	<p style="text-align: center;">PROCEDIMIENTO: TRATAMIENTO PROCESAMIENTO Y ANÁLISIS DE LA EVIDENCIA DIGITAL</p> <p style="text-align: center;">PROCESO: DISCIPLINARIO</p>	Versión	2
		Fecha	31/07/2022
		Código	DI-P-15

1. OBJETIVO

Garantizar la conservación, documentación, análisis y presentación de evidencias 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 evidencia digital 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: Extracción total o parcial de archivos de datos lógicos, contenedor o partición lógicos 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 por lo 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.

	<p align="center">PROCEDIMIENTO: TRATAMIENTO PROCESAMIENTO Y ANÁLISIS DE LA EVIDENCIA DIGITAL</p> <p align="center">PROCESO: DISCIPLINARIO</p>	Versión	2
		Fecha	31/07/2022
		Código	DI-P-15

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

4. DOCUMENTOS DE REFERENCIA


- 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

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

	PROCEDIMIENTO: TRATAMIENTO PROCESAMIENTO Y ANÁLISIS DE LA EVIDENCIA DIGITAL PROCESO: DISCIPLINARIO	Versión	2
		Fecha	31/07/2022
		Código	DI-P-15

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 la Evidencia Digital.
Encase Forensic, Access FTK, NuiX Investigator, P2 eXplorer, IEF Mangent, Belkasoft Evidence Center. Autopsy (Windows y Linux). DFF Forensics Framework. Bulk 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	<p>Estudiar el expediente.</p> <p>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.</p> <p>Es de aclarar que cada investigación implica situaciones únicas, que</p>	Servidor(es) designado(s).	<p>Auto de asignación, y delegación de funciones de policía judicial</p> <p>Expediente</p> <p>Sistema de Información Misional - SIM</p> <p>Documentos de trabajo</p>	

	PROCEDIMIENTO: TRATAMIENTO PROCESAMIENTO Y ANÁLISIS DE LA EVIDENCIA DIGITAL PROCESO: DISCIPLINARIO	Versión	2
		Fecha	31/07/2022
		Código	DI-P-15


N.	ACTIVIDAD/DESCRIPCIÓN	RESPONSABLE / DEPENDENCIA	SALIDAS	PUNTO DE CONTROL
	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	Servidor(es) designado(s)	Oficio de solicitud de información DI-F-01 Formato acta de visita	

	PROCEDIMIENTO: TRATAMIENTO PROCESAMIENTO Y ANÁLISIS DE LA EVIDENCIA DIGITAL PROCESO: DISCIPLINARIO	Versión	2
		Fecha	31/07/2022
		Código	DI-P-15


N.	ACTIVIDAD/DESCRIPCIÓN	RESPONSABLE / DEPENDENCIA	SALIDAS	PUNTO DE CONTROL
	<p>ser solicitada mediante oficio, o si es necesario realizar visita especial para practicar las pruebas pertinentes y/o recaudar la documentación faltante.</p> <p>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.</p>		<p>Registro fotográfico de la visita</p> <p>Material probatorio de acuerdo con el Manual único de policía judicial</p>	
8	<p>Analizar y validar la información.</p> <p>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.</p>	Servidor(es) designado(s)	Formatos y documentos de análisis de información	
9	<p>Verificar la cadena de custodia.</p> <p>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.</p>	Servidor(es) designado(s)	Formatos y documentos de análisis de información	
10	<p>Organizar la información.</p> <p>Para la obtención de resultados favorables. Por ello, se deben considerar los posibles escenarios: una imagen relacionada con un dispositivo, múltiples imágenes asociadas a un dispositivo o varias imágenes relacionadas con múltiples dispositivos.</p>	Servidor(es) designado(s)	Formatos y documentos de análisis de información	
11	<p>Preparar las herramientas de Hardware y Software forense a utilizar.</p> <p>Para esto es necesario realizar un</p>	Servidor(es) designado(s)		

 <p>PROCURADURIA GENERAL DE LA NACION</p>	<p>PROCEDIMIENTO: TRATAMIENTO PROCESAMIENTO Y ANÁLISIS DE LA EVIDENCIA DIGITAL</p> <p>PROCESO: DISCIPLINARIO</p>	Versión	2
		Fecha	31/07/2022
		Código	DI-P-15


