CONTENIDO

1 OBJETIVO 2
2 DESTINATARIOS 2
3 GLOSARIO 2
4 GENERALIDADES 6
5 DESCRIPCION DE ACTIVIDADES 7
5.1 ATENDER SOLICITUD 7
5.2 ADQUISICIÓN 7
5.2.1 PREPARAR ADQUISICIÓN 7
5.2.2 RECOLECTAR LA INFORMACIÓN DIGITAL 13
5.2.3 GESTIONAR LAS UNIFICACIONES 18
5.3 TRATAMIENTO 20
5.3.1 COPIA EN SERVIDORES 20
5.3.2 CREACIÓN LISTA DE PROCESAMIENTO 21
5.3.3 PROCESAMIENTO 21
5.3.4 GESTIÓN DE ACCESO EVIDENCIAS EN PLATAFORMA DE INVESTIGACIÓN 22
5.3.5 PUESTA A DISPOSICIÓN 23
5.4 INVESTIGACIÓN 23
5.4.1 GESTIONAR LAS INVESTIGACIONES 23
5.5 ATENDER SOLICITUDES COMPLEMENTARIAS 25
5.5.1 SOLICITUDES COMPLEMENTARIAS 25
5.6 CUSTODIAR MATERIAL PROBATORIO 36
5.6.1 CUSTODIA 36
5.6.2 ACTIVIDADES PARA EL MANEJO DE EVIDENCIAS 37
6 DOCUMENTOS RELACIONADOS 39
7 RESUMEN CAMBIOS RESPECTO A LA ANTERIOR VERSIÓN 39

Elaborado por:	Revisado y Aprobado por:	Aprobación Metodológica por:
Nombre: Eduar Enrique Navarro Morales Cargo: Grupo de Trabajo de Informática Forense y Seguridad Digital.	Nombre: Francisco Andres Rodriguez Eraso 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: 2020-02-20

1 OBJETIVO

Establecer los lineamientos generales para la atención de la solicitud, utilización del modelo ATI (Adquisición, Tratamiento e Investigación) y custodia del material probatorio y/o confidencial para cada una de las áreas o dependencias de la Superintendencia de Industria y Comercio (en adelante SIC).

2 DESTINATARIOS

El instructivo de informática forense aplica a los servidores públicos y/o contratistas que contribuyen directa o indirectamente en las actividades del Grupo de Trabajo de Informática Forense y Seguridad Digital - GTIFSD y a cada una de las áreas o dependencias de la SIC interesadas.

3 GLOSARIO

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 garantizar la integridad y confidencialidad de los elementos probatorios en las distintas etapas e instancias procesales. (FGN[1])

CONTENEDOR DE EVIDENCIA DIGITAL: Todo dispositivo de almacenamiento de datos en formato digital, cuya finalidad es albergar de forma permanente o temporal evidencias digitales.

COPIA DE MENSAJES DE DATOS: Actividad de realizar la copia espejo de los datos desde un dispositivo origen hasta un dispositivo de destino, preservando así toda la información que éste contenga, incluyendo los bloques de los ficheros eliminados, CD o Blu-Ray espacio libre tras cada bloque, metadatos, etc.

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

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

DESCARGA DE CONTENIDOS NUBE: Actividad que consiste en la adquisición de los mensajes de datos alojados dentro de las cuentas de correo electrónico y/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. (Ley 906 de 2004 artículo 275)

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.(FGN[2])

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.

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

EVIDENCIA DIGITAL: Cualquier dato o conjunto de datos de información generado, almacenado o transmitido en formato binario (digital) que evidencien elementos propios que pueden ser susceptibles de recaudo durante la práctica de una visita administrativa y entre otras actividades.

ADQUISICIÓN DE COMPUTADORAS (MAC, WINDOWS, LINUX): Actividad realizada durante Visita de Inspección Administrativa o audiencia en la cual se realiza una copia exacta de los mensajes de datos de ordenadores con sistema operativo MAC OS, WINDOWS Y/O LINUX.

ADQUISICIÓN DE MOVILES: Actividad de recolección de datos en dispositivos móviles que cuenten con capacidad de memoria interna y funciones de comunicación como: tabletas, celulares, tablets, GPS. Los métodos de extracción varían según el software especializado, las herramientas de fabricantes y backups

[2] Ibidem

de dispositivos. Las extracciones habilitadas en dispositivos con sistema iOS son la extracción lógica y la extracción de sistemas de archivos y las extracciones habilitadas en dispositivos con sistema Android son la extracción lógica, la extracción de sistema de archivos y la extracción física.

EXTRACCIÓN FÍSICA: Método de extracción similar a la extracción del disco duro de un computador, en el cual se efectúa una copia bit a bit de los contenidos de la memoria flash del dispositivo. Es el método más eficaz para la recuperación de archivos eliminados dentro del dispositivo.

EXTRACCIÓN LÓGICA: Método en el cual las herramientas forenses se comunican con el sistema operativo del dispositivo mediante una API (Application Programming Interface) y solicitan los datos del sistema. A través de este tipo de extracción, los datos típicos disponibles son los registros de llamadas, SMS, MMS, imágenes, videos, archivos de audio, contactos, calendarios y datos de aplicación. Los datos exportados en estas categorías serán datos en tiempo real y no tendrán la posibilidad de contener datos eliminados.

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. (FGN[3])

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

FUNCIÓN HASH: Se entiende como el algoritmo que consigue crear a partir de un mensaje de datos una salida alfanumérica que representa un resumen de toda la información contenida en el mismo; mediante esta salida podrá ser comprobada la confiabilidad, integridad y autenticidad del mensaje de datos permitiendo su admisibilidad y fuerza probatoria como elemento de prueba.

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.(MINTIC[4])

INSTRUCTIVO DE VISITA: Documento dirigido a los funcionarios encargados de realizar la visita de inspección administrativa, en el cual se encuentra la información

[3] Ibidem

[4] Tomado de la Guía de Evidencia Digital del Ministerio de la Tecnologías de la Información y las Comunicaciones - MINTIC.

necesaria para la identificación del caso, los hechos que en los que se fundamenta la actuación y, entre otros aspectos, la información a recaudar durante la visita mediante los medios de prueba contemplados en la Ley.

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

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 (Definición de acuerdo a Ley 527 de 1999 Artículo 2º)

MEMORIA VOLÁTIL: Mientras haya flujo eléctrico, es toda información activa que reposa en el dispositivo. Dicha información reposa en las memorias de acceso aleatorio conocidas como memorias RAM. Cuando se adquiere información de un computador, es necesario que también se obtenga la memoria volátil del mismo.

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 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. http://www.edrm.net/resources/glossaries/glossary.

MODELO ATI: Tomando como guía el modelo de referencia de descubrimiento electrónico. Se definen buenas prácticas para la adquisición, tratamiento e investigación de la evidencia digital.

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 Elementos Materiales Probatorios y Elementos Físicos y que por tanto

son responsables por su recolección, preservación y entrega a la autoridad competente. (FGN[5])

PROCESAMIENTO: Actividad en la cual se toma la evidencia digital de un caso en específico, y se construye un sistema de datos de la información para su consulta masiva.

SUITE DE LOS FABRICANTES DE DISPOSITIVOS MÓVILES: Los fabricantes de dispositivos móviles cuentan con software específico que permite la sincronización de los dispositivos móviles elaborados por su fábrica con los equipos de cómputo, lo anterior con el fin de realizar las tareas de administración, caracterización, respaldo del dispositivo y actualización.

UNIFICACIÓN: Actividad por medio del cual se reúne la información adquirida de uno o varios contenedores de evidencia de origen a uno o varios contenedores de evidencia destino en donde reposará la información de manera integral. Este actividad se encuentra soportado por informes técnicos de copiado y anotaciones en las respectivas cadenas de custodias de los contenedores de evidencia digital. Esta actividad es soportada por el Acta de Unificación.

VERIFICACIÓN IMAGEN FORENSE: Comprobación del estado de la imagen forense para garantizar la exactitud y validez de la copia de la información adquirida, refiérase al ejercicio de adquisición y verificación de la huella HASH, mediante los algoritmos SHA1 y MD5, tanto de los dispositivos del origen como los de destino.

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 ATI. Por lo tanto, el Grupo de Trabajo de Informática Forense y Seguridad Digital, es el encargado de atender las solicitudes de cada de las áreas o dependencias de la Superintendencia de Industria y Comercio (en adelante SIC) relacionadas con el servicio de apoyo en las técnicas de Adquisición, Tratamiento e Investigación de mensajes de datos y/o evidencias digitales, garantizando el valor probatorio de la información mediante herramientas de hardware y software especializado, descrito

[5] Ibidem

en el GS04-P01 Procedimiento de Acompañamiento de Visitas y Solicitudes de Informática Forense.

5 DESCRIPCION DE ACTIVIDADES

5.1 ATENDER SOLICITUD

Los servidores públicos y/o contratistas del grupo de Trabajo de Informática Forense y Seguridad Digital - GTIFSD analizan las solicitudes formuladas por los servidores públicos y/o contratistas de las áreas o dependencias solicitantes de la Superintendencia de Industria y Comercio.

