	• Software LIF • *GS04-F05 Formato de Informe de Copia*
6	Ajustes por errores en la copia	En caso de errores, ajustar las configuraciones del software de copia y repetir el proceso. Verificar nuevamente que no existan inconsistencias en los registros generados.	• Software LIF • FastCopy, Teracopy o Herramientas similares
7	Análisis del contenedor de destino	Ejecutar el software que permita obtener información técnica del dispositivo contenedor de evidencia digital	TreeSize (o herramientas similares)
8	Diligenciamiento del rótulo del contenedor	Imprimir y diligenciar el rótulo correspondiente con la información del dispositivo de destino.	*GS04-F03*
9	Diligenciamiento *GS04-F01 Registro Cadena de Custodia* contenedor destino	Imprimir y diligenciar formato de *GS04-F01 Registro Cadena de Custodia* con la información del contenedor destino	*GS04-F01 Registro Cadena de Custodia*
10	Creación de anexo digital	Almacenar la información técnica en un dispositivo óptico sin escritura. Para más detalle ver **Anexo Digital Copia**	
11	Registro de ubicación de contenedores fuera de expediente	Diligenciar el *GS04-F04 Formato Testigo Documental de Contenedor de Evidencia Digital* que especifica la ubicación física de contenedores de evidencia digital almacenados fuera del expediente, como discos duros o memorias USB.	*GS04-F04 Formato testigo documental de contenedor de evidencia digital ubicado fuera de expediente*
12	Elaboración de acta	Documentar en un acta los pasos, herramientas y métodos utilizados en el proceso de copia, asegurando trazabilidad y cumplimiento la normativa.	*GS04-F10 Acta de Traslado de Contenedores de Evidencia Digital*

Tabla 25. Flujo del traslado de contenedores de evidencias digitales.

5.6.1.4 Depuración de Mensajes de Datos.

La depuración de mensajes de datos en el contexto de la informática forense es un procedimiento esencial para garantizar la protección de información personal o privada, mientras se preserva la integridad y validez probatoria de la evidencia digital, mediante la aplicación de protocolos estrictos que aseguran la confidencialidad y trazabilidad de la información recolectad. Siempre en búsqueda de la protección de los derechos de los titulares de la información y la fiabilidad de las pruebas en el ámbito judicial.

ID TAREA	NOMBRE DE LA TAREA	DESCRIPCIÓN	ARTEFACTOS/FORMATOS/ EVIDENCIAS
1	Recibir requerimiento y asignar el experto forense encargado	La dependencia o área remitente envía la autorización para atender el requerimiento de depuración de la información.	Respuesta confirmando la atención de la solicitud.
2	Verificar documentación y contenedor	Validar la información del caso, incluyendo nombre, número de radicado, y tipo de contenedor asociado.	
3	Verificar tabla de relación de discos duros	Consultar la ubicación del contenedor en el documento de relación de dispositivos almacenados en el cuarto de evidencias.	Tabla de relación de discos duros
CASO 1			
4a	Retirar dispositivo y solicitar *GS04-F01 Registro Cadena de Custodia* correspondiente	Si el contenedor se encuentra almacenado en el cuarto de evidencias, retirarlo y solicitar el formato *GS04-F01 Registro Cadena de Custodia* correspondiente	
5a	Entrega *GS04-F01 Registro Cadena de Custodia*	La dependencia encargada entrega el *GS04-F01 Registro Cadena de Custodia*	*GS04-F01 Registro Cadena de Custodia*
6a	Diligenciar el *GS04-F01 Registro Cadena de Custodia*	Realizar anotación en *GS04-F01 Registro Cadena de Custodia*	*GS04-F01 Registro Cadena de Custodia*
CASO 2			
4b	Solicitar revisión del expediente	En caso de que el contenedor no esté en el cuarto de evidencias, solicitar a la dependencia responsable la revisión del expediente del caso para localizarlo.	Expediente del caso
5b	Entregar contenedor alojado en el expediente	La dependencia entrega el dispositivo contenedor de evidencia digital junto con su respectivo *GS04-F01 Registro Cadena de Custodia* y se confirmar la recepción del contenedor de evidencia digital en caso de ser retirado del expediente	• Expediente • Medio contenedor de evidencia digital

