|  |  |
| --- | --- |
| **ACTA- N°** | **[***Número asignado***]** |

**SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO**

**OFICINA DE TECNOLOGÍA E INFORMÁTICA**

**GRUPO DE TRABAJO DE INFORMÁTICA FORENSE Y SEGURIDAD DIGITAL**

**RADICADO [*EN NÚMERO EL RADICADO*]**

En la ciudad de Bogotá, el [*Día en letras*] ([*Día en números*]) del mes de [*Mes en letras*] de [*Año en letras*] ([*Año en números*]), el Grupo de Trabajo de Informática Forense y Seguridad Digital (en adelante “GTIFSD”) de la Superintendencia de Industria y Comercio (en adelante “SIC”), recibe por parte del [*Grupo que realiza la solicitud*] el expediente con radicado N° [*En números el número de radicado*] con el fin de realizar el peritaje de [*Número en letras*] ([*valor numerico*]) dispositivo(s) contenedor(es) de evidencia digital (CD/DVD/BLURAY/USB/DD). El objetivo de este peritaje es [*escribir objetivo de la actividad a realizar*].

1. **DESCRIPCIÓN DEL REQUERIMIENTO**

[*Nombre de la persona que hace la solicitud*], [*Cargo*], [*Grupo de trabajo y Delegatura*] solicita al GTIFSD el día [*Día en letras*] ([*Día en números*]) del mes de [*Mes en letras*] de [*Año en letras*] ([*Año en números*]) el peritaje de [*Número en texto*] ([*Valor numerico*]) dispositivos contenedores de evidencia digital ([*Especificar los tipos de dispositivos*])**,** con número de radicado N° [*En números el número de radicado*] **–** [*NOMBRE DEL CASO EN MAYUSCULA SOSTENIDA*]. Al finalizar el peritaje se solicita al GTIFSD todos los mensajes de datos almacenados en los dispositivos de origen revisados en ([*Identificar los tipos de dispositivo de destino*]), esto con el fin de [*escribir objetivo de la actividad a realizar*].

1. **CONTENEDOR DE EVIDENCIA DIGITAL EXAMINADO**

[*Nombre de la persona que hace la solicitud*], [*Cargo*], [*Grupo de trabajo y Delegatura*] hace allegar dispositivos contenedores de evidencia digital ([*Especificar los tipos de dispositivos*])

| **CARACTERISTICA** | **DESCRIPCION DE DISPOSITIVO DESTINO** |
| --- | --- |
| Tipo de Dispositivo | [*Identificar tipo de dispositivo*] |
| Marca | [*Identificar marca del dispositivo*] |
| Serial Físico | [*Describir el serial físico*] |
| Estado Físico | [*Describir el estado fisico*] |
| Capacidad total | [*Describir la capacidad del dispositivo*] |
| Espacio utilizado o Peso | [*Describir espacio usado* (Xinorbis)] |
| Número Archivos | [*Describir número de archivos total* (Xinorbis)] |
| Número Carpetas | [*Describir número de carpetas total* (Xinorbis)] |
| Serial Lógico | [*Describir serial lógico*] |
| Estado Lógico | [*Describir estado lógico*] |

Tabla 1. Inspección preliminar del contenedor de evidenica Digital

1. **DESCRIPCIÓN GENERAL DEL PROCEDIMIENTO**
	1. **BÚSQUEDA Y COMPROBACION DEL SITIO WEB**

**a. Identificación física:** Este procedimiento consiste en establecer el estado físico del dispositivo, para lo cual se identifica el tipo de embalaje en el cual se entrega los dispositivos contenedores de evidencia digital (([*Especificar los tipos de dispositivos*]), se identifica el serial físico, se toman fotografías para establecer las características visuales tales como marcaciones y adhesivos.

**b. Revisión de datos lógicos:** Este procedimiento consiste en utilizar diferentes herramientas de software tales como Vista preliminar de Dispositivos y Unidades de Windows, con el fin de obtener los datos lógicos tales como serial, cantidad de archivos, cantidad de carpetas [*Listar las diferentes herramientas de hardware empeladas durante esta etapa separadas por comas*].

* 1. **GRADO DE ACEPTACIÓN POR LA COMUNIDAD TÉCNICO - CIENTÍFICA DE LOS PROCEDIMIENTOS REALIZADOS**

Los procedimientos técnicos empleados para realizar la preservación, recolección y análisis de la información almacenada en dispositivos de almacenamiento digital, gozan de total aceptación por la comunidad técnico - científica, al tratarse de actividades debidamente reconocidas y avaladas en la realización de los diferentes análisis forenses de computadoras y dispositivos electrónicos de datos que se efectúan a nivel mundial por parte de expertos en esta área, en donde apoyados en herramientas de software y hardware especializado se lleva a la práctica un conjunto de conocimientos científicos y de técnicas que hace posible el tratamiento de la información almacenada en un medio digital preservando la integridad de la evidencia.