El Coordinador del GTIFSD recibe y la asigna la solicitud al Servidor Público y/o Contratista del GTIFSD para la gestión y cumplimiento de las funciones:

Acompañar las visitas administrativas, la recolección de evidencias digitales, el aseguramiento de la evidencia digital y la unificación de la información recolectada.

Copiar de la información recolectada en las visitas administrativas, procesamiento de las evidencias digitales, la gestión y el soporte de la creación de usuarios, asignados de permisos y uso sobre las herramientas de investigación web.

Apoyar las investigaciones que se lleven a cabo por parte de las áreas o dependencias de la Superintendencia de Industria y Comercio, mediante vectores de búsqueda y análisis de información

Gestionar las solicitudes complementarias de Copia de Evidencia Digital, Preservación de Páginas Web, ***Informe Técnico***, Traslado de Evidencia Digital, Depuración de Mensajes de Datos, Exportación de Elementos de Evidencias Digitales

5.2 ADQUISICIÓN

5.2.1 PREPARAR ADQUISICIÓN

El GTIFSD establece las siguientes tareas para la recolección de las evidencias digitales:

5.2.1.1 Establecer Lineamientos Iniciales

El servidor público o contratista debe preparar los elementos precisos (Software, hardware y documentación) para la recolección de las evidencias digitales, lo anterior mediante el estudio riguroso 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 hacer una recolección adecuada de esta, minimizando la pérdida o alteración de los mensajes de datos, lo anterior mediante la revisión del instructivo de visita del 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) • Grabadora (1) • Cámara Fotográfica (1) • Batería de repuesto para grabadora (2) • Maletín UFED con su respectiva Dongle en caso de ser necesario (1) • GS04-F02 Formato de Adquisición de Imágenes Forenses (7) • GS04-F01 Registro Cadena de Custodia (7) • DVD con funda (1) • Sello (5) • Disco Duro (2) • Testigos Métricos • GS04-F03 Rotulo Elemento Materia de Prueba o Evidencia Física
4	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 • MAC OS X • MD5 Sumer • FTK Imager • Winaudit • Evidence Collector • Crystal disk • Bat inventario redes • Bat inventario PC • Bat unificación • Easy Robocopy • Encase • Fastcopy • Treezise • VSO Inspector • CD Burner • Xinorbis • UFED 4 PC • UFED Physical Analyzer

			• Suite de los fabricantes de dispositivos móviles.

Tabla 1 - Preparar Visita

5.2.1.2 Aislar la Escena o Ubicación

Una vez los servidores públicos y/o contratistas designados para practicar la visita de inspección administrativa se encuentren en el lugar de la diligencia deben aislar la escena y fijar mediante fotografía o video los dispositivos contenedores de mensajes de datos

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 adquirio 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.	
		Realizar un registro fotográfico en cual se debe identificar el dispositivo al cual se realizará la imagen forense. Se deben tomar tres fotos Fotografía frontal del dispositivo Fotografía trasera del dispositivo Fotografía lateral del dispositivo.	Dispositivo electrónico con cámara fotográfica Testigo métrico

Tabla 2 Aislar escena

5.2.1.3 Estructura de Carpetas y Nombrar Imágenes

Los servidores públicos 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 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 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. WEB: Almacenamiento en la nube, incluidos los correos electrónicos. DEC: Declaraciones y/o Testimonios. REQ: Requerimientos de información. SER: La información tomada de servidores. DDI: La información tomada de Discos Duros internos. DDE: La información tomada de Discos Duros externos. USB: La información tomada de un Dispositivo USB. MULT: Archivos multimedia, fotos y/o videos INFO: Información tomada de las tareas en ejecución. CD: La información tomada de un dispositivo óptico CD. DVD: La información tomada de un dispositivo óptico DVD. BD: La información tomada de un dispositivo óptico BD. 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 tendrán una numeración independiente de manera secuencial iniciando igualmente desde el número uno.	01-DEC_ NOMBRE-APELLIDO 02-DEC_ NOMBRE-APELLIDO 03-DEC_ NOMBRE-APELLIDO

7	Enumerar información de anexos	Los anexos tendrán una numeración independiente y única, relacionada con la evidencia a la que pertenecen.	01-PC_MULT_NOMBRE_APELLIDO 01-INFO_MULT_NOMBRE_APELLIDO 02-PC_MULT_NOMBRE_APELLIDO 02-INFO_MULT_NOMBRE_APELLIDO
8	Estructurar Carpetas de computadores	Cuando se adquiere la información de computadores la carpeta principal debe nombrarse igual que la imagen forense, adicional a ello es necesario crear 4 subcarpetas, una primera en donde se almacenará la imagen forense, en la segunda se almacenará la información de las tareas en ejecución con su respectiva función hash, en la tercera se almacenará la información multimedia con su respectivo hash, y una cuarta en donde se almacenará únicamente la memoria volátil.	01-PC_ NOMBRE-APELLIDO • IMG_PARC (IMAGEN FORENSE DEL COMPUTADOR) • INFORMACIÒN DATOS HASH • MULTIMEDIA DATOS HASH • MV
9	Estructurar Carpetas de celulares	Cuando se adquiere la información de celulares la carpeta principal debe nombrarse igual que la imagen forense, adicional a ello es necesario crear 2 sub carpetas, una primera en donde se almacenará la imagen forense, y otra en donde se almacenarán las adquisiciones generadas por la herramienta para la extracción de dispositivos móviles	01-CEL_ NOMBRE-APELLIDO • IMG_CEL (imagen forense de las adquisiciones obtenidas) • Adquisición (Extracciones obtenidas por medio de la herramienta)
10	Estructurar carpetas de Declaraciones	Cuando se graban audios de testimonios o videos de inspecciones oculares, es necesario crear una carpeta con el nombre "DECLARACIONES" y otra con el nombre "INSPECCIÒN OCULAR", dentro de estas se almacenarán todas las declaraciones y/o videos de inspecciones oculares, cada una tendrá 2 sub carpetas, una primera en donde se almacenará la imagen forense de la declaración y/o inspección ocular, y otra en donde se almacenará el archivo de audio y/o video generado.	DECLARACIONES • 01-DEC_ NOMBRE-APELLIDO GRABACIÓN HASH • 02-DEC_ NOMBRE-APELLIDO GRABACIÓN HASH • INSPECCIÒN OCULAR MULTIMEDIA HASH
11	Estructurar otras carpetas	Para todos los otros tipos de adquisiciones se tendrá la carpeta con el nombre de la imagen forense y dos subcarpetas, una primera en donde se almacenará la imagen forense de la información, y otra en donde se almacenará el archivo de información.	• 01-WEB_ NOMBRE-APELLIDO DATOS HASH • 02-REQ_ NOMBRE-APELLIDO DATOS HASH

Tabla 3 Estructurar Carpetas y nombrar evidencias

5.2.1.4 Identificar Fuentes de Información

Las fuentes de información digital son variadas, por lo cual, el servidor público o contratista designado debe identificar todas las posibles fuentes de información que almacenen mensajes de datos relevantes para la investigación.

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, USB, Disquete
		Identificar si la fuente de información es un dispositivo electrónico	Computadores, tabletas, celulares, servidores, 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
3	Identificar fuentes de información de respaldo	identifica si existen copias de seguridad de la información contenida en estos dispositivos y si estos tienen conexiones externas	Cintas, redes de área de almacenamiento entre otros

Tabla 4 Identificar Fuentes de información

5.2.1.5 Planificar Orden de Adquisición

El servidor público y/o contratista debe planificar el orden de adquisición de los múltiples dispositivos que almacenan mensajes de datos, esto con el fin de asegurar que la información con mayor grado de volatilidad sea adquirida, garantizando así la integridad de los mensajes de datos, en esta actividad pueden existir variaciones dependiendo de la naturaleza de investigación.

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 correos electrónicos	Solicitar y corroborar las credenciales de acceso a los correos electrónicos para que el servidor público o contratista designado para realizar las descargas de correo electrónico tenga el tiempo suficiente para confirmar el inicio de descarga durante la visita de inspección administrativa.
3	Adquirir información de Dispositivos móviles	Si es posible solicitar con anterioridad los dispositivos móviles para efectuar la mayor cantidad de extracciones y para tener el tiempo suficiente para probarlas.

4	Adquirir información de computadores	Solicitar los computadores con anterioridad con el fin de garantizar la finalización de la imagen forense en sitio.
5	Adquirir información de las tareas en ejecución	Adquirir la información de las tareas en ejecución y realizar la imagen forense de los mismos.
6	Adquirir testimonios	Realizar la imagen forense de los testimonios perpetrados durante la visita.

Tabla 5 Planificar orden de adquisición

5.2.1.6 Examinar Ejecución y Detalles Técnicos

La ejecución en el dispositivo deben ser identificados para determinar si existen tareas que puedan destruir o modificar los mensajes de datos a recolectar, también se identificarán las características de los dispositivos como identificadores únicos (serial físico, marca, modelo) y elementos de hardware y software del equipo inspeccionado, en esta actividad pueden existir variaciones dependiendo del tipo de dispositivo contenedor de mensajes de datos.