ID TAREA	NOMBRE DE LA TAREA	DESCRIPCIÓN	ARTEFACTOS/FORMATOS/ EVIDENCIAS
6b	Diligenciar el *GS04-F01 Registro Cadena de Custodia*	Realizar anotación en *GS04-F01 Registro Cadena de Custodia*	*GS04-F01 Registro Cadena de Custodia*
7	Identificar información en herramienta forense	Revisar la información en el contenedor utilizando herramientas forenses, identificando los ítems a depurar según la solicitud.	• FTK LAB • FTK Central
8	Generar etiqueta o filtros con la información requerida	Crear etiquetas o filtros que clasifiquen y detallen los ítems seleccionados para depuración.	• FTK LAB • FTK Central
9	Revisión de la información a depurar	Una vez los ítems se encuentren almacenados en la(s) etiqueta(s) o filtros se debe solicitar la revisión de la dependencia solicitante para avalar el borrado.	Correo electrónico
10	Borrado de la información contenida en las etiquetas o filtros	Borrar la información que fue objeto de la solicitud de depuración	• FTK LAB • FTK Central
11	Generar imagen derivada en dispositivo forense	Crear una imagen derivada de la información requerida utilizando herramientas forenses	• FTK LAB • FTK Central • FTK Imager
15	Ejecutar borrado seguro	Realizar un borrado seguro del contenedor origen utilizando software especializado. Para más detalle ver **Borrado Seguro**	• EnCase • Eraser • Herramientas similares
16	Diligenciar el *GS04-F01 Registro Cadena de Custodia* del contenedor origen	Actualizar la *GS04-F01 Registro Cadena de Custodia* del contenedor origen con la información de la actividad efectuada	
17	Copiar imagen derivada en contenedor origen	Almacenar la imagen derivada en el contenedor origen de acuerdo con el procedimiento establecido.	
18	Diligenciar *GS04-F01 Registro Cadena de Custodia* del contenedor origen	Actualizar el *GS04-F01 Registro Cadena de Custodia* del contenedor origen con información relacionada con el almacenamiento de la imagen derivada.	*GS04-F01 Registro Cadena de Custodia*
19	Elaboración de acta	Documentar en el acta todos los pasos realizados, herramientas empleadas y métodos aplicados durante el proceso de depuración.	*GS04-F11 Acta de Depuración de Mensajes de Datos.*

Tabla 26. Flujo de Depuración de Mensajes de Datos.

5.6.1.5 Exportación de Elementos de Evidencia Digital

El proceso de exportación de elementos de evidencia digital consiste en extraer mensajes de datos clave desde las herramientas forenses para responder a un procedimiento administrativo en curso, lo cual incluye la generación de una nueva imagen forense denominada *imagen derivada*, que garantiza la integridad y validez probatoria de la información, tal y como fue recolectada originalmente. La exportación es realizada mediante herramientas especializadas, que permiten etiquetar, filtrar y exportar los datos, cumpliendo con los estándares forenses establecidos que permiten documentar cada etapa del proceso en formatos específicos y al final se elaborar un acta que respalda todas las actividades realizadas.

