1. OBJETIVO

Garantizar la conservación, documentación, análisis del material probatorio y que llegado el caso puedan ser aceptadas legalmente en un proceso disciplinario.

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 el tratamiento, procesamiento y análisis de dispositivos móviles y termina con la entrega del informe dando respuesta al auto de asignación.

3. DEFINICIONES Y SIGLAS

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.

DISPOSITIVO MOVIL: un dispositivo puede definirse con cuatro características que lo diferencian de otros dispositivos que, aunque pudieran parecer similares, carecen de algunas de las características de los verdaderos dispositivos móviles. Estas cuatro características son: 1) movilidad 2) tamaño reducido 3) comunicación inalámbrica 4) interacción con las personas.

IMAGEN FORENSE: Extracción total o parcial de archivos de datos lógicos, contenedor lógico o partición lógica de un dispositivo físico que almacene información electrónica.

FUNCION 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.

DATOS VOLÁTILES: Son aquellos que se almacenan en la memoria del sistema (Por ejemplo, registro del sistema, caché, memoria RAM) y se pierde si el equipo se apaga o reinicia. Se puede determinar quién o quienes se encuentran con una sesión de usuarios abierta ya sean locales o remotos, registra procesos, aplicaciones y servicios activos.

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

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. etc.

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.

Estas son algunas herramientas de análisis forense que por su característica se utiliza en este procedimiento

- Herramientas de disco y de captura de datos
- Visores de archivos
- Análisis de archivos
- Análisis de registros
- Análisis de Internet
- Análisis de Correo Electrónico
- Herramienta de análisis de la integridad de la imagen forense

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
- Software para Análisis de Dispositivos Móviles.
  AFLogical OSE - Open source Android Forensics app and framework.
  Open Source Android Forensics.
  Andriller.
  FTK Imager Lite.
  NowSecure Forensics Community Edition.
  LIME- Linux Memory Extractor.
  Android Data Extractor Lite (ADEL) .
  WhatsApp Xtract.
  Skype Xtractor.
  Cellebrite Touch.
  Encase Forensics.
  Passware Kit Forensic,
  Oxygen Forensic Suite.
  MOBILedit! Forensic.
  Elcomsoft iOS Forensic Toolkit.

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	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
	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.			
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	**Verificar la cadena de custodia.** Verificar los seriales de identificación de los dispositivos a analizar material probatorio con respecto al rotulo, registro de continuidad de la cadena de custodia, el resguardo de la evidencia y la caracterización del dispositivo digital de estudio.	Servidor(es) designado(s)	Formatos y documentos de análisis de información	
10	**Determinar si el teléfono celular está encendido o apagado**. a. Si está apagado, debe quedar apagado. b. Si está encendido debe ser aislado de la red de telefonía celular lo antes posible con la opción que se estime apropiada: i) Configurando el modo “Avión” en el teléfono celular, si lo permite ii) Colocándolo en una caja de Faraday iii) Encendiendo un inhibidor de señal en cercanía del teléfono celular iv) Envolviéndolo con tres o más capas de papel de aluminio v) Apagando el teléfono y retirando la batería	Servidor(es) designado(s).	Formatos y documentos de análisis de información	
11	**Obtener información sobre el modelo del teléfono celular y planificar el método para la extracción de evidencia digital** a. Identificar la tecnología general del teléfono celular	Servidor(es) designado(s).	Formatos y documentos de análisis de información	

N.	ACTIVIDAD/DESCRIPCIÓN	RESPONSABLE / DEPENDENCIA	SALIDAS	PUNTO DE CONTROL
	b. Localizar cables, drivers y determinar el software o hardware forense a utilizar para la pericia informática, la selección de herramientas forenses para una pericia informática sobre telefonía celular depende de diversos factores, como el nivel de detalle requerido en los puntos de pericia, el modelo de teléfono celular en cuestión y la presencia de otras funcionalidades de almacenamiento externo del dispositivo. c. Determinar funcionalidades del teléfono celular y posibles datos almacenados en el mismo. d. Si el teléfono celular no tiene puerto de datos, no se cuenta con el cable de datos, o no existe software o hardware forense disponible para dicho modelo, se registra esta situación.			
12	**Consultar las especificaciones técnicas** del teléfono celular y sus capacidades de almacenamiento de datos	Servidor(es) designado(s).	Formatos y documentos de análisis de información	
13	**Preservar y analizar las fuentes de evidencia digital.** a. Tarjeta de Memoria Externa i. Realizar una imagen forense con la herramienta de informática forense. ii. Extraer la evidencia digital que resulte relevante conforme al Auto de designación y/o la solicitud de Apoyo Técnico y el cuestionario de Informática forense. b. Tarjeta SIM i. Generar una copia de la información de la SIM o leer la información digital de dicho dispositivo utilizando un lector de SIM protegido contra escritura. ii. Si el SIM está bloqueado por PIN y éste no es conocido, se deja constancia o se utiliza el PUK en caso de estar disponible. iii. Si el SIM no está bloqueado, se extrae la información digital relevante al caso.	Servidor(es) designado(s).	Formatos y documentos de análisis de información	