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

Tabla 6 Examinar tareas en ejecución

5.2.2 RECOLECTAR LA INFORMACIÓN DIGITAL

Se lleva a cabo la adquisición de mensajes de datos desde mediante la adquisición de computadoras con sistema operativo Windows o IOS, extracción de móviles con sistema operativo Android o IOS e extracción de información en la nube; las tareas que se presentan a continuación pueden variar dependiendo del tipo de adquisición, el tamaño de los mensajes de datos y el nivel de seguridad con el que cuente el sistema operativo de la computadora y/o dispositivo móvil.

5.2.2.1 Adquisición de evidencia digital desde computadoras con sistema operativo Windows

ID TAREA	NOMBRE DE LA TAREA	DESCRIPCIÓN	ARTEFACTOS/FORMATOS/ EVIDENCIAS
1	Preparar software forense de creación de Imágenes	Introducir dispositivo magnético con el software para la creación de imágenes de datos.	USB de Visita
2	Abrir software para la creación de imágenes de datos.	Ejecutar software forense de creación de imágenes,	FTK IMAGER
3	Identificar ruta origen	Seleccionar ruta, fuente de la información.	FTK IMAGER
4	Identificar ruta destino	Seleccionar ruta en donde se almacenará la imagen forense.	FTK IMAGER
5	Generar Imagen Forense	Parametrizar herramienta y utilizar estándar para nombrar imágenes forenses	FTK IMAGER
6	Verificar Imagen Forense	Asegurarse de que la imagen forense haya terminado satisfactoriamente.	.TXT generado por FTK IMAGER

Tabla 7 Adquisición PC WINDOWS

5.2.2.2 Adquisición de Evidencia Digital desde Computadoras con Sistema Operativo IOS.

Se recomiendan dos alternativas para la creación de imágenes forenses desde computadoras con sistema operativo IOS.
Método 1: Este método implica ejecutar comandos por medio de la interfaz de línea de comandos (Terminal) con la que cuentan las computadoras con sistema operativo IOS.

ID TAREA	NOMBRE DE LA TAREA	DESCRIPCIÓN	ARTEFACTOS/FORMATOS/ EVIDENCIAS
1	Abrir Terminal de MAC		
2	Identificar ruta de almacenamiento de la herramienta de creación de imágenes de datos	Identificar dispositivos detectados por la computadora MAC	Terminal (MAC)
3	Ejecutar FTK Imager		Terminal (MAC)
4	Identificar ruta destino	Identificar el Disco en el que se generará la imagen Forense	Terminal (MAC)
5	Generar Imagen Forense	Parametrizar herramienta y utilizar estándar para nombrar imágenes forenses	FTK IMAGER
6	Verificar Imagen Forense	Asegurarse de que la imagen forense haya terminado satisfactoriamente.	Terminal (MAC)

Tabla 8 Adquisición 1 PC IOS

Método 2: En este método es necesario manejar la herramienta Evidence Collector.

ID TAREA	NOMBRE DE LA TAREA	DESCRIPCIÓN	ARTEFACTOS/FORMATOS/ EVIDENCIAS
1	Preparar software forense de creación de Imágenes	Introducir dispositivo magnético con el software para la creación de imágenes de datos.	• USB de Visita
2	Abrir software para la creación de imágenes de datos.	Ejecutar software forense de creación de imágenes,	• Evidence Collector
3	Identificar ruta origen	Seleccionar ruta, fuente de la información.	• Evidence Collector
4	Identificar ruta destino	Seleccionar ruta en donde se almacenará la imagen forense.	• Evidence Collector
5	Verificar Imagen Forense	Asegurarse de que la imagen forense haya terminado satisfactoriamente.	• Evidence Collector

Tabla 9 Adquisición 2 PC IOS

5.2.2.3 Adquisición de Evidencia Digital Desde Dispositivos Móviles con Sistema Operativo Android O IOS

ID TAREA	NOMBRE DE LA TAREA	DESCRIPCIÓN	ARTEFACTOS/FORMATOS/ EVIDENCIAS
1	Identificar Fabricante del dispositivo móvil	Asegurarse de que se cuenta con la suite del Fabricante, en caso de no tenerla es necesario que esta sea descargada desde la página del fabricante.	
2	Realizar Copia de respaldo de la información del dispositivo móvil	Realizar mediante la suite del fabricante la copia de respaldo de la información del celular	• Hisuite • Kíes • ITunes • Al Suite • Motorola PC Sync • Entre otros.
3	Extraer información del dispositivo móvil	Efectuar mediante UFED 4PC las siguientes extracciones: Extracción Lógica Extracción del sistema de archivos APK Downgrade	• UFED 4 PC
4	Verificar Extracción en Physical Analyzer	Abrir extracciones mediante Physical Analyzer para verificar si la extracción no cuenta con ningún tipo de cifrado y para validar si se ha extraído satisfactoriamente la información del dispositivo móvil.	• Physical Analyzer
5.	Solicitar contraseña de cifrado de dispositivo móvil	En caso de que se identifique que la información del dispositivo móvil se encuentra cifrada es necesario solicitar al dueño del dispositivo dicha contraseña.	
6	Documentar el Acta de Visita	Especificar en la documentación del acta lo ocurrido con el cifrado de la información,	• Acta de Visita

ID TAREA	NOMBRE DE LA TAREA	DESCRIPCIÓN	ARTEFACTOS/FORMATOS/ EVIDENCIAS
		indicando si la contraseña de descifrado fue entregada o si no lo fue.	
7	Abrir software para la creación de imágenes de datos.	Ejecutar software forense de creación de imágenes,	• FTK IMAGER
8	Identificar ruta origen	Seleccionar ruta, fuente de la información.	• FTK IMAGER
9	Identificar ruta destino	Seleccionar ruta en donde se almacenará la imagen forense.	• FTK IMAGER
10	Generar Imagen Forense	Parametrizar herramienta y utilizar estándar para nombrar imágenes forenses	• FTK IMAGER
11	Verificar Imagen Forense	Asegurarse de que la imagen forense haya terminado satisfactoriamente.	• TXT generado por FTK IMAGER

Tabla 10 Adquisición Dispositivos móviles

5.2.2.4 Adquisición de Información en la Nube

ID TAREA	NOMBRE DE LA TAREA	DESCRIPCIÓN	ARTEFACTOS/FORMATOS/ EVIDENCIAS
1	Verificar credenciales	Validar el Ingreso del correo electrónico con el usuario y contraseña solicitada.	Yahoo!, Gmail, Outlook, Office365, Zimbra, Godaddy, entre otros.
2	Habilitar IMAP	Verificar si se encuentra habilitada la opción de Habilitar IMAP	Yahoo!, Gmail, Outlook, Office365, Zimbra, Godaddy, entre otros.
3	Permitir acceso a aplicaciones menos Seguras	Para los correos de Gmail, dirigirse a aplicaciones con acceso a la cuenta y luego asegurarse de que la opción Permitir acceso a aplicaciones menos Seguras se encuentre habilitada	• Gmail
4	Sincronizar Cuenta por IMAP	Ingresar a la aplicación de escritorio de Outlook para sincronizar cuenta por medio de	• OULOOK
5	Validar Puertos IMAP Y SMTP		
6	Verificar descarga de contenidos web - correos electrónicos		
7	Abrir software para la creación de imágenes de datos.	Ejecutar software forense de creación de imágenes,	• FTK IMAGER
8	Identificar ruta origen	Seleccionar ruta, fuente de la información.	• FTK IMAGER
9	Identificar ruta destino	Seleccionar ruta en donde se almacenará la imagen forense.	• FTK IMAGER

ID TAREA	NOMBRE DE LA TAREA	DESCRIPCIÓN	ARTEFACTOS/FORMATOS/ EVIDENCIAS
10	Generar Imagen Forense	Parametrizar herramienta y utilizar estándar para nombrar imágenes forenses	• FTK IMAGER
11	Verificar Imagen Forense	Asegurarse de que la imagen forense haya terminado satisfactoriamente.	• TXT generado por FTK IMAGER

Tabla 11 Adquisición de información en la nube

5.2.2.5 Adquisición de Anexos

Generar imagen forense de información de tareas en ejecución y de archivos multimedia como fotos y videos soporte de la adquisición de la evidencia digital.