ID TAREA	NOMBRE DE LA TAREA	DESCRIPCIÓN	ARTEFACTOS/FORMATOS/ EVIDENCIAS
1	Recibir requerimiento y asignar analista encargado	Recepción de la solicitud autorizada por el área o dependencia correspondiente y asignación de un analista para atender el requerimiento.	Respuesta indicando la atención de la solicitud.
2	Verificar documentación y contenedor final	Validar la información del caso, incluyendo nombre, radicado y tipo de contenedor de evidencia donde se almacenará la imagen derivada	
3	Identificar información en herramienta forense	Identificar los elementos relevantes procesados previamente en la herramienta forense que deben ser exportados, aplicando filtros y etiquetas según lo requerido.	• FTK LAB • FTK Central • Pathfinder Enterprise
4	Generar etiqueta con la información requerida	Crear etiquetas para los elementos seleccionados, ajustándose al tipo de solicitud y asegurando su correcta organización para la exportación.	• FTK LAB • FTK Central • Pathfinder Enterprise
5	Exportar y generar imagen derivada	Realizar la exportación de los elementos de evidencia digital seleccionados y generar una nueva imagen forense derivada en un contenedor de evidencia.	• FTK LAB • FTK Central • Pathfinder Enterprise
6	Diligenciar *GS04-F01 Registro Cadena de Custodia* del contenedor origen	Actualizar la *GS04-F01 Registro Cadena de Custodia* del contenedor origen, documentando las actividades realizadas en el proceso.	*GS04-F01 Registro Cadena de Custodia*
7	Realizar apertura de *GS04-F01 Registro Cadena de Custodia*	Iniciar un nuevo registro de cadena de custodia para el contenedor destino donde se almacenará la imagen derivada según lo solicitado.	*GS04-F01 Registro Cadena de Custodia*
8	Diligenciar Rótulo	completar el formato de rótulo con la información correspondiente al contenedor destino de evidencia digital.	*GS04-F03*

ID TAREA	NOMBRE DE LA TAREA	DESCRIPCIÓN	ARTEFACTOS/FORMATOS/ EVIDENCIAS
9	Elaborar acta	Documentar los pasos, herramientas y métodos utilizados durante el procedimiento en el acta de exportación de elementos de evidencia digital.	*GS04-F12 Acta de Exportación de Elementos de Evidencias Digitales*

Tabla 27. Flujo de Exportación de Elementos de Evidencia Digital.

5.6.1.6 Realizar Unificación en Cascada

El procedimiento de unificación en cascada consiste en consolidar información de múltiples contenedores de evidencia digital en un único contenedor final, optimizando los recursos de almacenamiento, asegurando la integridad de los datos y facilitando su posterior acceso. Asimismo, la unificación en cascada es fundamental para garantizar una gestión eficiente de la evidencia digital, evitando duplicidades y pérdidas de información.

ID TAREA	NOMBRE DE LA TAREA	DESCRIPCIÓN	ARTEFACTOS/FORMATOS/ EVIDENCIAS
1	Identificar la cantidad de contenedores origen	Verificar la cantidad de contenedores origen que serán sometidos al procedimiento de unificación en cascada.	
2	Identificar el contenedor origen con menor tamaño	Determinar cuál de los contenedores origen tiene el menor tamaño para priorizar la transferencia hacia el nuevo contenedor.	
3	Analizar los contenedores origen	Ejecutar el software TreeSize para analizar y documentar las características del contenedor origen.	TreeSize (o herramientas similares)
4	Ejecutar Software LIF	Configurar y ejecutar el software LIF ingresando los parámetros adecuados para la transferencia de datos y selección del método requerido.	Software LIF
5	Revisar el formato de copia	Validar que el informe generado por el Software LIF no contenga errores o inconsistencias en los registros.	*GS04-F05 Formato de Informe de Copia*
6	Ajustes por errores en la copia	En caso de errores, ajustar las configuraciones del software de copia y repetir el proceso. Verificar nuevamente que no existan inconsistencias en los registros generados.	
7	Analizar contenedor destino	Realizar un análisis técnico detallado del contenedor destino utilizando herramientas especializadas.	TreeSize (o herramientas similares)
8	Actualizar el registro Cadena de Custodia del contenedor origen con el cambio de contenedor	Diligenciar *GS04-F01 Registro Cadena de Custodia* de contenedor origen indicando la transferencia de datos y el cambio de contenedor.	*GS04-F01 Registro Cadena de Custodia*

