1. OBJETIVO

Generar una imagen forense de la memoria RAM (Datos Volátiles) sin apagar el dispositivo que permita posteriormente en la fase de análisis “extraer” información valiosa del Sistema Operativo.

2. ALCANCE

Inicia con la notificación del auto de asignación, que hace el Director Nacional de Investigaciones Especiales – DNIE, a los funcionarios para atender la solicitud de apoyo y/o de asesoría técnica; aplicando los modelos y/o metodologías para recolectar datos volátiles y termina con la entrega del informe dando respuesta al auto de asignación.

3. DEFINICIONES Y SIGLAS

COMPUTADOR: Conjunto de software y hardware, el primero consiste en la parte lógica de la computadora (programas, aplicaciones, etc.) el segundo en la parte física (elementos que la forman como Disco Duro, Procesador CPU, Memoria RAM, tarjetas electrónicas de Red, Sonido, Video, etc.). capaz de recibir, procesar y devolver resultados en torno a determinados datos y que para realizar esta tarea cuenta con un medio de entrada y uno de salida.

DISPOSITIVO DE ALMACENAMIENTO DIGITAL Y/O ELECTRÓNICO: Es un dispositivo capaz de leer y escribir información con el propósito de almacenarla permanentemente, pueden almacenar información en su interior, como en el caso de los discos rígidos, tarjetas de memoria y pendrives, o como en el caso de las unidades de almacenamiento óptico como las lector grabadoras de Blu-Ray, DVD o CD, grabándolas en un soporte en forma de disco.

BORRADO SEGURO: Es la acción que se realiza sobrescribiendo toda la información contenida en un medio de almacenamiento digital o electrónico, remplazándola por datos sin significado alguno, haciéndola irrecuperable.

CIFRADO: El cifrado utiliza un conjunto complejo de reglas llamado algoritmo para hacer que los datos sean ilegibles. Por ejemplo, el algoritmo podría cambiar un archivo de texto en una colección aparentemente sin sentido de números y símbolos. Si requiere leer los datos necesitaría la clave de encriptación, que revierte el proceso de encriptación para que los números y símbolos se conviertan en texto.

IMAGEN FORENSE FÍSICA: Copia o extracción total o parcial de archivos de datos lógicos, contenedor o partición lógicos de un dispositivo físico que almacene información electrónica.

FUNCIÓN HASH*:* Función Criptográfica, esta función se aplica para garantizar la integridad de los datos contenidos en la imagen forense, el cual consiste en una función matemática que genera un resultado numérico (claves o llaves a un documento o conjunto de datos). Ese valor debe ser inmutable siempre y cuando el contenido de la información no haya cambiado. Si dicho contenido en este caso de la imagen forense varía en un solo bit o carácter, el resultado numérico va a ser diferente. Por ello es que, desde el levantamiento de la evidencia, durante la investigación y el reporte final de la misma los valores hash son revisados con el fin de mantener un material probatorio íntegro y confiable, asegurando así la veracidad e integridad de las evidencias.

SUMA DE VERIFICACIÓN: Corresponde a la actividad de calcular la integridad de una información, a través de un algoritmo matemático.

4. DOCUMENTOS DE REFERENCIA

- Constitución Política de Colombia de 1991.
- Ley 1273 de 2009, Por medio del cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado – denominado “De la Protección de la información y de los datos"
- Ley 734 de 2002, Código disciplinario único.
- Ley 600 de 2000. Código de procedimiento penal.
- Ley 1474 de 2011. Estatuto anticorrupción.
- Decreto 262 de 2000, Artículo 10. Por el cual se modifica la estructura de la Procuraduría General de la Nación.
- Resolución 291 del 21 de julio de 2018. Por la cual se crea el grupo de informática forense de la DNIE.
- Orden Jurisdiccional C-1121/05
- Corte Constitucional en sentencia C-336 de 2007
- Manual único de policía judicial y Cadena de custodia.
- ISO/IEC 27041: Tecnología de la información. Técnicas de seguridad. Directrices para garantizar la idoneidad y adecuación del método de investigación de incidentes.
- ISO/IEC 27042**:** Tecnología de la información. Técnicas de seguridad. Directrices para el análisis y la interpretación de las evidencias electrónicas.
- ISO/IEC 27050**:** Tecnología de la información. Técnicas de seguridad. Directrices para descubrir información pertinente almacenada electrónicamente (ESI) o datos de una o más partes involucradas en una investigación o litigio.
- ISO/IEC 27037**:** Tecnología de la información. Técnicas de seguridad. Directrices para la identificación, recogida, adquisición y preservación de evidencias electrónicas.