ID TAREA	NOMBRE DE LA TAREA	DESCRIPCIÓN	ARTEFACTOS/FORMATOS/ EVIDENCIAS
7	Abrir software para la creación de imágenes de datos.	Ejecutar software forense de creación de imágenes.	• FTK IMAGER
8	Identificar ruta origen	Seleccionar ruta, fuente de la información.	• FTK IMAGER
9	Identificar ruta destino	Seleccionar ruta en donde se almacenará la imagen forense.	• FTK IMAGER
10	Generar Imagen Forense	Parametrizar herramienta y utilizar estándar para nombrar imágenes forenses	• FTK IMAGER
11	Verificar Imagen Forense	Asegurarse de que la imagen forense haya terminado satisfactoriamente.	• TXT generado por FTK IMAGER

Tabla 12 Adquisición de Anexos

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

ID TAREA	NOMBRE DE LA TAREA	DESCRIPCIÓN	ARTEFACTOS/FORMATOS/ EVIDENCIAS
1	Documentar Acta de visita	El resultado de cada actividad debe ser documentado mediante el acta de visita realizada durante la diligencia,	Acta de Visita
2	Diligenciar GS04-F02 Formato de Adquisición de Imágenes Forenses	Diligenciar por cada adquisición de evidencia digital el GS04-F02 Formato de Adquisición de Imágenes Forenses de imagen forense (exceptuando las declaraciones).	GS04-F02 Formato de Adquisición de Imágenes Forenses
3	Abrir GS04-F01 Registro Cadena de Custodia	Abrir GS04-F01 Registro Cadena de Custodia por dispositivo de almacenamiento y por requerimiento de información	GS04-F01 Registro Cadena de Custodia
4	Diligenciar rótulo	Diligenciar rótulo para los requerimientos de información almacenados en dispositivos ópticos	Formato Rótulo de evidencia física

Tabla 13 Soportes de adquisición

5.2.2.7 Transportar el Dispositivo de Almacenamiento

Los funcionarios y/o contratistas se comprometen a transportar y allegar a las instalaciones de la entidad SIC , el dispositivo de almacenamiento de evidencias digitales que contiene todos los mensajes de datos recolectados durante la visita de inspección, evitando el daño y garantizando la originalidad, autenticidad e inalterabilidad de la información recaudada.

*El Servidor Público y/o Contratista que se identifica como primer responsable debe allegar las evidencias digitales recolectadas al día siguiente de finalizada la visita, en los casos que están fuera de los horario laboral de la entidad.

5.2.2.8 Entrega de la Visita, Lista de Imágenes y Control de Evidencias

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.	Excel de control de evidencias
2	Ejecutar BAT de unificación	Ejecutar Script para detallar el contenido de carpetas, y el peso del disco.	• BAT de unificación • Xinorbis
3	Preparar formatos de adquisición y GS04-F01 Registro Cadena de Custodia	Organizar formatos de adquisición y adquisición en orden de adquisición del hallazgo	GS04-F02 Formato de Adquisición de Imágenes Forenses GS04-F01 Registro Cadena de Custodia
4	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 los contenedores de evidencia digital	

Tabla 14 Entrega de Visita

5.2.3 GESTIONAR LAS UNIFICACIONES

A partir de la ejecución y entrega de la de Visita, se da inicio a esta actividad. Su objetivo es procesar los datos o archivos de información que pueden llegar a ser indicios de prácticas en contra los regímenes que protege y vigila la Superintendencia de Industria y Comercio. Cuando la actividad de visita concluye, el Coordinador GTIFSD mediante la evaluación de las empresas visitadas durante la Visita de Inspección Administrativa llevará a cabo la asignación de las actividades de Unificación a los servidores públicos y/o contratistas disponibles para ejecutar dicha labor.

5.2.3.1 Gestionar las Unificaciones

Está compuesto por las tareas que se relacionan a continuación:

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.	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 deberá realizar sesiones de entendimiento con el servidor público y/o contratista encargado de la Visita.	GS04-F01 Registro Cadena de Custodia. Rótulo GS04-F02 Formato de Adquisición de Imágenes Forenses
3	Actividad - Realizar unificación en cascada	La unificación en cascada consiste en almacenar la información recolectada en todas las empresas visitadas bajo un mismo radicado, en un solo contenedor de evidencia digital utilizado dentro de la misma. Para realizar la unificación en cascada, es necesario verificar el tamaño de los dispositivos hasta identificar el dispositivo con mayor tamaño utilizado, lo anterior con el fin de seleccionarlo como el contenedor temporal de destino, el cual albergará la información recolectada en las demás empresas visitadas. Al finalizar esta actividad toda la información de la visita de inspección administrativa debe encontrarse en el contenedor temporal de destino, para más detalle ver SUBACTIVIDAD REALIZAR UNIFICACIÓN EN CASCADA.	GS04-F01 Registro Cadena de Custodia Origen y Destino Tree-Size LIRIS Informes de Copia Informes Técnicos
4	Copiar información en contenedor	Seleccionar un dispositivo contenedor final de evidencias digitales de acuerdo al estándar propuesto en el SUBACTIVIDAD REALIZAR COPIA DE CONTENEDORES para la selección de contenedor. Copiar información de contenedor temporal de destino a contenedor final de evidencias digitales. Realizar documentación técnica de la actividad Para más detalle ver ACTIVIDAD DE COPIA DE CONTENEDORES	GS04-F01 Registro Cadena de Custodia Origen y Destino LIRIS TREE SIZE Informes de Copia Informes Técnicos
5	Cerrar GS04-F01 Registro Cadena de Custodia Origen	Una vez realizadas las actividades del ACTIVIDAD DE BORRADO SEGURO es necesario que el encargado del método de 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.	GS04-F01 Registro Cadena de Custodia Origen

ID TAREA	NOMBRE DE LA TAREA	DESCRIPCIÓN	ARTEFACTOS FORMATOS EVIDENCIAS
6	Generar registro(s) de la actividad	Realizar la documentación del detalle de la forma en la que técnicamente se soportará el requerimiento.	GS04-F06 Acta de Unificación de Evidencias Digitales
7	Aprobar registro(s) de la actividad	Validar las actividades y la documentación técnica.	
8	Firmar registro de unificación	Formalizar la aceptación de la actividad de Unificación.	
9	Archivar información	Clasificar y almacenar información en archivo físico y/o digital Determinar si el contenedor se anexa al expediente o se almacena en el cuarto de evidencias. Contenedores que se almacenan en el expediente: CD, DVD, BLU-RAY. Contenedores que se almacenan en el cuarto de evidencias: DISCO DURO, USB.	
10	Verificar el tipo de contenedor	Valorar el tipo de contenedor 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, 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) Entregar al líder del caso, la documentación correspondiente.	
14	Almacenar hoja de recibido para archivo	Sacar copia de primera hoja de documentación entregada para firma del solicitante como soporte de la entrega. Almacenar primera hoja de documentación entregada dentro de archivo del GTIFSD	

Tabla 15 Flujo de Gestionar las unificaciones

5.3 TRATAMIENTO

5.3.1 COPIA EN SERVIDORES

En esta tarea se transfiere/copia a los servidores de almacenamiento del GTIFSD, la información adquirida en el desarrollo de una Visita de inspección administrativa o en audiencia. Durante la actividad de copia en servidores de los mensajes de datos los servidores públicos 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 permita crear un registro de:	• FASTCOPY

	permita crear un registro 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) Fecha y hora en que fue realizada la copia.	
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 16 Flujo de Copia de Servidores

5.3.2 CREACIÓN LISTA DE PROCESAMIENTO

Una vez sea almacenada la información recolectada durante la Visita Administrativa dentro de los dispositivos de almacenamiento del GTIFSD, los servidores públicos y/o contratistas del Laboratorio deberán crear como buena práctica de procesamiento una lista con la información de las evidencias que deberán ser procesadas, de esta manera podrá conocer la cantidad y el tamaño de las evidencias que se deberán procesar.

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

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

5.3.3 PROCESAMIENTO

Hace referencia al procesamiento de las evidencias digitales adquiridas en la etapa anterior. 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, la extracción y/o recuperación de datos dentro de las evidencias digitales, entre otros. El procesamiento está clasificado en tres tipos:

i. Procesamiento cortó. Este método solamente incluye la extracción de los mensajes de datos contenidos en las muestras tomadas, con herramientas de software que tan solo identifican los archivos digitales dentro de estas, lo anterior sin la realización de acciones de recuperación propias de procesamientos más avanzados.

ii. Procesamiento completo. Este procesamiento también incluye la extracción de mensajes de datos contenidos en las muestras tomadas, pero también realiza otras acciones como la recuperación de datos borrados o perdidos, y la organización o indexación del volumen de mensajes de datos adquiridos.

iii. Procesamiento alterno. Este tipo de procesamiento tiene las mismas características del procesamiento mencionado en el numeral anterior, pero con otras herramientas de software. Esto se hace con el fin de agilizar y personalizar los procesamientos de muestras tomadas, de acuerdo a las necesidades del negocio. Para efectuar el procesamiento de los mensajes de datos es necesario contar con software diseñado para el tratamiento de información.

5.3.4 GESTIÓN DE ACCESO EVIDENCIAS EN PLATAFORMA DE INVESTIGACIÓN

Las solicitudes de acceso a los casos que contienen las evidencias digitales se realizan por medio de los coordinadores, delegados y/o jefes de áreas o Delegaturas de la entidad.

El acceso a las evidencias en la plataforma de investigación, tiene como finalidad tener un control de los grupos y usuarios los cuales se les asignan permisos para el acceso y visualización de las evidencias digitales y con la trazabilidad de obtener un registro de las evidencias consultadas.

El administrador de la plataforma es el encargado de realizar todo tipo de gestión de creación y asignación de permisos sobre los casos donde se encuentran las evidencias digitales.