ID TAREA	NOMBRE DE LA TAREA	DESCRIPCIÓN	ARTEFACTOS/FORMATOS/ EVIDENCIAS
9	Actualizar el registro Cadena de Custodia del contenedor destino	Diligenciar *GS04-F01 Registro Cadena de Custodia* de contenedor destino con la novedad de la adición de evidencia del contenedor origen	*GS04-F01 Registro Cadena de Custodia*
10	Realizar borrado seguro en contenedor origen	Ejecutar un procedimiento de borrado seguro en los contenedores origen, asegurando que no queden datos residuales. Para más detalle ver **Borrado Seguro**	
11	Elaborar acta	Documentar los pasos, herramientas y métodos utilizados durante el procedimiento en el acta de exportación de elementos de evidencia digital.	*GS04-F06 Acta de Unificación de Evidencias Digitales*
12	Generar anexo digital de la unificación	Documentar la información técnica, incluir los documentos necesarios y almacenar en dispositivos ópticos con medidas de seguridad contra escritura o en donde se garantice la no modificación de la información. Para más detalle ver **Anexo Digital Copia**	

Tabla 28. Flujo de Unificación en Cascada.

5.6.1.7 Borrado Seguro

El borrado seguro es un proceso técnico que busca eliminar de forma permanente la información almacenada en dispositivos digitales, asegurando que los datos no puedan ser recuperados mediante técnicas convencionales o herramientas avanzadas de recuperación, por lo cual, en el contexto del **Laboratorio de Informática Forense** es fundamental para garantizar la confidencialidad y protección de la información sensible al final de su ciclo de vida. Existen diversos métodos de borrado seguro, entre los más comunes están:

Para discos duros (HDD):

- Sobre-escritura de datos: Reemplaza repetidamente los datos originales con patrones de bits aleatorios, asegurando su eliminación definitiva.

- Desmagnetización: Elimina los datos en medios magnéticos mediante campos magnéticos intensos.

- Destrucción física: Utilizada para dispositivos donde la eliminación digital no es viable, garantizando la imposibilidad de recuperar información.

Para discos de estado sólido (SSD) y dispositivos móviles:

- Utilidades del fabricante: Estas herramientas están diseñadas específicamente para borrar celdas de memoria NAND de forma segura.

- Software especializado: Herramientas especializadas que permiten el borrado seguro de SSDs, adaptándose a su arquitectura específica.
- Destrucción física: En casos críticos, se rompen físicamente las celdas NAND para garantizar que los datos no sean recuperables.

En **Laboratorio de Informática Forense**, el borrado seguro se realiza siguiendo estrictos estándares forenses mediante herramientas especializadas como Erase, que aseguran la trazabilidad y documentación del proceso.

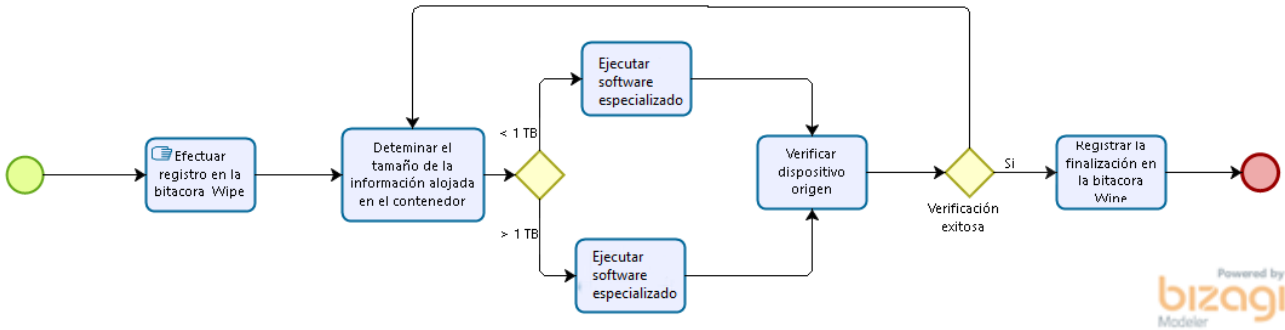

Diagrama 1. Procedimiento de borrado seguro.

5.6.1.8 Selección de Contenedor de Destino

En el **Laboratorio de Informática Forense**, la selección del contenedor de destino se realiza considerando el tamaño de la evidencia digital a transferir y las características del dispositivo de almacenamiento requerido. Para este propósito, se utilizan los siguientes criterios:

- Contenedores ópticos (CD, DVD, BLU-RAY): Recomendados para evidencias pequeñas, con capacidades de hasta 25 GB, dependiendo del formato.