* 1. **PRINCIPIOS TÉCNICOS– CIENTÍFICOS APLICADOS Y SU GRADO DE ACEPTACIÓN**

**a**. **Principio de disponibilidad:** Cuando la información es accesible a los usuarios autorizados por el [*Grupo de trabajo y Delegatura*] en el momento de requerirla.

**b.** **Principio de no repudiación:** Cuando la información involucrada en un evento corresponde a quien participa en el mismo, quien no podrá desconocer su intervención en dicho evento.

**c.** **Principio de integridad:** cuando se garantiza que la información es exacta y completa, no se modifica desde el momento de su creación y se almacena en un formato que asegura la exactitud de la información original mediante la huella HASH.

**d. Observancia:** Cuando se lleva el registro de los eventos importantes en la respectiva cadena de custodia.

1. **HERRAMIENTAS DE SOFTWARE Y HARDWARE UTILIZADAS**

A continuación se relacionan las herramientas de software y hardware utilizadas para realizar la actividad de identificación y peritaje de [*Numero en letras*] ([*Valor numerico*]) dispositivos contenedores de evidencia digital ([*Identificar los tipos de dispositivo*]):

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **SOFTWARE/HARDWARE** | **PROPÓSITO** | **NOMBRE** | **VERSIÓN** | **FABRICANTE** |
| [*Identificar si es Software o Hardware*] | [*Identificar el propósito u objetivo de la herramienta empleada*] | [*Identificar el nombre del software o la placa SIC del hardware*] | [*Identificar versión o modelo de la herramienta empleada*] | [*Identificar el fabricante o la marca de la herramienta*] |
| [*Identificar si es Software o Hardware*] | [*Identificar el propósito u objetivo de la herramienta empleada*] | [*Identificar el nombre del software o la placa SIC del hardware*] | [*Identificar versión o modelo de la herramienta empleada*] | [*Identificar el fabricante o la marca de la herramienta*] |

Tabla 2 Relación de herramientas de software y hardware utilizadas en la actividad.

1. **RESULTADOS DEL PERITAJE**
	1. **IDENTIFICACIÓN FÍSICA:**

| **CARACTERISTICA** | **DESCRIPCION DE DISPOSITIVO DESTINO** |
| --- | --- |
| Tipo de Dispositivo | [*Identificar tipo de dispositivo*] |
| Marca | [*Identificar marca del dispositivo*] |
| Serial Físico | [*Describir el serial físico*] |
| Estado Físico | [*Describir el estado fisico*] |
| Capacidad total | [*Describir la capacidad del dispositivo*] |
| Espacio utilizado o Peso | [*Describir espacio usado* (Xinorbis)] |
| Número Archivos | [*Describir número de archivos total* (Xinorbis)] |
| Número Carpetas | [*Describir número de carpetas total* (Xinorbis)] |
| Serial Lógico | [*Describir serial lógico*] |
| Estado Lógico | [*Describir estado lógico*] |
| Registro fotográfico Frontal | [*Incluir registro fotográfico frontal*] |
| Registro fotográfico Posterior | [*Incluir registro fotográfico posterior*] |

Tabla 3. Identificación del Contenedor de Evidenica Digital.

* 1. **REVISIÓN DE DATOS LÓGICOS**
1. **Vista preliminar de Dispositivos y Unidades de Windows**

Se utiliza la Vista preliminar de Dispositivos y Unidades de Windows para determinar la unidad conectada que puede identificarse mediante la letra ([*nombre de unidad en Windows]*) y sus propiedades.

|  |
| --- |
|  |

<Imagen >,. Visualización de navegación mediante Vista preliminar de Dispositivos y Unidades de Windows, Obtenida con impresión por pantalla la Aplicación de Microsoft Windows Recortes.

1. **FTK Imager**

Se utiliza la herramienta FTK Imager para realizar la navegación en el Dispositivo Contenedor de Evidenica Digtal la cual se encuentra en la unidad con la letra ([*nombre de unidad en Windows]*)

|  |
| --- |
|  |

<Imagen >,. *Visualización de navegación mediante FTK Imager, Obtenida con impresión por pantalla la Aplicación de Microsoft Windows Recortes.*

1. **TreeSize**

Se realiza la inspección del Dispositivo Contenedor de Evidenica Digtal mediante la herramienta TreeSize para determinar el contenido, estructura de carpeta, peso por cada archivo, carpeta y peso total del dispositivo.

|  |
| --- |
|  |

<Imagen >,. Inspección realizada mediante TreeSize, Obtenida con impresión por pantalla la Aplicación de Microsoft Windows Recortes

1. **CONCLUSIÓN**
2.

La actividad termina el día en números de mes en texto de año a la hora en formato militar, firman los encargados de las actividades técnicos mencionados y la revisión de la presente acta por parte del GTIFSD,

|  |  |
| --- | --- |
| **Realizado por:**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**NOMBRE**C.C CEDULA de CIUDADServidor Público y/o Contratista – ACE Accessdata Certified Examiner | **Revisado por:**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**NOMBRE**C.C CEDULA de CIUDADServidor Público y/o Contratista – ACE Accessdata Certified Examiner  |