ID TAREA	NOMBRE DE LA TAREA	DESCRIPCIÓN	ARTEFACTOS FORMATOS EVIDENCIAS
1	Solicitud para creación y/o permisos de usuario	Recibir solicitud con previa autorización de coordinadores, delegados y/o jefes de área.	Correo electrónico de la solicitud
2	Autorización de coordinadores, delegados y/o jefes de área	Comprobar autorización por parte de coordinadores, delegados y/o jefes de área	
3	Información requerida para la creación y/o asignación de permisos	Ejecutar la creación y/o asignación de permisos en la plataforma de investigación.	Evento de creación y/o asignación de permisos

4	creación y/o asignación de permisos	Verificar la creación y/o asignación de permisos para revisión de las evidencias digitales	
5	creación y/o asignación de permisos	Responder al solicitante de la creación y/o asignación de permisos en la plataforma de investigación	Correo Electrónico

Tabla 17 Flujo de Gestión de Acceso en Plataforma de Investigación

5.3.5 PUESTA A DISPOSICIÓN

La puesta a disposición de los diferentes casos procesados para que los expertos en la materia de la que se está investigando, puedan analizar, revisar o cualquier otra actividad que consideren pertinente dentro de la etapa de investigación, en esta actividad es clave que las herramientas usadas para la puesta a disposición sean intuitivas en su uso para personal no técnico con el fin de identificar el mayor número de elementos materiales probatorios. El Laboratorio tiene distintos softwares licenciados para colocar a disposición los mensajes de datos adquiridos y procesados en las etapas anteriores, con el fin de que estos puedan ser consultados y analizados únicamente al interior de la entidad por el personal del GTIFSD indicado y autorizado, estos softwares son:

Clase de software	Nombre	Descripción
Plataforma Web	Summation	Consulta para análisis de mensajes de datos adquiridos de dispositivos ópticos, magnéticos y electrónicos, excluyendo dispositivos móviles.
Plataforma Web	UFED ANALYTICS ENTERPRISE	Consulta para análisis de mensajes de datos adquiridos de dispositivos móviles
Aplicación	FTK Lab	Procesamiento y consulta para análisis de mensajes de datos adquiridos de dispositivos ópticos, magnéticos y electrónicos, excluyendo dispositivos móviles.
Aplicación	FTK Stand Alone	Procesamiento y consulta para análisis de mensajes de datos adquiridos de dispositivos ópticos, magnéticos y electrónicos, excluyendo dispositivos móviles.
Aplicación	FTK Imager	Consulta para análisis de mensajes de datos adquiridos de dispositivos ópticos, magnéticos y electrónicos, excluyendo dispositivos móviles.
Aplicación	UFED Physical Analyzer	Procesamiento y consulta para análisis de mensajes de datos adquiridos de dispositivos móviles
Aplicación	UFED Reader	Consulta para análisis de mensajes de datos adquiridos de dispositivos móviles

Tabla 18 Descripción Herramientas Forenses

5.4 INVESTIGACIÓN

5.4.1 GESTIONAR LAS INVESTIGACIONES

La actividad de GESTIONAR LAS INVESTIGACIONES se desarrolla actualmente a partir de la puesta a disposición de los mensajes de datos, esta actividad está compuesta por las tareas que se relacionan a continuación:

ID TAREA	NOMBRE DE LA TAREA	DESCRIPCIÓN	ARTEFACTOS FORMATOS EVIDENCIAS
1	Pre investigación	Evaluar las interacciones entre los actores del caso	
2	Selección de grupo de información por niveles de relevancia	Seleccionar la información de acuerdo a su nivel de importancia	
3	Selección de técnicas de búsqueda para mejorar la eficiencia de las mismas	Escoger técnicas de búsquedas que faciliten los hallazgos	
|4	Selección de mensajes de datos finales	Seleccionar los objetos que muestren tendencias para convertirse en hallazgos.	
5	Revisión de caso	Para identificar posibles actores a tener en cuenta dentro de la investigación, se realiza un seguimiento a la información mediática del caso.	
6	Formato metodología de investigación	En conjunto con el líder investigativo del caso, mediante el diligenciamiento del formato: Metodología investigación creación de etiquetas en Summation, se reconstruye los hechos y se identifican personas y se generan hipótesis muchas más acertadas respecto al caso objeto de investigación.	
7	Personas de interés	Personas naturales o jurídicas que surgen como agentes relevantes en el caso y que facilita la reconstrucción de los hechos en el mismo.	
8	Creación de etiquetas y filtrado de información	método que canaliza todos los agentes, personas y factores investigados en etiquetas para posibilitar la segregación y fácil inspección de la información	
9	Creación de la lista de investigación	Documento que contiene los agentes participantes en la conducta, actividad o tarea investigada y la relación que tienen directa o indirectamente sobre la misma	
10	Refuerzo de búsquedas:	Búsqueda de parámetros adicionales para recrear los agentes terceros que posiblemente tengan incidencia sobre la información investigada	
11	Línea de tiempo	Relación cronológica de los hechos, eventos e incidentes investigados para visualizar, contextualizar y facilitar la reconstrucción del caso.	
12	Revisión sobre las etiqueta creada previamente y las que se van creando en Summation	Depuración de la información revisada y posibles nuevos parámetros de búsqueda junto con los agentes relevantes en la investigación.	
13	APERTURA	Adquisición de los elementos pertenecientes a las imágenes forenses recolectadas los cuales contienen	

ID TAREA	NOMBRE DE LA TAREA	DESCRIPCIÓN	ARTEFACTOS FORMATOS EVIDENCIAS
		la información necesaria para demostrar una conducta ilegal	

Tabla 19 Flujo de Gestionar las Investigaciones

5.5 ATENDER SOLICITUDES COMPLEMENTARIAS

5.5.1 SOLICITUDES COMPLEMENTARIAS

5.5.1.1 Copia de Contenedores de Evidencias Digitales

La secuencia de Copiar información en contenedor está compuesta por las tareas que se relacionan a continuación:

ID TAREA	NOMBRE DE LA TAREA	DESCRIPCIÓN	ARTEFACTOS FORMATOS EVIDENCIAS
1	Analizar contenedor Origen mediante herramienta Forense	Ejecutar Software Forense que permita obtener información del Dispositivo contenedor de evidencia digital	SOFTWARE TREE-SIZE
2	Identificar información de contenedor origen	Identificar tamaño de carpetas, subcarpetas, cantidad de archivos. Identificar Serial Lógico y Físico del dispositivo contenedor de evidencia digital.	
3	Gestionar dispositivo de destino valorando el tamaño de la evidencia	Para más detalle ver **SELECCIÓN DE CONTENEDOR DE DESTINO**	
4	Ejecutar Software LIRIS	Ejecutar LIRIS Ingresar los datos solicitados por la herramienta. Ajustar la herramienta de acuerdo al tipo de método que se desea realizar.	
5	Revisar GS04-F05 Formato de Informe de Copia generado por LIRIS	Validar que no se hayan presentado errores en los registros que genera la herramienta LIRIS	
6	Ajustar herramienta de copia en modo Diff/Size	En caso de que se evidencian errores en los registros es necesario ajustar la herramienta LIRIS en modo Diff/Size Ejecutar LIRIS nuevamente. Validar nuevamente que no se presenten errores en los registros que genera la herramienta LIRIS	
7	Analizar contenedor Destino	Ejecutar Software Forense que permita obtener información técnica del Dispositivo contenedor de evidencia digital	

ID TAREA	NOMBRE DE LA TAREA	DESCRIPCIÓN	ARTEFACTOS FORMATOS EVIDENCIAS
	mediante herramienta forense		
8	Diligenciar Rótulo	Imprimir y diligenciar formato de RÓTULO con la información del contenedor destino	RÓTULO
9	Diligenciar 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	Anexo Digital Copia	Seleccionar información Técnica Imprimir Información Técnica Realizar Imagen Forense de información Técnica Almacenar en dispositivo óptico sin escritura información técnica con su respectiva Imagen Forense Almacenar en dispositivo óptico utilizado previamente la nueva información técnica con su respectiva Imagen Forense Para más detalle ver **ANEXO DIGITALCOPIA**	
11	Diligenciar GS04-F04 Formato testigo documental de contenedor de evidencia digital ubicado fuera de expediente	Para el caso de los Discos Duros y la USB, Imprimir y diligenciar formato GS04-F04 Formato testigo documental de contenedor de evidencia digital ubicado fuera de expediente para indicar el lugar en donde se va almacenar el contenedor de evidencia digital	GS04-F04 Formato testigo documental de contenedor de evidencia digital ubicado fuera de expediente
12	Elaboración de acta	Se realiza la elaboración del acta donde se registra los pasos, herramientas y métodos usados para la actividad.	ACTA DE COPIA DE CONTENEDORES DE EVIDENCIA DIGITAL Y CONTENEDOR (CD/DVD/BR,/USB/ DD)

Tabla 20 Flujo de Copiar información en contenedores

5.5.1.2 Preservación de Páginas Web

ID TAREA	NOMBRE DE LA TAREA	DESCRIPCIÓN	ARTEFACTOS FORMATOS EVIDENCIAS
1	Instalar Software	Instalación de herramientas de preservación.	
2	Iniciar descarga sitio Web	Descargar sitio web mediante herramienta de preservación	
3	Validar requerimiento	Dependiendo de la solicitud se verifican y documentan los puntos del requerimiento.	