- Memorias USB: Adecuadas para evidencias de tamaño medio, con capacidades entre 4 GB y 115 GB.

- Discos duros externos: Seleccionados para evidencias mayores a 115 GB, ya que ofrecen una mayor capacidad y durabilidad.

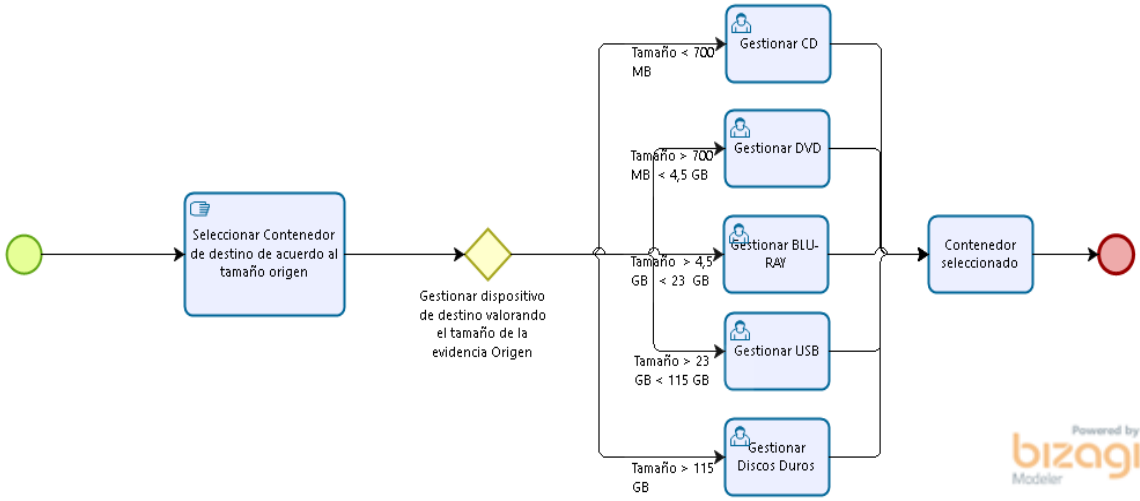

Diagrama 2. Procedimiento de selección de contenedor de destino.

5.6.1.9 Anexo Digital Copia

La consolidación de la información técnica resultante de la copia de contenedores de evidencia digital es un procedimiento que garantiza la transparencia, integridad y trazabilidad de las actividades realizadas durante el manejo de evidencias. Así como, centraliza todos los datos técnicos generados durante la copia en un dispositivo electrónico protegido contra escritura, de modo que se preserve su autenticidad y se facilite su consulta por las partes interesadas en cualquier etapa del análisis forense o del procedimiento administrativo.

ID TAREA	NOMBRE DE LA TAREA	DESCRIPCIÓN	ARTEFACTOS/FORMATOS/ EVIDENCIAS
1	Seleccionar información técnica	Identificar y seleccionar la información técnica de los contenedores de origen y destino. Anexar el *GS04-F05 Formato de Informe de Copia*.	• TreeSize (o herramientas similares) • *GS04-F05 Formato de Informe de Copia*
2	Imprimir información técnica (si aplica)	Generar una copia física de la documentación técnica seleccionada para incluirla en el expediente y anexarla a la entrega.	
3	Almacenar en dispositivo electrónico sin escritura	Transferir la información técnica a un medio óptico (CD, DVD o Blu-Ray) o dispositivo electrónico protegido contra escritura para garantizar su preservación.	• CD, DVD o Blu-Ray • Otros

Tabla 29. Flujo de anexo digital copia.