N.	ACTIVIDAD/DESCRIPCIÓN	RESPONSABLE / DEPENDENCIA	SALIDAS	PUNTO DE CONTROL
	c. Equipo de telefonía celular i. Aislar el dispositivo de la red de telefonía celular previamente a la extracción de información digital y si es posible, durante todo el proceso. ii. Realizar una extracción física de la memoria del teléfono celular o bien una extracción lógica utilizando todas las herramientas forenses apropiadas, tanto de hardware como de software iii. Verificar los resultados obtenidos. Validar mediante funciones hash la evidencia extraída.			
14	**Elaborar el Informe de laboratorio.** Adjuntar los elementos probatorios siguiendo los lineamientos de Cadena de Custodia, en cuanto a la verificación de resultados, adjuntar las validaciones sobre el sistema de archivos de los dispositivos celulares generando valores hash de todos los elementos extraídos y haciendo una segunda extracción al concluir el análisis forense con el objeto de chequear la integridad de dichos archivos. Cualquier cambio debería ser analizado en profundidad para determinar si se trata de archivos del sistema operativo o bien son archivos de usuario con el objeto de intentar determinar la razón de dichos cambios. Sin perjuicio de los pasos indicados en el procedimiento operativo estandarizado para el Análisis de evidencia digital, sobre dispositivos de telefonía celular, el Servidor(es) designado(s) por el Director Nacional de Investigaciones Especiales debe aplicar los conocimientos especializados sobre la materia y tener presente los aportes de otras guías de mejores prácticas y de procedimiento a nivel internacional como [NIST, 2007], [ACPO & 7Safe, 2008], [SWGDE-1, 2013], [NIST-1,2014] .	Servidor(es) designado(s).	Formatos y documentos de análisis de información	
15	**Generar reporte** con información de metadatos, propiedades y listado de archivos.	Servidor(es) designado(s)	Formatos y documentos de análisis de información	

N.	ACTIVIDAD/DESCRIPCIÓN	RESPONSABLE / DEPENDENCIA	SALIDAS	PUNTO DE CONTROL
16	**Crear reporte de hallazgos.** Durante esta fase se reúnen todos los archivos encontrados durante las fases de recuperación de archivos borrados, recuperación de información escondida, identificación de archivos no borrados e identificación de archivos protegidos.	Servidor(es) designado(s)	Formatos y documentos de análisis de información	
17	**Generar (CDs o DVDs)** Es necesario que toda la información, archivos, documentos digitales que se haya generado de este análisis sea adjuntado, copiado a un dispositivo de almacenamiento digital (CDs, DVDs, Discos Duros), que permita que el investigador pueda visualizar la información, de acuerdo a esto el perito deberá explicar detalladamente la información que se encuentra en el dispositivo de almacenamiento que se va entregar y generar al archivo la sumas de verificación Hash y MD5, que garantizaran su autenticidad.	Servidor(es) designado(s)	Formatos y documentos de análisis de información	
18	**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	
19	**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	Servidor(es) designado(s)	Manual Cadena de Custodia. Formato Cadena de Custodia. Formato Rotulo	

N.	ACTIVIDAD/DESCRIPCIÓN	RESPONSABLE / DEPENDENCIA	SALIDAS	PUNTO DE CONTROL
	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.			
20	**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	
21	**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	
22	**¿Existen observaciones al informe de apoyo y/o asesoría técnica?** No, continuar con la actividad 24 Si, continuar con la actividad 23	Servidor(es) designado(s)	DI-F-02 Formato Informe Técnico Científico	X
23	**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	
24	**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.	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-016.