|  |  |
| --- | --- |
| **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*]) de [*Mes en letras*] del año [*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 informe técnico de [*Número en letras*] ([*valor numérico*]) dispositivo(s) contenedor(es) de evidencia digital ([identificar el tipo de dispositivo]CD/DVD/BLURAY/USB/DD). El objetivo de este informe técnico 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*]) de [*Mes en letras*] del año [*Año en letras*] ([*Año en números*]) el informe técnico de [*Número en texto*] ([*Valor numérico*]) dispositivos contenedores de evidencia digital ([*Especificar los tipos de dispositivos*])**,** con número de radicado [*En números el número de radicado*]**.** Al finalizar el informe técnico se solicita al GTIFSD todos los mensajes de datos[[1]](#footnote-1) almacenados en los dispositivos de origen revisados en [*Número en texto*] ([*Valor numérico*]) ([*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 los dispositivos contenedores de evidencia digital ([*Especificar los tipos de dispositivos*])

| **CARACTERÍSTICA** | **DESCRIPCIÓN 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 físico*] |
| Capacidad total | [*Describir la capacidad del dispositivo*] |
| Espacio utilizado o tamaño | [*Describir espacio usado*] |
| Número Archivos | [*Describir número de archivos total*] |
| Número Carpetas | [*Describir número de carpetas total*] |
| Serial Lógico | [*Describir serial lógico*] |
| Estado Lógico | [*Describir estado lógico*] |

Tabla 1. Inspección preliminar del contenedor de evidencia Digital

1. **DESCRIPCIÓN GENERAL DEL PROCEDIMIENTO**
   1. **ANÁLISIS TÉCNICO DE LOS DISPOSITIVOS DE ORIGEN**

**a. Identificación física:** Este procedimiento consiste en establecer el estado físico de los dispositivos, para lo cual se identifica el tipo de embalaje en el que se entrega cada contenedor de evidencia digital (([*Especificar los tipos de dispositivos*]), el serial físico y 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 para visualizar el estado lógico de los dispositivos contenedores de evidencia digital, tales como, la vista preliminar de Dispositivos y Unidades de Windows, el serial lógico, la cantidad de archivos y de carpetas, entre otros. Para esta verificación se utilizaron las herramientas de hardware [*Listar las diferentes herramientas de hardware empleadas durante esta etapa separadas por comas*] y las herramientas de software [*Listar las diferentes herramientas de software empleadas 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 e informe técnico de [*Número en letras*] ([*Valor numérico*]) 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 INFORME TECNCO**
   1. **IDENTIFICACIÓN FÍSICA:**

| **CARACTERÍSTICA** | **DESCRIPCIÓN 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 físico*] |
| Capacidad total | [*Describir la capacidad del dispositivo*] |
| Espacio utilizado o tamaño | [*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 Evidencia 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 que la unidad conectada pueda 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 Imagen**

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

|  |
| --- |
|  |

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

1. **TreeSize**

Se realiza la inspección del Dispositivo Contenedor de Evidencia Digital mediante la herramienta TreeSize para determinar el contenido, estructura de carpetas, tamaño por cada archivo, carpeta y tamaño total del dispositivo.

|  |
| --- |
|  |

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

1. **CONCLUSIONES**

La actividad termina el [*Día en letras*] ([*Valor* numérico]) del mes de [*Identificar el mes*] de [*Año en letras*] ([*Valor numérico*]) a las [*Horas*]: [*Minutos*] [*en formato militar*], firman los encargados de las actividades técnicas mencionadas y la revisión de la presente acta por parte del GTIFSD,

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

1. Mensaje de Datos: “información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el Intercambio Electrónico de Datos (EDI), Internet, el correo electrónico, el telegrama, el télex o el telefax” Ley 527 de 1999 [↑](#footnote-ref-1)