5.6.1.10 Anexo Digital de Unificación

El Anexo Digital de Unificación es un procedimiento que permite consolidar, en un repositorio seguro, toda la información técnica, administrativa y forense generada durante las actividades de unificación de evidencias digitales. A diferencia del *Anexo Digital de Copia*, este proceso incluye no solo los datos técnicos obtenidos durante la copia de contenedores, sino también los documentos asociados a cada Visita de Inspección Administrativa, como formatos de adquisición de imágenes forenses y registros de cadena de custodia.

ID TAREA	NOMBRE DE LA TAREA	DESCRIPCIÓN	ARTEFACTOS/FORMATOS/ EVIDENCIAS
1	Seleccionar información técnica	Seleccionar la información técnica de los contenedores de origen y destino.	• TreeSize (o herramientas similares) • *GS04-F05 Formato de Informe de Copia*
2	Imprimir información técnica (si aplica)	Generar una copia física de la documentación técnica seleccionada para incluirla en el expediente y anexarla a la entrega.	
3	Almacenar en dispositivo electrónico sin escritura	Transferir la información técnica a un medio óptico (CD, DVD o Blu-Ray) o dispositivo electrónico protegido contra escritura para garantizar su preservación.	• CD, DVD o Blu-Ray • Otros

5.7 CUSTODIAR MATERIAL PROBATORIO

El servidor público y/o contratista designado para la custodia de material probatorio debe preservar y salvaguardar todos los elementos adquiridos y vincularlos debidamente al sistema de cadena de custodia durante los actos administrativos.

Previo al almacenamiento de los elementos materiales probatorios, se llevan a cabo labores de unificación de evidencias que se encuentren asociadas a un mismo radicado, con el objetivo de optimizar los recursos del **Laboratorio de Informática Forense**. Estas labores son registradas en el documento de cadena de custodia y se conserva el registro histórico al realizar el traslado de contenedor y se hace apertura de un nuevo documento de cadena de custodia.

De igual manera, es necesario garantizar que cada uno de los dispositivos que ingresan al cuarto de evidencias, se encuentren debidamente embalados y rotulados, debido a que el almacenamiento de los dispositivos contenedores de evidencia digital, en el cuatro de evidencia o el sitio designado para tal fin, se efectúa por medio del número de radicado en orden ascendente y en caso de haber más de un contenedor con el mismo número de radicado, estos se organizan por orden alfabético de acuerdo con el serial físico del dispositivo.

Por otro lado, las copias controladas de dispositivos contenedores de evidencia digital y/o cualquier otra solicitud deben contar con la autorización del coordinador, jefe, director o delegado del área o dependencia solicitante y debe ser aprobado por el Coordinador del **GTIFSD**. Una vez se cuente con la autorización del caso, el servidor público y/o contratista designado para la custodia de material probatorio, atiende la respectiva solicitud dejando constancia en el **GS04-F01 Registro Cadena de Custodia**, documento que reposa en el expediente del área o dependencia solicitante.

Es importante resaltar que, si bien cada área solicitante es el dueño de la información recolectada, la custodia debe ser conservada por el **GTIFSD**, ya que de este modo es posible proteger la integridad, disponibilidad y confidencialidad de los datos. Adicional, el **Laboratorio de Informática Forense** cuenta con el personal idóneo para realizar cada una de las labores relacionadas con la evidencia digital y cuentan con los controles acceso suficientes, medios físicos necesarios y las herramientas de software para salvaguardar la información.

Nota: Es necesario que cada persona que interactúe con el contenedor de evidencia digital registre adecuadamente en la cadena de custodia, todas las interacciones y actividades que se realicen entorno a las evidencias digitales que reposan en él o al dispositivo en sí mismo

5.7.1 CUSTODIA

La custodia de la información se establece desde la etapa de Adquisición del Modelo API, momento en el cual se realiza la apertura del *GS04-F01 Registro Cadena de Custodia* que incluye elementos esenciales para garantizar la trazabilidad de la evidencia digital, como la identificación del dispositivo contenedor, el tipo de dispositivo, el método de embalaje, las personas involucradas en la recolección y las anotaciones correspondientes. Esta actividad se denomina anclaje del dispositivo de información con el *GS04-F01 Registro Cadena de Custodia* que asegura que cada evidencia digital quede vinculada a su registro de custodia desde el inicio del proceso, garantizando su integridad y validez probatoria.