ID TAREA	NOMBRE DE LA TAREA	DESCRIPCIÓN	ARTEFACTOS FORMATOS EVIDENCIAS
4	Herramientas web: - Borderware - Symanter - Borderware - RUES - Ultratools - Virus total - SSL Checker	• Incluir geolocalización. • Categoría del sitio web. • Reputación. • Rúes de la empresa responsable. • Información del dominio. • Revisión del virus. • Revisión de seguridad, verificar certificados	
5	Otros	Documentos, imágenes, capturas de pantalla, videos, etc.	
6	Adquisición de imagen	• Generar imagen de carpeta con sitio Web. • Generar imagen de consultas Web • Generar imagen de otros. La imagen forense se almacenara en un contendor de evidencia (CD/DVD/BR,/USB/DD)	
7	Diligenciar Rótulo	Imprimir y diligenciar formato de RÓTULO con la información del contenedor destino	RÓTULO
7	Diligenciar 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
8	Anexo Digital Copia	Seleccionar información Técnica Imprimir Información Técnica Realizar Imagen Forense de información Técnica Almacenar en dispositivo óptico sin escritura información técnica con su respectiva Imagen Forense Almacenar en dispositivo óptico utilizado previamente la nueva información técnica con su respectiva Imagen Forense Para más detalle ver **ANEXO DIGITALCOPIA**	
9	Diligenciar GS04-F04 Formato testigo documental de contenedor de evidencia digital ubicado fuera de expediente	Para el caso de los Discos Duros y la USB, Imprimir y diligenciar formato de GS04-F04 Formato testigo documental de contenedor de evidencia digital ubicado fuera de expediente para indicar el lugar en donde se va almacenar el contenedor de evidencia digital	GS04-F04 Formato testigo documental de contenedor de evidencia digital ubicado fuera de expediente
10	Elaboración de acta	Se realiza la elaboración del acta donde se registra los pasos, herramientas y métodos usados para la actividad.	ACTA DE PRESERVACION DE PÁGINAS WEB Y CONTENEDOR

ID TAREA	NOMBRE DE LA TAREA	DESCRIPCIÓN	ARTEFACTOS FORMATOS EVIDENCIAS
			(CD/DVD/BR,/USB/DD)

Tabla 21 Flujo de Preservación Pagina Web

5.5.1.3 Informe Técnico

ID TAREA	NOMBRE DE LA TAREA	DESCRIPCIÓN	ARTEFACTOS FORMATOS EVIDENCIAS
1	Analizar contenedor Origen mediante herramienta Forense	Ejecutar Software Forense que permita obtener información del Dispositivo contenedor de evidencia digital	SOFTWARE TREE-SIZE
2	Identificar información de contenedor origen	Identificar tamaño de carpetas, subcarpetas, cantidad de archivos. Identificar Serial Lógico y Físico del dispositivo contenedor de evidencia digital.	Identificar información de contenedor origen
3	Analizar contenedor Origen mediante herramienta Forense	Realizar la navegación en el Dispositivo Contenedor de Evidenica Digtal	FTK IMAGER
4	Identificar información de contenedor origen	Identificar tamaño de carpetas, subcarpetas, cantidad de archivos del dispositivo contenedor de evidencia digital.	Identificar información de contenedor origen
5	Herramienta de Windows	Vista preliminar de Dispositivos y Unidades de Windows para determinar la unidad conectada	Símbolo del sistema CMD
6	Identificar información de contenedor origen	Identificar tamaño de carpetas, subcarpetas, cantidad de archivos. Identificar Serial Lógico y Físico del dispositivo contenedor de evidencia digital.	Identificar información de contenedor origen
7	Elaboración de acta	Se realiza la elaboración del acta donde se registra los pasos, herramientas y métodos usados para la actividad.	ACTA DE ***INFORME TÉCNICO***

Tabla 22 Flujo de ***Informe Técnico***

5.5.1.4 Traslado de Contenedores de Evidencias Digitales.

ID TAREA	NOMBRE DE LA TAREA	DESCRIPCIÓN	ARTEFACTOS FORMATOS EVIDENCIAS
1	Analizar contenedor Origen mediante herramienta Forense	Ejecutar Software Forense que permita obtener información del Dispositivo contenedor de evidencia digital	SOFTWARE TREE-SIZE

ID TAREA	NOMBRE DE LA TAREA	DESCRIPCIÓN	ARTEFACTOS FORMATOS EVIDENCIAS
2	Identificar información de contenedor origen	Identificar tamaño de carpetas, subcarpetas, cantidad de archivos. Identificar Serial Lógico y Físico del dispositivo contenedor de evidencia digital.	• FTK IMAGER
3	Gestionar dispositivo de destino valorando el tamaño de la evidencia	Para más detalle ver **SELECCIÓN DE CONTENEDOR DE DESTINO**	
4	Ejecutar Software LIRIS	Ejecutar LIRIS Ingresar los datos solicitados por la herramienta. Ajustar la herramienta de acuerdo al tipo de método que se desea realizar (Numero de radicado al cual se va a trasladar)	
5	Revisar GS04-F05 Formato de Informe de Copia generado por LIRIS	Validar que no se hayan presentado errores en los registros que genera la herramienta LIRIS	
6	Ajustar herramienta de copia en modo Diff/Size	En caso de que se evidencian errores en los registros es necesario ajustar la herramienta LIRIS en modo Diff/Size Ejecutar LIRIS nuevamente. Validar nuevamente que no se presenten errores en los registros que genera la herramienta LIRIS	
7	Analizar contenedor Destino mediante herramienta forense	Ejecutar Software Forense que permita obtener información técnica del Dispositivo contenedor de evidencia digital	
8	Diligenciar Rótulo	Imprimir y diligenciar formato de RÓTULO con la información del contenedor destino	RÓTULO
9	Diligenciar GS04-F01 Registro Cadena de Custodia a 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	Anexo Digital Copia	Seleccionar información Técnica Imprimir Información Técnica Realizar Imagen Forense de información Técnica Almacenar en dispositivo óptico sin escritura información técnica con su respectiva Imagen Forense Almacenar en dispositivo óptico utilizado previamente la nueva información técnica con su respectiva Imagen Forense Para más detalle ver **ANEXO DIGITALCOPIA**	
11	Diligenciar GS04-F04 Formato testigo documental de contenedor de evidencia digital	Para el caso de los Discos Duros y la USB, Imprimir y diligenciar formato de GS04-F04 Formato testigo documental de contenedor de evidencia digital ubicado fuera de expediente para indicar el lugar en donde se va almacenar el contenedor de evidencia digital	GS04-F04 Formato testigo documental de contenedor de evidencia digital

ID TAREA	NOMBRE DE LA TAREA	DESCRIPCIÓN	ARTEFACTOS FORMATOS EVIDENCIAS
	ubicado fuera de expediente		ubicado fuera de expediente
12	Elaboración de acta	Se realiza la elaboración del acta donde se registra los pasos, herramientas y métodos usados para la actividad.	ACTA DE TRASLADO DE CONTENEDORES DE EVIDENCIA DIGITAL Y , CONTENEDOR (CD/DVD/BR,/USB/DD)

Tabla 23 Flujo de Traslado de Contenedores de Evidencias Digitales

5.5.1.5 Depuración de Mensajes de Datos.

ID TAREA	NOMBRE DE LA TAREA	DESCRIPCIÓN	ARTEFACTOS FORMATOS EVIDENCIAS
1	Recibir requerimiento y asignar analista encargado	El área o dependencia envía la autorización para atender el requerimiento.	Respuesta indicando la atención de la solicitud.
2	Verificar documentación y contenedor final	Validar la información del caso (nombre, radicado), tipo de contenedor,	
3	Verificar Tabla de relación de discos duros guardados en el cuarto de evidencias	Identificar la ubicación del contenedor	DOCUMENTO Tabla de relación de discos duros.xls
4	Retirar Dispositivo y Solicitar GS04-F01 Registro Cadena de Custodia correspondiente	Si se encuentra Almacenado en cuarto de evidencias retirar dispositivo y Solicitar GS04-F01 Registro Cadena de Custodia correspondiente	
5	Entregar GS04-F01 Registro Cadena de Custodia	La dependencia entrega el GS04-F01 Registro Cadena de Custodia	GS04-F01 Registro Cadena de Custodia
6	Realizar GS04-F01 Registro Cadena de Custodia	Realizar anotación en GS04-F01 Registro Cadena de Custodia	GS04-F01 Registro Cadena de Custodia
7	Solicitar la revisión del expediente para identificar el contenedor de evidencia digital	Si el contenedor no se encuentra almacenado en el cuarto de evidencias, se solicita a la dependencia encargada del caso la revisión del expediente.	Expediente del caso

