|  |  |
| --- | --- |
| 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 la copia de [*Número en letras*] ([*valor numérico*]) dispositivo(s) contenedor(es) de evidencia digital (CD/DVD/BLURAY/USB/DD). El objetivo de esta copia 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*]) la copia exacta de [*Número en texto*] ([*Valor numérico*]) dispositivos contenedores de evidencia digital ([*Especificar los tipos de dispositivos*])**,** que se encuentran en el expediente con número de radicado N° [*En números el número de radicado*]. Al finalizar la copia, se solicita al GTIFSD todos los mensajes de datos 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. **HERRAMIENTAS DE SOFTWARE Y HARDWARE UTILIZADAS**

A continuación, se relacionan las herramientas de software y hardware utilizadas para realizar la actividad de identificación y copia 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 1 Relación de herramientas de software y hardware utilizadas en la actividad.

1. **DESCRIPCIÓN GENERAL DE LA ACTIVIDAD**

Se realiza la actividad de copia de los mensajes de datos[[1]](#footnote-1) de [*Número en letras*] ([*valor numérico*]) dispositivos contenedores de evidencia digital ([*describir los tipos de dispositivos copiados*]) en [*Número en letras*] etapas así:

1. **(SÍ APLICA)** Registro fotográfico de dispositivos de origen: Se capturan 4 tipos de fotografías: (i) embalaje, (ii) vista frontal, (iii) vista posterior y (iv) serial físico del dispositivo, esto para identificar visualmente el estado físico y otros elementos de identificación únicos del contenedor, tales como, el serial físico, la etiqueta, entre otros. Para esta etapa son utilizadas las herramientas de hardware [*Listar las diferentes herramientas de hardware empeladas durante esta etapa separadas por comas*].
2. Análisis técnico de dispositivos de origen: Se realiza la identificación de los dispositivos de origen mediante dos análisis: (i) análisis físico, en donde se identifican las características físicas del contenedor de evidencia digital, es decir, su ubicación exacta en el expediente, el tipo de dispositivo, marca, serial físico y estado físico, y (ii) análisis lógico, en donde se identifican las características lógicas del dispositivo contenedor de evidencia digital, es decir, la capacidad del dispositivo, el tamaño de la información digital, el serial lógico, el número de archivos, carpetas e imágenes forenses y el estado. Para esta etapa son utilizadas las herramientas de software [*Listar las herramientas de software empleadas en esta etapa separadas por comas*], así como las herramientas de hardware [*Listar las diferentes herramientas de hardware empeladas durante esta etapa separadas por comas*].
3. Copia de los mensajes de datos1: Se realiza la copia de la totalidad de los mensajes de datos que contienen los dispositivos identificados anteriormente usando el software [*Listar las herramientas de software empleadas en esta etapa separadas por comas*], a un contenedor de evidencia digital de destino [*Identificar el tipo de dispositivo de almacenamiento del contenedor temporal o final*].
4. Análisis técnico de dispositivo de destino: Se realiza la identificación del dispositivo contenedor de evidencia digital final, en el cual reposará la compilación de los dispositivos de origen anteriormente identificados y copiados. En esta etapa se realizan dos análisis: (i) análisis físico, en donde se identifican las características físicas del contenedor de evidencia digital, es decir, el tipo de dispositivo, marca, capacidad, embalaje, serial físico y estado físico, y (ii) análisis lógico, en donde se identifican las características lógicas del dispositivo contenedor de evidencia digital, es decir, la capacidad del dispositivo, el serial lógico, número de archivos, carpetas e imágenes forenses y el estado lógico. Para esta etapa son utilizados las herramientas de software [*Listar las herramientas de software empleadas en esta etapa separadas por comas*], así como la herramienta de hardware [*Listar las diferentes herramientas de hardware empleadas durante esta etapa separadas por comas*].
5. **(SÍ APLICA) REGISTRO FOTOGRÁFICO DE DISPOSITIVOS DE ORIGEN**

Para realizar la identificación física y visual del tipo de embalaje, el estado del dispositivo se realiza 4 tipos de fotografías (i) embalaje, (ii) vista frontal, (iii) vista posterior y (iv) serial físico del dispositivo, con una cámara fotográfica propiedad del GTIFSD con las siguientes características técnicas:

|  |  |
| --- | --- |
| **CARACTERÍSTICA** | **VALOR** |
| Dimensión | [*Identificar las dimensiones de la fotografía*] |
| Resolución  | [*Identificar la resolución de la fotografía*] |

Tabla 2 Características técnicas de las fotografías tomadas.