5. CONDICIONES GENERALES

Cuando la evidencia que se quiere recolectar o archivo, se encuentra en una infraestructura compleja, el servidor se apoya en las personas que administran esa infraestructura para que ellos extraigan los archivos y firmen el acta de la diligencia y la cadena de custodia.

Tener en cuenta la preparación de las herramientas de Hardware y Software forense a utilizar, para esto es necesario realizar proceso de Borrado Seguro en los dispositivos de almacenamiento digital que se deban utilizar temporal o definitivamente durante el tratamiento, copia, imagen, extracción, análisis y entrega de resultados, esto con el fin de asegurar que los medios forenses se encuentran estériles o sanitizar los que se encuentren disponibles. Se hace la salvedad que no se utilizan discos duros que contengan evidencia de otro caso.

Dar aplicación a la versión vigente de los protocolos, guías, reglamentos y manuales que sobre la materia el estado de la ciencia aporte y que la criminalística establezca.

Para llevar a cabo la asignación se otorga generalmente cuarenta (40) días hábiles, dentro de los cuales se debe realizar el apoyo técnico o de asesoría especializada. En el evento que el tiempo no sea suficiente, debido a que no se han obtenido o no se han practicado en su totalidad las pruebas, o no se ha recabado el material necesario para el estudio o análisis, se solicitará ampliación de términos.

Anexos:

- Manual Único de Policía Judicial y Cadena de custodia.
- Formato cadena de custodia
- Rotulo cadena de custodia.
- Oficio de notificación y /o comunicación
- Formatos y documentos de análisis de información
- Informe técnico – científico
- DI-F-01 Formato Acta Visita
- Software para Recolectar Datos Volátiles.
  Encase Forensic, Access FTK, Nuix Investigator, P2 eXplorer, IEF Mangent, Belkasoft Evidence Center. Autopsy (Windows y Linux). DFF Forensics Framework. Builk Extractor. Set de herramientas de DEFT o CAINE, tanto lado Windows como lado Linux. FTK imager y herramientas auxiliares.
  SANS Investigación Forense Toolkit - SIFT

6. PROCEDIMIENTO

N.	ACTIVIDAD/DESCRIPCIÓN	RESPONSABLE / DEPENDENCIA	SALIDAS	PUNTO DE CONTROL
1	**Estudiar el expediente.** Revisar la documentación del expediente y determinar que documentación adicional se requiere para dar respuesta al cuestionario del auto de asignación y determinar en que se enfocan las preguntas del auto de pruebas, Un primer paso para adquirir la imagen forense es determinar si los dispositivos electrónicos susceptibles de recolección cuentan con un sistema operativo (no son solamente de almacenamiento) se encuentran encendidos, de la posibilidad de encontrarlos encendidos dependerá el orden de prioridad y volatilidad. Es de aclarar que cada investigación implica situaciones únicas, que requieren de información particular, la cual debe ser solicitada en caso de que el expediente no la contenga.	Servidor(es) designado(s).	Auto de asignación, y delegación de funciones de policía judicial Expediente Sistema de Información Misional - SIM Documentos de trabajo	

