Superintendencia de Sociedades

PROCEDIMIENTO
EXTRACCIÓN DE EVIDENCIA DIGITAL

1 OBJETIVO

Establecer las actividades a realizar en la toma de evidencia digital, para los procesos de las diferentes delegaturas de la Superintendencia de Sociedades, que tienen a su cargo funciones de investigación

2 ALCANCE

El procedimiento incluye la solicitud de acompañamiento a la visita, la extracción de imágenes forenses, su custodia durante la visita y la entrega de las evidencias tomadas a la bodega de evidencias digitales

3 DEFINICIONES

Dispositivo o medio de almacenamiento de información digital: Es un medio o elemento que permite almacenar información en formato digital tal como discos duros, memorias, DVDs entre otros.

DVD (*digital versatile disc*): Es un formato y soporte de almacenamiento óptico, están codificados con formato distinto y capacidad mayor a la de un disco compacto, cerca de siete veces.

EMP: Elemento Material Probatorio, son los documentos de toda índole hallados en diligencia investigativa de inspección o que han sido entregados voluntariamente por quien los tenía en su poder o que han sido abandonados allí. Involucra entre otros:

- Materiales obtenidos mediante grabación, filmación, fotografía, video o cualquier otro medio avanzado, utilizados como cámaras de vigilancia, en recinto cerrado o en espacio público.
- Mensajes de datos, como el intercambio electrónico de datos, internet, correo electrónico, telegrama, télex, telefax o similar, regulados por la Ley 527 de 1999 o las normas que la sustituyan, adicionen o reformen.

Evidencia digital: También conocida como evidencia computacional son:

- Registros o archivos generados por computador u otro medio equivalente;
- Registros o archivos no generados sino simplemente almacenados en computadores o medios equivalentes; y
- Registros o archivos híbridos, que incluyen tanto registros generados por computador o medio equivalente, como almacenados en los mismos.

FAT (*File Allocation Table*)**:** Tabla de asignación de archivos; es un sistema de archivos desarrollado para MS-DOS, así como el sistema de archivos principal de las ediciones no empresariales de Microsoft Windows en diferentes versiones.

HASH: En informática, HASH se refiere a una función o método para generar claves o llaves que representen de manera casi unívoca a un documento, registro, archivo, etc., resumir o identificar un dato a través de la probabilidad, utilizando una función HASH o algoritmo HASH. Un HASH es el resultado de dicha función o algoritmo.

Imagen forense: Es una copia idéntica (bit a bit) de un dispositivo de almacenamiento, tanto del área ocupada como del área libre, realizada a través de software y/o equipos especializados que realizan automáticamente rutinas de comprobación y verificación de la imagen, lo que garantiza su exactitud.

Indexación: Proceso por medio del cual se extrae información legible de una copia digital; esta información puede indexarse por medio de palabras claves. La indexación se realiza por medio de herramientas especializadas (*Forensic Tools Kit – FTK*).

Informática forense: Es la ciencia de la informática que permite el proceso de identificación, preservación, análisis y presentación de evidencias digitales en una forma que sea legalmente aceptable en cualquier proceso judicial o administrativo.

MD5 (*Message-DigestAlgorithm 5* o Algoritmo de Resumen de Mensaje 5)**:** En criptografía, MD5 es un algoritmo de reducción criptográfico HASH de 128 bits ampliamente usado, representado en 32 caracteres hexadecimales, comúnmente conocido como huella digital de un archivo, dato o medio de almacenamiento de información, que identifica un archivo o mensaje de datos.

NTFS (*New Technology File System*): es un sistema de archivos de Windows NT incluido en las versiones de Windows 2000, Windows XP, Windows Server 2003, Windows Server 2008, Windows Vista, Windows 7 y Windows 8.

PARTICIÓN: es el nombre genérico que recibe cada división presente en una sola unidad física de almacenamiento de datos. Toda partición tiene su propio sistema de archivos (formato); generalmente, casi cualquier sistema operativo interpreta, utiliza y manipula cada partición como un disco físico independiente, a pesar de que dichas particiones estén en un solo disco físico.