Tipos de custodia:

- Recolección de información en actuaciones de visita de investigación administrativa.
- Requerimientos de información allegados a la entidad.
- Delaciones efectuadas en audiencia en la entidad.
- Delaciones allegadas por la empresa sujeta a investigación

ID TAREA	NOMBRE DE LA TAREA	DESCRIPCIÓN	ARTEFACTOS/FORMATOS / EVIDENCIAS
1	Recolección de la evidencia digital	Registrar los datos de identificación del contenedor de evidencia digital, como: hora, fecha, tipo de dispositivo, capacidad de almacenamiento, y personas involucradas en la recolección de información.	*GS04-F01 Registro Cadena de Custodia* anterior
2	Registro en la cadena de custodia	Documentar el transporte de la evidencia hacia la SIC	*GS04-F01 Registro Cadena de Custodia* posterior
3	entrega de dispositivo y registro en la Cadena de Custodia	Entregar el dispositivo contenedor de evidencia digital al custodio de la información, asegurando el traspaso con el correspondiente en el registro de cadena de custodia posterior.	*GS04-F01 Registro Cadena de Custodia* posterior
4	Verificación de la evidencia y la cadena de custodia	Verificar que los datos de identificación del dispositivo de evidencia digital coincidan con la información registrada en el registro de cadena de custodia.	GS04- *GS04-F01 Registro Cadena de Custodia* posterior
5	Registro en inventario	Registrar en el inventario del cuarto de evidencias los datos de identificación del contenedor de evidencia digital, como número de radicado, empresa, tipo de dispositivo, marca, serial físico y lógico, capacidad y volumen ocupado.	Inventario de dispositivos almacenados en cuarto de evidencias/caja fuerte
6	Almacenamiento de la evidencia digital	Almacenar el dispositivo contenedor de evidencia digital en el cuarto de evidencias y/o caja fuerte, dejando constancia en el registro de cadena de custodia sobre la ubicación y estado del dispositivo..	*GS04-F01 Registro Cadena de Custodia* con la anotación de la custodia en el cuarto de evidencias

Tabla 30. Flujo de Custodia.

5.7.2 ACTIVIDADES PARA EL MANEJO DE EVIDENCIAS

El manejo de las evidencias digitales establece los lineamientos necesarios para gestionar adecuadamente la información contenida en los contenedores de evidencia digital, para tal efecto, en todos los casos, debe existir una solicitud formal de aprobación realizada por parte de los coordinadores, delegados y/o jefes de área de la Entidad que necesiten acceso a las evidencias. Dichas solicitudes deberán incluir información clara y detallada como el número del caso, el tipo de evidencia, y el tipo de procedimiento que se requiere realizar (e.g., análisis, copia, exportación, consulta, entre otras).

Los tipos de evidencia digital:

- Evidencias recolectadas en visita administrativa.
- Evidencias de requerimientos allegadas a la entidad.
- Evidencias por delación realizada en la entidad.
- Evidencias por delación allegadas a la entidad.

5.7.2.1 Flujo del Manejo de Evidencias Digitales

El flujo del manejo de evidencias permite garantizar las medidas de seguridad necesarias para preservar la integridad, disponibilidad y confidencialidad de la información custodiada por el **GTIFSD**. Para ello, se documentan todas las interacciones con las evidencias digitales en el *GS04-F01 Registro Cadena de Custodia*, asegurando la trazabilidad completa de cada acción y procedimiento realizado.