N.	ACTIVIDAD/DESCRIPCIÓN	RESPONSABLE / DEPENDENCIA	SALIDAS	PUNTO DE CONTROL
2	**¿Se requiere orden jurisdiccional?** No, continuar con la actividad 4 Si, continuar con la actividad 3.	Servidor(es) designado(s).		X
3	**Solicitar orden jurisdiccional** La orden jurisdiccional debe ser solicitada cuando la información requerida pueda vulnerar algún derecho fundamental. El auto de asignación contiene cuales son los motivos que tiene la procuraduría (test de necesidad, razonabilidad y proporcionalidad)	Asesor de la dirección	Orden jurisdiccional.	
4	**¿Se requiere información adicional mediante oficio o visita?** No, continuar en la actividad 5 Sí; continuar en la actividad 7 y 5	Servidor(es) designado(s)		X
5	**¿Se requiere notificar y/o comunicar a la defensa o a las partes la práctica de pruebas?** Si, continua en la actividad 6 No, continua en la actividad 8	Servidor(es) designado(s)		X
6	**Notificar y/o comunicar a la defensa o a las partes la práctica de pruebas** Se notifica y/o comunica a los implicados o a la defensa la información con relación a la práctica de pruebas que se va a realizar mediante solicitud de información o visita.	Servidor(es) designado(s)	Oficio de notificación y /o comunicación	
7	**Realizar la visita o solicitud de información.** Definir si la información que se requiere allegar al expediente puede ser solicitada mediante oficio, o si es necesario realizar visita especial para practicar las pruebas pertinentes y/o recaudar la documentación faltante.	Servidor(es) designado(s)	Oficio de solicitud de información DI-F-01 Formato Acta Visita Registro fotográfico de la visita Material probatorio	

N.	ACTIVIDAD/DESCRIPCIÓN	RESPONSABLE / DEPENDENCIA	SALIDAS	PUNTO DE CONTROL
	En caso de requerirse visita, se debe relacionar lo evidenciado en el formato de acta de visita, haciendo claridad en los diferentes campos en los cuales se requiere indagar.		de acuerdo con el Manual único de policía judicial	
8	**Analizar y validar la información** Se analiza la información y elementos recopilados, también se validan los procedimientos aplicados en lo que respecta al plan de trabajo y cronograma de actividades, condiciones de trabajo y logística para desplazamientos dentro y/o fuera de la ciudad de ser necesario.	Servidor(es) designado(s)	Formatos y documentos de análisis de información	
9	**Identificar el Elemento de Naturaleza Digital:** Identificar el tipo de dispositivo electrónico, si es una unidad interna o externa, si es un computador si está el computador encendido Si/No	Servidor(es) designado(s)	Formatos y documentos de análisis de información	
10	**Asegurar el lugar del hecho:** Esta actividad requiere la aplicación de normas de seguridad personal, y por supuesto de los elementos que puedan encontrarse en el lugar del hecho, entre ellas el aislamiento, tener especial cuidado con los equipos que se encuentren en funcionamiento, sobre todo si estos hacen parte de un sistema centralizado de datos (Equipos servidores), ya que desconectarlos o apagarlos, podría causar daños a nivel de información que afectarían una organización y conllevarían a una responsabilidad civil por esa causa, adicionalmente debemos tener en cuenta que un equipo en funcionamiento puede contener información volátil en su memoria que podría perderse.	Servidor(es) designado(s)	Formatos y documentos de análisis de información	

N.	ACTIVIDAD/DESCRIPCIÓN	RESPONSABLE / DEPENDENCIA	SALIDAS	PUNTO DE CONTROL
11	**Asegurar que en el caso de que NO se encontrara el dispositivo o computador encendido.** Remitirse al Procedimiento DI-P-14 Realizar Imágenes Forenses, **No** continuar con este Procedimiento.	Servidor(es) designado(s)	Formatos y documentos de análisis de información	
12	**Recolectar datos volátiles: (computador encendido).** Consiste en realizar una copia total o parcial de la información contenida en la memoria RAM de un equipo de cómputo o dispositivo electrónico con sistema operativo, con el fin de realizar un trabajo posterior en el laboratorio y determinar que eventos, aplicaciones, tareas, conexiones de red, usuarios conectados, aplicaciones ejecutadas se estaban ejecutando en el dispositivo en un momento determinado mientras se encontraba encendido, datos que se consideran de gran relevancia para correlacionar información durante el análisis posterior en el laboratorio.	Servidor(es) designado(s)	Formatos y documentos de análisis de información	
13	**Aplicar Procedimiento de Cadena de Custodia.** Con el fin de preservar los materiales probatorios y garantizar su validez en el proceso, aplicando los principios de Integridad, Identidad, Preservación, Seguridad, Almacenamiento y continuidad. Adicionalmente va acompañado por un proceso de embalaje de los elementos y un sistema documental a través del registro de la información en formatos.	Servidor(es) designado(s)	Manual Cadena de Custodia. Formato Cadena de Custodia. Rotulo Cadena de Custodia.	