SHA1 (*Secure Hash Algorithm* o Algoritmo de Hash Seguro): es una familia de funciones hash de cifrado, publicadas por el Instituto Nacional de Estándares y Tecnología (NIST). La primera versión del algoritmo fue creada en 1993 con el nombre de SHA, aunque en la actualidad se la conoce como SHA-0, para evitar confusiones con las versiones posteriores. La segunda versión del sistema, publicada con el nombre de SHA-1, fue publicada dos años más tarde. Posteriormente se han publicado SHA-2 en 2001 (formada por diversas funciones: SHA-224, SHA-256, SHA-384, y SHA-512) y la más reciente SHA-3, que fue seleccionada en una competición de funciones hash celebrada por el NIST en 2012.

Software: Es el conjunto de los programas de cómputo, procedimientos, reglas, documentación y datos asociados que forman parte de las operaciones de un sistema de computación. Considerando esta definición, el concepto de software va más allá de los programas de computación en sus distintos estados: código fuente, binario o ejecutable; también su documentación, los datos a procesar e incluso la información de usuario forman parte del software: es decir, abarca todo lo intangible, todo lo «no físico» relacionado.

Unidad Lógica: Dispositivo de almacenamiento de información creado por el sistema operativo u otro software, éste último es responsable de mapear las operaciones en la unidad lógica en una o más operaciones, en una o más unidades físicas (equipamiento, hardware). Una unidad física puede está dividida en varias unidades lógicas.

4 DOCUMENTOS DE REFERENCIA

- GC-PO-001 Documento de Políticas del SGI
- GC-MO-001 Documento de Modelos del SGI
- GTI-FM-016 Formato de extracción de evidencias forenses
- GTI-FM-017 Cadena de Custodia

5 CONDICIONES GENERALES

5.1 La informática forense es una ciencia que permite presentar apropiadamente las evidencias digitales, de tal manera que conserven su valor probatorio. Para realizar el examen se aplican técnicas de la informática forense, cuya finalidad es asegurar los principios de:

- Confidencialidad: Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.
- Disponibilidad: Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada.
- Integridad: Propiedad de salvaguardar la exactitud y estado completo de la información.

5.2 Para efectos de los procedimientos para la recolección y gestión de información de uso forense, los roles se denominan:

- ANALISTAS FORENSES: Los profesionales de las delegaturas asignados a las visitas;
- COORDINADOR DE LA VISITA FORENSE: Analista forense responsable de conducir la visita;
- TÉCNICOS FORENSES*:* Profesionales en sistemas y carreras afines con formación en informática y experiencia en técnicas forenses, asignados a los procedimientos de Extracción de evidencia digital e Indexación y procesamiento de la información;
- RESPONSABLE DE LA BODEGA DE EVIDENCIAS Y ELEMENTOS FORENSES: Profesional responsable de administrar la bodega de evidencias y elementos forenses (recibir, entregar y custodiar las evidencias digitales capturadas, así como los elementos tecnológicos para las tomas de información e indexación de información) y articular las actividades de extracción e indexación de evidencia forense. El responsable será determinado por la Coordinación del Grupo de Seguridad e Informática Forense.

5.3 Para la extracción, el procesamiento, la indexación y la organización de información para los analistas forenses, la Superintendencia de Sociedades deberá contar con los elementos técnicos y las capacidades requeridas. Los recursos empleados para el presente procedimiento son:

- Equipo forense: elementos tecnológicos disponibles para el procesamiento de evidencia digital (extracción, almacenamiento e indexación de datos)
- Software forense: programas de computador utilizados para realizar el tratamiento de los datos recolectados (indexación y preparación de datos para los analistas forenses)

- Elementos de empaque y sellamiento seguro: bolsas de burbujas antiestáticas con cierre adhesivo, cintas especiales para sellamiento de áreas, entre otros
- Otras herramientas de software/hardware, las cuales deben estar en adecuado estado de funcionamiento. Para la toma de evidencia forense en las visitas que se adelanten, siempre debe realizarse una imagen forense (bit a bit), mediante el uso de los equipos forenses disponibles en la Superintendencia de Sociedades. Los técnicos forenses asignados no deben realizar copias o manipular la información de los equipos y dispositivos pertenecientes a la entidad evaluada, sino solamente tomar la imagen forense (bit a bit).