N.	ACTIVIDAD/DESCRIPCIÓN	RESPONSABLE / DEPENDENCIA	SALIDAS	PUNTO DE CONTROL
	proceso de Borrado Seguro en los dispositivos de almacenamiento digital que se deban utilizar temporal o definitivamente durante el tratamiento, extracción, análisis y entrega de resultados, esto con el fin de asegurar que los medios forenses se encuentran estériles.			
12	Realizar la creación del caso , En la herramienta de análisis, una vez se determina por parte del Perito que herramienta de análisis forense es la adecuada para dar cumplimiento a la solicitud, se crea un archivo de caso con los datos del análisis y de configuración de hardware o software.	Servidor(es) designado(s)	Formatos y documentos de análisis de información	
13	Confirmar la integridad de la imagen forense . Se realiza la comparación de valores o sumas de verificación HASH (MD5, SHA1), se almacena y se adiciona esta información al producto y reporte final.	Servidor(es) designado(s)	Formatos y documentos de análisis de información	
14	Crear la línea de tiempo de análisis	Servidor(es) designado(s)	Formatos y documentos de análisis de información	
15	Recuperar la configuración de la zona horaria del dispositivo de estudio y aplicarla a las herramientas forenses de análisis.	Servidor(es) designado(s)	Formatos y documentos de análisis de información	
16	Configurar la herramienta , De análisis forense para la recuperación de carpetas y archivos eliminados.	Servidor(es) designado(s)	Formatos y documentos de análisis de información	
17	Configurar los criterios de búsqueda , por palabras claves, Números, Direcciones, Nombres, en la totalidad del disco incluyendo espacio no asignado y áreas Slack.	Servidor(es) designado(s)	Formatos y documentos de análisis de información	

	PROCEDIMIENTO: TRATAMIENTO PROCESAMIENTO Y ANÁLISIS DE LA EVIDENCIA DIGITAL PROCESO: DISCIPLINARIO	Versión	2
		Fecha	31/07/2022
		Código	DI-P-15

N.	ACTIVIDAD/DESCRIPCIÓN	RESPONSABLE / DEPENDENCIA	SALIDAS	PUNTO DE CONTROL
18	Generar reporte con información de metadatos, propiedades y listado de archivos.	Servidor(es) designado(s)	Formatos y documentos de análisis de información	
19	Crear reporte de hallazgos , que contenga metadatos de los archivos, extensión de archivo, tamaño físico y lógico, ruta de los archivos.	Servidor(es) designado(s)	Formatos y documentos de análisis de información	
20	Generar (CDs o DVD) 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, DVD, 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	
21	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	
22	Embalar, Marcar, Rotular el dispositivo que contiene la Imagen forense: El Servidor(es) designado(s) por el Director Nacional de Investigaciones	Servidor(es) designado(s)	Manual Cadena de Custodia. Formato Cadena de Custodia. Formato Rotulo	

	PROCEDIMIENTO: TRATAMIENTO PROCESAMIENTO Y ANÁLISIS DE LA EVIDENCIA DIGITAL PROCESO: DISCIPLINARIO	Versión	2
		Fecha	31/07/2022
		Código	DI-P-15

N.	ACTIVIDAD/DESCRIPCIÓN	RESPONSABLE / DEPENDENCIA	SALIDAS	PUNTO DE CONTROL
	<p>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.</p> <p>El servidor marca el contenedor con la información básica del dispositivo encontrado.</p> <p>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.</p> <p>Se realiza el registro de fecha, hora y el motivo del contacto con el elemento.</p>			
23	<p>Elaborar el informe</p> <p>Elaborar informe consolidado dando respuesta a cada una de las preguntas del cuestionario presentadas en el auto de asignación.</p>	Servidor(es) designado(s)	DI-F-02 Formato informe técnico científico	
24	<p>Entregar informe de apoyo y/o asesoría técnica.</p> <p>Remitir el informe al asesor de despacho de la dirección para revisión.</p>	Servidor(es) designado(s) Asesor de despacho de la dirección	DI-F-02 Formato informe técnico científico	
25	<p>¿Existen observaciones al informe de apoyo y/o asesoría técnica?</p> <p>No, continuar con la actividad 27 Si, continuar con la actividad 26</p>	Servidor(es) designado(s)	DI-F-02 Formato informe técnico científico	X

	PROCEDIMIENTO: TRATAMIENTO PROCESAMIENTO Y ANÁLISIS DE LA EVIDENCIA DIGITAL PROCESO: DISCIPLINARIO	Versión	2
		Fecha	31/07/2022
		Código	DI-P-15

N.	ACTIVIDAD/DESCRIPCIÓN	RESPONSABLE / DEPENDENCIA	SALIDAS	PUNTO DE CONTROL
26	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	
27	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) Secretaría 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-015.