N.	ACTIVIDAD/DESCRIPCIÓN	RESPONSABLE / DEPENDENCIA	SALIDAS	PUNTO DE CONTROL
14	**Embalar, Marcar, Rotular el dispositivo que contiene la Imagen forense:** El Servidor(es) designado(s) por el Director Nacional de Investigaciones Especiales, embala el dispositivo que incluye el elemento en un contenedor adecuado para su preservación y diligencia, el formato de rótulo donde se especifica el hallazgo, la cantidad y su forma de preservación. El servidor marca el contenedor con la información básica del dispositivo encontrado. Se deben tener en cuenta aspectos como la verificación visual entre seriales de identificación de los dispositivos a analizar y los correspondientes al rotulo, registro de continuidad de la cadena de custodia, orden jurisdiccional, solicitud apoyo técnico, Auto de asignación, etc. Se realiza el registro de fecha, hora y el motivo del contacto con el elemento.	Servidor(es) designado(s)	Manual Cadena de Custodia. Formato Cadena de Custodia. Rotulo Cadena de Custodia.	
15	**Elaborar el informe** Elaborar informe consolidado dando respuesta a cada una de las preguntas del cuestionario presentadas en el auto de asignación.	Servidor(es) designado(s)	DI-F-02 Formato Informe Técnico Científico	
16	**Entregar informe de apoyo y/o asesoría técnica.** Remitir el informe al asesor de despacho de la dirección para revisión.	Servidor(es) designado(s) Asesor de despacho de la dirección	DI-F-02 Formato Informe Técnico Científico	

N.	ACTIVIDAD/DESCRIPCIÓN	RESPONSABLE / DEPENDENCIA	SALIDAS	PUNTO DE CONTROL
17	**¿Existen observaciones al informe de apoyo y/o asesoría técnica?** No, continuar con la actividad 19 Si, continuar con la actividad 18	Servidor(es) designado(s)	DI-F-02 Formato Informe Técnico Científico	X
18	**Realizar correcciones y ajustes al informe de apoyo y/o asesoría técnica** De acuerdo con las observaciones realizadas por el asesor del despacho de la dirección, se deben hacer los ajustes y correcciones requeridos.	Servidor(es) designado(s)	DI-F-02 Formato Informe Técnico Científico	
19	**Entregar informe final de apoyo y/o asesoría técnica.** Se entrega el informe con el visto bueno del asesor a la Secretaría de la Dirección y se descarga en el Sistema de Información Misional – SIM por parte del Servidor(es) designado(s), cargando a la vez el informe en PDF. La Secretaría de la Dirección remite al operador disciplinario correspondiente	Servidor(es) designado(s) Secretaria del despacho de la dirección	DI-F-02 Formato Informe Técnico Científico Registro en el Sistema de Información Misional - SIM	

7. CONTROL DE CAMBIOS

FECHA	VERSIÓN DEL DOCUMENTO QUE MODIFICA	DESCRIPCIÓN DEL CAMBIO
7/12/2018	1	Versión ISO9001:2015
31/07/2022	2	Teniendo en cuenta lo dispuesto en el memorando 005 del 22 de julio de 2022, referente a la “Implementación y mantenimiento del Sistema de Gestión de Calidad – SGC”, se actualiza este documento conforme a los lineamientos establecidos para la gestión de la información documentada; por lo anterior, se aplica la nueva plantilla y su codificación toda vez que este documento se encontraba identificado con el código PRO-DI-TC-014.