5.4. La imagen forense debe estar cifrada con los algoritmos autorizados por entidad, con el fin de reducir el riesgo de pérdida de confidencialidad ante la pérdida o robo de esta.

5.5. La nomenclatura para nombrar las imágenes digitales tomadas es la siguiente:
- Entidad investigada: sigla de la entidad investigada
- Fecha: fecha del día en que se toma la evidencia
- Tipo de dispositivo de almacenamiento: puede ser un medio externo del kit de forense
- Referencia o número de serie del medio de almacenamiento utilizado: consecutivo del medio si se requiere mas de uno

5.7 Durante la visita a entidades investigadas, la custodia de los elementos forenses y de la evidencia digital capturada será responsabilidad única y exclusiva del técnico forense.

5.8 Las herramientas forenses en el proceso de extracción realizan escaneo de virus. En caso de que se detecte alguno, se debe limpiar con la misma herramienta forense, y continuar el proceso de extracción normalmente. En caso de detección de virus se debe anotar en el formato de bitácora. Formato GTI-FM-016 Formato extracción evidencias forenses.doc, en anotaciones.

NOTA: Los procedimientos que se refieren a la recolección y al manejo de evidencias recolectadas en visitas forenses, definen las actividades para realizar la extracción de Evidencia Digital, la preparación de la

información para indexación y procesamiento, así como, la administración de la bodega de evidencias y elementos forenses. Las actividades técnicas forenses se desarrollarán al tenor de lo establecido en el Manual de Cadena de Custodia y del Manual de Bodega de Evidencias vigentes en la fiscalía general de la Nación.

6 PROCEDIMIENTO

No.	Actividad	Responsable	Punto de Control	Registro
	Inicio			
	Asignación de técnicos forenses			
1	El grupo que requiere realizar la toma de información a una sociedad investigada, solicita al responsable de la bodega de evidencias y elementos forenses, la asignación de Técnico(s) Forense(s) para la visita a realizar, indicando lugar y fecha de la visita, número de técnicos forenses requeridos y nombre del coordinador de la visita. Responsable de la bodega de evidencias y elementos forenses remite correo electrónico al(los) funcionario(s) asignado(s) a la visita. El coordinador de la visita citará al(los) técnico(s) forense(s) asignado(s) a una reunión preparatoria de la visita, con el fin de identificar los elementos forenses que serán necesarios para la extracción	Responsable de la bodega de evidencias y elementos forenses Coordinador de la visita		Correos electrónicos
	Extracción de evidencia digital			
2	**Identificación de dispositivos a los cuales se les tomará imagen forense** El coordinador de la visita entregará a los técnicos forenses la lista y los datos correspondientes a los dispositivos que serán objeto de toma de imagen forense (PCs, portátiles, celulares, discos duros externos, CDs, USBs, etc.). El técnico forense identifica físicamente cada dispositivo indicado en la lista	Coordinador de la visita Técnico Forense	X	Lista de dispositivos con identificación Formato