ID TAREA	NOMBRE DE LA TAREA	DESCRIPCIÓN	ARTEFACTOS FORMATOS EVIDENCIAS
8	Entregar el medio contenedor de evidencia digital alojado en el expediente.	Si el contenedor no se encuentra almacenado en el cuarto de evidencias, la dependencia entrega el medio contenedor con su respectiva GS04-F01 Registro Cadena de Custodia	Expediente Medio contenedor de evidencia digital
9	Recibir medio Contenedor	Si el contenedor no se encuentra almacenado en el cuarto de evidencias, el servidor público o contratista LIF recibe el medio contenedor de evidencia digital	
10	Realizar Registro en GS04-F01 Registro Cadena de Custodia	Cuando el servidor público y/o contratista tiene en su poder el medio contenedor de evidencia digital debe realizar anotación en GS04-F01 Registro Cadena de Custodia	
11	identificar información en herramienta forense	Una vez se verifique que la información se encuentre adecuadamente procesada es necesario identificar los ítems que se necesiten filtrar.	FTK LAB
12	Generar etiqueta con la información requerida	Cada uno de estos ítems debe ser almacenado en una o varias etiquetas dependiendo del tipo de solicitud	
13	Generar Imagen Derivada de la información requerida en dispositivo forense	Cuando cuente con la autorización del borrado seguro, el servidor público o contratista asignado para efectuar la actividad de filtrado genera la imagen derivada de la información requerida	FTK LAB STAND ALONE
14	Autorizar Borrado Seguro Contenedor Origen	Una vez los ítems se encuentren almacenados en la(s) etiqueta(s) se debe solicitar la revisión al abogado asignado por la dependencia solicitante.	
15	Borrado Seguro en Contenedor Origen	Realizar borrado seguro mediante software forense, para más detalle ver **BORRADO SEGURO**	ENCASE
16	Diligenciar 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 elementos de imagen derivada en contenedor origen	
18	Diligenciar GS04-F01 Registro Cadena de Custodia del contenedor origen	Informar del almacenamiento de la imagen derivada en la GS04-F01 Registro Cadena de Custodia del contenedor origen.	GS04-F01 Registro Cadena de Custodia
19	Elaboración de acta	Se realiza la elaboración del acta donde se registra los pasos, herramientas y métodos usados para la actividad.	ACTA DE DEPURACION DE MENSAJES

ID TAREA	NOMBRE DE LA TAREA	DESCRIPCIÓN	ARTEFACTOS FORMATOS EVIDENCIAS
			DE DATOS Y , CONTENEDOR (CD/DVD/BR,/USB/DD)

Tabla 24 Flujo de Depuración de Mensajes de Datos

5.5.1.6 Exportación de Elementos de Evidencia Digital

ID TAREA	NOMBRE DE LA TAREA	DESCRIPCIÓN	ARTEFACTOS FORMATOS EVIDENCIAS
1	Recibir requerimiento y asignar analista encargado	El área o dependencia envía la autorización para atender el requerimiento.	Respuesta indicando la atención de la solicitud.
2	Verificar documentación y contenedor final	Validar la información del caso (nombre, radicado), tipo de contenedor,	
3	identificar información en herramienta forense	Una vez se verifique que la información se encuentre adecuadamente procesada es necesario identificar los ítems que se necesiten filtrar.	FTK LAB
4	Generar etiqueta con la información requerida	Cada uno de estos ítems debe ser almacenado en una o varias etiquetas dependiendo del tipo de solicitud	
5	Explotar y Generar Imagen Derivada de la información requerida en dispositivo forense	Se genera la exportación de los elementos de evidencia digital y posterior se genera la imagen derivada la cual se almacenara en un contendor de evidencia (CD, DVD, BR, USB, DD)	FTK LAB
6	Diligenciar 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	GS04-F01 Registro Cadena de Custodia
8	Elaboración de acta	Se realiza la elaboración del acta donde se registra los pasos, herramientas y métodos usados para la actividad.	ACTA DE EXPORTACION DE ELEMENTOS DE EVIDENCIAS DIGITALES Y , CONTENEDOR (CD/DVD/BR,/USB/DD)

Tabla 25 Flujo de Exportación de Elementos de Evidencia Digital

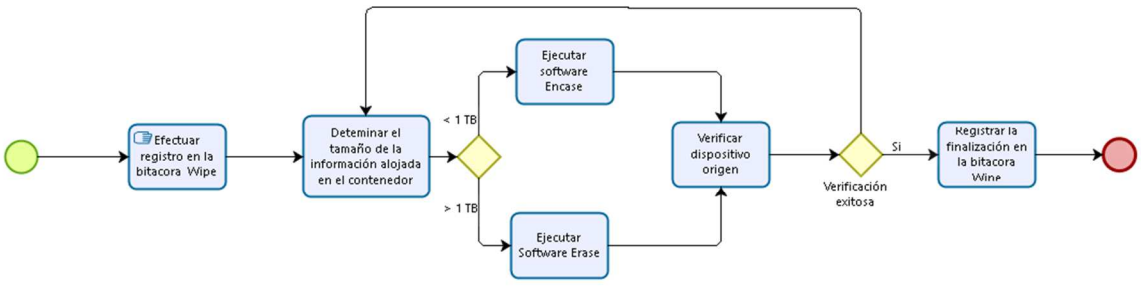
5.5.1.7 Realizar Unificación en Cascada

ID TAREA	NOMBRE DE LA TAREA	DESCRIPCIÓN	ARTEFACTOS FORMATOS EVIDENCIAS
1	Identificar Cantidad de contenedores origen	Verificar la cantidad de contenedores origen a los cuales practicarles la unificación en cascada.	
2	Identificar el contenedor origen con el menor tamaño	Verificar el tamaño de los contenedores origen con el objeto de determinar el contenedor con el menor tamaño.	
3	Identificar el contenedor origen con el mayor tamaño	Verificar el tamaño de los contenedores origen con el objeto de determinar el contenedor con el mayor tamaño.	
4	Seleccionar contenedor origen con mayor tamaño como contenedor Temporal de destino	Una vez identificado el contenedor con el mayor tamaño, se emplea como contenedor temporal de destino, de este modo será posible transferir la información de los contenedores origen a un contenedor temporal de destino.	
5	Analizar contenedor Destino mediante Tree-Size	Ejecutar Software Forense que permita obtener información del Dispositivo contenedor de evidencia digital	
6	Analizar contenedor Origen mediante Tree-Size	Ejecutar Software Forense que permita obtener información del Dispositivo contenedor de evidencia digital	
7	Ejecutar Software LIRIS	Ejecutar LIRIS Ingresar los datos solicitados por la herramienta. Ajustar la herramienta de acuerdo al tipo de método que se desea realizar.	
8	Revisar GS04-F05 Formato de Informe de Copia generado por LIRIS	Validar que no se hayan presentado errores en los registros que genera la herramienta LIRIS	
9	Realizar anotación en GS04-F01 Registro Cadena de Custodia de contenedor destino informando que se agrega la información del contenedor de Origen	Diligenciar GS04-F01 Registro Cadena de Custodia de contenedor destino con la novedad de la adición de evidencia del contenedor origen	
10	Analizar contenedor Destino mediante herramienta forense	Ejecutar Software Forense que permita obtener información técnica del Dispositivo contenedor de evidencia digital	
11	Ajustar herramienta en modo Diff/Size	En caso de que se evidencien errores en los registros es necesario ajustar la herramienta LIRIS en modo Diff/Size Ejecutar LIRIS nuevamente. Validar nuevamente que no se presenten errores en los registros que genera la herramienta LIRIS	
12	Realizar anotación en GS04-F01 Registro Cadena de Custodia de disco Origen informando el cambio	Diligenciar GS04-F01 Registro Cadena de Custodia de contenedor origen con la novedad de la adición de evidencia del contenedor origen	

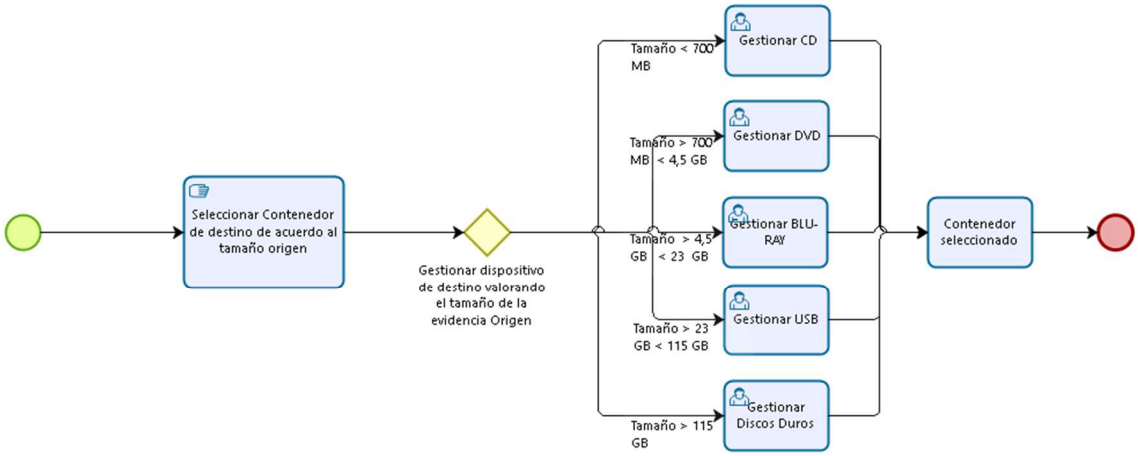
ID TAREA	NOMBRE DE LA TAREA	DESCRIPCIÓN	ARTEFACTOS FORMATOS EVIDENCIAS
	de contenedor a disco de Destino		
13	Borrado Seguro en Contenedor Origen	Realizar **BORRADO SEGURO**	
14	Anexo Digital Unificación	Seleccionar información Técnica Imprimir Información Técnica Realizar Imagen Forense de información Técnica Almacenar en dispositivo óptico sin escritura información técnica con su respectiva Imagen Forense Almacenar en dispositivo óptico utilizado previamente la nueva información técnica con su respectiva Imagen Forense Para más detalle ver ANEXO DIGITAL COPIA	