ID TAREA	NOMBRE DE LA TAREA	DESCRIPCIÓN	ARTEFACTOS FORMATOS EVIDENCIAS
1	Solicitud para actividad	Recibir solicitud formal con autorización previa de los coordinadores, delegados y/o jefes de área, o de entidades de vigilancia y control.	Correo electrónico de la solicitud
2	Autorización de coordinadores, delegados y/o jefes de área	Comprobar la autorización para la actividad, verificando los datos del contenedor de evidencia digital.	
3	Identificación del dispositivo contenedor de evidencia	Identificar los datos del dispositivo: número de radicado, empresa, tipo de dispositivo, marca, serial físico, serial lógico, capacidad y volumen ocupado.	Correo electrónico indicando disponibilidad de dispositivo y solicitud de allegar *GS04-F01 Registro Cadena de Custodia*
4	Referir el contenedor de evidencia	Extraer el contenedor de evidencia digital del lugar de almacenamiento designado (cuarto de evidencias o caja fuerte).	Contenedor de evidencia digital
5	Suministrar el contenedor de evidencia digital	Entregar el dispositivo contenedor de evidencia digital al servidor público y/o contratista del **GTIFSD** para que realice la	

ID TAREA	NOMBRE DE LA TAREA	DESCRIPCIÓN	ARTEFACTOS FORMATOS EVIDENCIAS
		actividad requerida.	
6	Comprobar herramientas usadas para la actividad	Corroborar que las herramientas usadas sean fiables y que con ellas se garantice la integridad y la inalterabilidad de la información.	
7	Asegurar que el procedimiento sea realizado correctamente	Confirmar que el método utilizado por el servidor público y/o contratista del **GTIFSD** para llevar a cabo la actividad cumpla con los lineamientos establecidos y registrar la actividad en la cadena de custodia.	*GS04-F01 Registro Cadena de Custodia* con el registro de la actividad
8	Revisión física del contenedor de evidencia digital	Recibir el contenedor de evidencia digital debidamente embalado y acompañado por su cadena de custodia, registrando la actividad en el documento.	*GS04-F01 Registro Cadena de Custodia* con anotación
9	Elaborar acta	Documentar los pasos, herramientas y métodos utilizados durante el procedimiento en el acta de exportación de elementos de evidencia digital.	

Tabla 31. Flujo de cuarto de evidencias/caja fuerte.

6 DOCUMENTOS RELACIONADOS

GS04-P01 Procedimiento de Acompañamiento de Visitas y Solicitudes de Informática Forense
GA02-I01 Instructivo para la Reclamación en Caso de Siniestro
GS04-F01 Registro Cadena de Custodia
GS04-F02 Formato de Adquisición de Imágenes Forenses
GS04-F03 Rotulo Elemento Materia de Prueba o Evidencia Física
GS04-F04 Formato testigo documental de contenedor de evidencia digital ubicado fuera de expediente
GS04-F05 Formato de Informe de Copia
GS04-F06 Acta de Unificación de Evidencias Digitales
GS04-F07 Acta de Copia de Contenedores de Evidencia Digital
GS04-F08 Acta de Preservación de Páginas Web
GS04-F09 Acta de Informe Técnico
GS04-F10 Acta de Traslado de Contenedores de Evidencia Digital
GS04-F11 Acta de Depuración de Mensajes de Datos
GS04-F12 Acta de Exportación de Elementos de Evidencias Digitales

6.1 DOCUMENTOS EXTERNOS

NA

7 RESUMEN CAMBIOS RESPECTO A LA ANTERIOR VERSIÓN

Se reemplaza el modelo ATI por el modelo API, incluyendo una descripción detallada de las características, ventajas y particularidades del nuevo enfoque en el numeral 4.1.

Se agregan nuevos términos relevantes y se actualizan las definiciones existentes, adaptándolos a los estándares actuales del manejo de evidencia digital y cómputo forense.

Se revisan y actualizan todos los puntos del documento para alinearlos con las actividades que se realizan actualmente en el Laboratorio de Informática Forense, así como con las normativas nacionales e internacionales aplicables al manejo de evidencia digital.

Se agregan los siguientes numerales, que detallan procedimientos específicos para la adquisición de evidencia digital:

- 5.3.6.4: Adquisición de Evidencia Digital de Correos Electrónicos.
- 5.3.6.5: Adquisición de Evidencia Digital desde Páginas Web.
- 5.3.6.6: Adquisición de Evidencia Digital de Aplicaciones Móviles.
- 5.3.6.7: Adquisición de Evidencia Digital de Requerimientos de Información.

_____

Fin documento