No.	Actividad	Responsable	Punto de Control	Registro
	recibida; para cada dispositivo, el técnico forense diligencia el formato correspondiente, anotando las características del dispositivo y del sitio.			GTI-FM-016 Formato de extracción de evidencias forenses
3	**Ejecución de procesos de generación y extracción de imágenes forenses.** Por cada dispositivo a inspeccionar, el técnico forense realizará las siguientes actividades: - Identificar o rotular el dispositivo - Identificar la herramienta a utilizar - Realizar con el debido cuidado las conexiones entre el dispositivo y los equipos forenses. - Utilizar la herramienta de extracción y ejecutar las instrucciones para realizar imagen forense (bit a bit). - Realizar las anotaciones de las actividades realizadas en la bitácora. Adicionalmente, cuando sea necesario interrumpir la toma de evidencia: El dispositivo en inspección y los elementos forenses deberán asegurarse con las cintas y demás elementos proporcionados para ello, y se dejará anotación de ello en la bitácora. Al reanudar las actividades, el técnico forense revisará, juntamente con los responsables de la institución evaluada, la integridad del sello y de los elementos dejados en la entidad: - Si todo está correcto, se reanuda el proceso de extracción de evidencia. - Si los sellos fueron removidos o alterados o si falta algún elemento	Técnico forense		Formato GTI-FM-016 Formato de extracción de evidencias forenses

No.	Actividad	Responsable	Punto de Control	Registro
	forense, el técnico forense avisará al coordinador de la visita y dejará la anotación en el formato. Hará inventario, dejará acta de los faltantes o de la situación acontecida y dará por terminado el proceso de toma de evidencia digital.			
4	**Autenticación y marcación de las imágenes forenses** Por cada elemento forense utilizado para la extracción de evidencia digital, se debe: 1. Tomar y almacenar la marca o firma *hash* que la herramienta emite de la imagen forense tomada. 2. Marcar la evidencia digital recogida, según nomenclatura adoptada 3. Embalar los elementos forenses con el procedimiento definido y almacenarlas en los contenedores especiales para su transporte. 4. Tomar registro fotográfico de las evidencias antes, durante y al finalizar su embalaje y rotulado. 5. Realizar las anotaciones en el formato	Técnico forense	X	Imágenes de firmas digitales (hash) Formato GTI-FM-016 Formato de extracción de evidencias forenses
5	**Diligenciar formato de cadena de custodia** Una vez tomada la imagen forense con evidencia digital, el técnico forense iniciará la cadena de custodia, realizará los registros respectivos y lo firmará; el formato de cadena de custodia deberá ser adjuntado a la bolsa de la evidencia digital, y acompañar la evidencia hasta su disposición final. Así mismo, deberá realizar las anotaciones específicas de cada actividad realizada, en el formato de extracción de evidencia digital, incluidos los escaneos de virus que puedan haberse realizado.	Técnico forense		GTI-FM-017 Cadena de Custodia Formato GTI-FM-016 Formato de extracción de evidencias forenses

No.	Actividad	Responsable	Punto de Control	Registro
6	**Entrega de evidencia digital a bodega de evidencias y elementos forenses** La evidencia digital debidamente embalada y los elementos forenses utilizados en la toma deberán entregarse a la Bodega de evidencias y elementos forenses, a la mayor brevedad, según procedimiento de Administración de Bodega de evidencias y elementos forenses	Técnico forense		GTI-FM-017 Cadena de Custodia
	Fin			

7. CONTROL DE CAMBIOS

Versión	Fecha	Descripción del Cambio
001	11-07-2018	Creación del documento
002	12-07-2021	Se actualizan nombres de áreas y se incluyen actividades de verificación de virus en los componentes de la plataforma del Laboratorio Forense
003	01-12-2024	Se actualiza el logo de la entidad de acuerdo con las nuevas convenciones del gobierno nacional. En el numeral 2.2 se incluyó en el rol del responsable de la bodega de evidencias y elementos forenses, quien lo asigna.
004	25/04/2025	Se actualiza la plantilla nueva de procedimientos

Elaboró	Revisó	Aprobó
Nombre: Jenny Díaz Cargo: Coordinador Grupo de Seguridad e informática forense Fecha: 20/03/2025	Nombre: Jenny Díaz Cargo: Coordinador Grupo de Seguridad e informática forense Fecha:20/03/2025	Nombre: Ricardo Fernelix Ríos Rosales Cargo: director de Tecnología de la Información y Comunicaciones Fecha:21/04/2025