Tabla 26 Flujo de Unificación en Cascada

5.5.1.8 Borrado Seguro



5.5.1.9 Selección de Contenedor de Destino

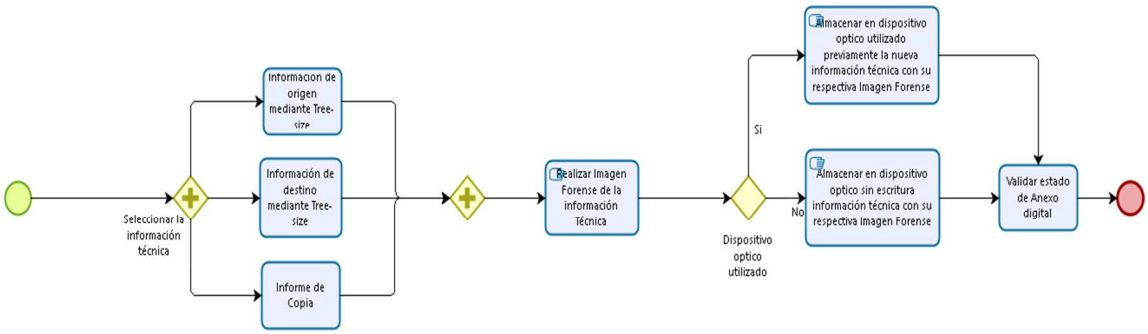


5.5.1.10 Anexo Digital Copia

ID TAREA	NOMBRE DE LA TAREA	DESCRIPCIÓN	ARTEFACTOS FORMATOS EVIDENCIAS
1	Seleccionar información Técnica	Seleccionar la información de origen que entrega el software treesize Seleccionar la información de destino que entrega el software treesize Adjunta GS04-F05 Formato de Informe de Copia	Treesize
2	Imprimir Información Técnica	Imprimir la documentación técnica para anexar a la entrega.	
3	Realizar Imagen Forense de información Técnica	Realizar imagen forense de la documentación técnica	FTK IMAGER
4	Almacenar en dispositivo óptico sin escritura información técnica con su respectiva Imagen Forense	Almacenar en CD o Blu-Ray sin escritura la información técnica.	
5	Almacenar en dispositivo óptico utilizado previamente la nueva información técnica con su respectiva Imagen Forense	Almacenar en el CD o Blu-Ray sin escritura la Imagen Forense	CD o Blu-Ray

Tabla 27 Flujo de Anexo Digital Copia

5.5.1.11 Anexo Digita Unificación



5.6 CUSTODIAR MATERIAL PROBATORIO

El servidor público y contratista designado para la administración del cuarto de evidencias debe asegurarse de que todos los dispositivos que van a ingresar al cuarto de evidencias se encuentren empacados adecuadamente y cuenten con rótulo sobre su envoltura.

El almacenamiento de los dispositivos contenedores de evidencia digital se efectuará por número de radicado en orden ascendente. Si hay más de un contenedor con mismo número de radicado se organizan por orden alfabético del nombre de la empresa.

Los préstamos de dispositivos contenedores de evidencia digital deben contar con la autorización de los coordinadores del caso. Una vez se cuente con la autorización del caso servidor público y contratista designado para la administración del cuarto de evidencias debe realizar la búsqueda del dispositivo contenedor de evidencias para entrega del dispositivo en calidad de préstamo bajo su acompañamiento.

5.6.1 CUSTODIA

La custodia de la información inicia en la etapa de Adquisición de la modelo ATI del cuando se hace apertura al GS04-F01 Registro Cadena de Custodia con los elementos necesarios para la identificación del dispositivo contenedor de evidencia digital, tipo de dispositivo, modo de embalar, personas que intervinieron en la recolección de información y las debidas anotaciones. Esta actividad se denomina anclaje del dispositivo de información con el GS04-F01 Registro Cadena de Custodia.

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	Actividad en la que se relacionan los datos de identificación del contenedor de evidencia digital tales como: Hora, fecha, tipo de dispositivo, capacidad de almacenamiento, personas que intervienen en la recolecciones información	GS04-F01 Registro Cadena de Custodia anterior
2	Registro en GS04-F01 Registro Cadena de Custodia	Realizar la anotación correspondiente al transporte de la evidencia hacia la SIC	GS04-F01 Registro Cadena de Custodia posterior
3	Contenedor de evidencia digital y GS04-F01 Registro Cadena de Custodia	Entrega del dispositivo contenedor evidencia digital al custodio de la información.	GS04-F01 Registro Cadena de Custodia posterior
4	Contenedor de evidencia digital y GS04-F01 Registro Cadena de Custodia	Verificar la GS04-F01 Registro Cadena de Custodia con los datos de identificación del dispositivo de evidencia digital.	GS04-F01 Registro Cadena de Custodia posterior
5	Contenedor de evidencia digital y GS04-F01 Registro Cadena de Custodia	Registrar la ubicación del contenedor de evidencia digital, número de radicado, empresa, tipo de dispositivo, marca, serial físico, serial lógico, capacidad y volumen ocupado.	Inventario de dispositivos almacenados en cuarto de evidencias/cajja fuerte
6	Contenedor de evidencia digital y GS04-F01 Registro Cadena de Custodia	Almacenar el dispositivo contenedor de evidencia digital en el cuarto de evidencias y/o caja fuerte.	GS04-F01 Registro Cadena de Custodia con la anotación de la custodia en el cuarto de evidencias

Tabla 28 Flujo de Custodia

5.6.2 ACTIVIDADES PARA EL MANEJO DE EVIDENCIAS

El manejo de las evidencias permite definir lineamientos referentes al manejo de la información contenida tanto en los contenedores de evidencia digital, para tal efecto siempre se requiere una solicitud de aprobación por parte de los coordinadores, delegados y/o jefes de área en caso de requerir algún tipo de acceso a las evidencias con los datos de número de caso, tipo de evidencia.

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

5.6.2.1 Flujo del Manejo de Evidencias

Las acciones del manejo de evidencias es cumplir con las medidas de seguridad requeridas para garantizar la integridad, disponibilidad y confidencialidad de la información custodiada por el GTIFSD.

Para evidenciar la trazabilidad del manejo de evidencias se cuenta con el GS04-F01 Registro Cadena de Custodia el cual permite tener un seguimiento de cada una de las acciones a las que esté sujeta la evidencia digital, por tal motivo se debe hacer la anotación correspondiente.

ID TAREA	NOMBRE DE LA TAREA	DESCRIPCIÓN	ARTEFACTOS FORMATOS EVIDENCIAS
1	Solicitud para actividad	Recibir solicitud con previa autorización de coordinadores, delegados y/o jefes de área y entidades de vigilancia y control.	Correo electrónico de la solicitud
2	Autorización de coordinadores, delegados y/o jefes de área	Comprobar autorización por parte de coordinadores, delegados y/o jefes de área y datos del contenedor de evidencia digital	
3	Identificación del dispositivo contenido de evidencia	Identificación de 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 su almacenamiento	Contenedor de evidencia digital
5	Préstamo del contenedor de evidencia digital	Préstamo del dispositivo contenedor de evidencia al servidor público y/o contratista del GTIFSD para que realice su actividad. Para las entidades de vigilancia y control se realizar un acompañamiento durante la actividad.	Entrega del contenedor de evidencia y anotación en GS04-F01 Registro Cadena de Custodia
6	Comprobar herramientas usada para la actividad	Supervisar el método para las entidades de vigilancia y control con la finalidad de garantizar la integridad inalterabilidad de la información.	Correo electrónico con observaciones de la supervisión
7	Asegurar que el método es realizado adecuadamente	Confirmar que el método realizado por el servidor público y/o contratista del GTIFSD cumpla con los lineamientos	GS04-F01 Registro Cadena de Custodia

		establecidos y se realice la anotación del método en la GS04-F01 Registro Cadena de Custodia	con el registro de la actividad
8	Revisión física del contenedor de evidencia digital	Recibir el contendor de evidencia digital, embalado y con su respectiva GS04-F01 Registro Cadena de Custodia, se debe realizar anotación de la custodia	GS04-F01 Registro Cadena de Custodia con anotación

Tabla 29 Flujo de cuarto de evidencias/caja fuerte

6 DOCUMENTOS RELACIONADOS

GS04-P01 Procedimiento de Acompañamiento de Visitas y Solicitudes de Informática Forense
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

7 RESUMEN CAMBIOS RESPECTO A LA ANTERIOR VERSIÓN

Se modifica el nombre del formato GS04-F09 y se sustituye la palabra "peritaje" por "Informe Técnico"

Fin documento