Estas fotografías se anexan a la presente acta *(Ver Anexo* [*Identificar si es físico o digital*][*Número secuencial de anexo*]*)* en las que pueden ser identificadas de acuerdo al folio asignado al dispositivo por parte de [*Identificar grupo que solicitó la actividad*].

1. **ANÁLISIS TÉCNICO DE DISPOSITIVOS DE ORIGEN**

[*Identificar el grupo que solicitó la actividad*] entrega un total de [*Número en texto*] ([*Valor numérico*]) dispositivos contenedores de evidencia digital ([*Describir los tipos de dispositivos copiados*]) correspondientes al caso N° [*En número el radicado*].

A continuación, se adjunta un cuadro resumen de los cuadernos del expediente en donde se encuentran los dispositivos contenedores de evidencia digital:

|  |  |  |
| --- | --- | --- |
| **N° TOTAL DE DISPOSITIVOS POR CUADERNO** | **NOMBRE DE CUADERNO PUBLICO** | **NOMBRE DE CUADERNO RESERVADO** |
| [*Escriba valor numérico*] | [*Identificar el cuaderno*] | [*Identificar el cuaderno*] |
| [*Escriba valor numérico*] | [*Identificar el cuaderno*] | [*Identificar el cuaderno*] |

Tabla 3 Resumen de cuadernos con dispositivos.

Se identifican [*Número en texto*] ([*Valor numérico*]) dispositivos contenedores de evidencia digital ([*Describir los tipos de dispositivos copiados*]), el detalle de los mismos se anexa a la presente acta *(Ver Anexo* [*Identificar si es físico o digital*][*Número secuencial de anexo*]*)* con la siguiente información por cada dispositivo de origen identificado:

1. NÚMERO DEL DISPOSITIVO
2. ANÁLISIS FÍSICO:
	* Radicado del caso al que pertenece.
	* Ubicación exacta (cuaderno y folio) en el que reside el dispositivo.
	* Tipo de dispositivo.
	* Marca.
	* Serial físico.
	* Estado físico.
3. ANÁLISIS LÓGICO:
	* Capacidad total del dispositivo.
	* Espacio utilizado o tamaño.
	* Número de archivos que contiene el dispositivo.
	* Número de carpetas que se encuentran en el dispositivo.
	* Serial lógico.
	* Estado lógico.

**(SÍ APLICA)** Los soportes técnicos de verificación lógica y física del estado de los archivos digitales y la capa física de cada uno de los dispositivos se anexan a la presente acta *(Ver Anexo* [*Identificar si es físico o digital*][*Número secuencial de anexo*]*)*.

1. **COPIA DE DISPOSITIVOS CONTENEDORES DE EVIDENCIA DIGITAL**

Al finalizar la identificación de los dispositivos contenedores de evidencia digital de origen, se procede a hacer la copia de la información contenida en cada uno de los dispositivos utilizando el software [*Listar las herramientas de software empleadas en esta etapa separadas por comas*]. El proceso de copia de los mensajes de datos comienza el día [*Día en letras*] ([*Valor numérico*]) de [*Identificar el mes*] del [*Año en letras*] [*Valor numérico*] a las [*Horas*]:[*Minutos*] [*en formato militar*] y finaliza el [*Día en letras*] ([*Valor numérico*]) de [*Identificar el mes*] del [*Año en letras*] [*Valor numérico*] a las [*Horas*]:[*Minutos*] [*en formato militar*] el informe ejecutivo se anexan a la presente acta *(Ver Anexo* [*Identificar si es físico o digital*][*Número secuencial de anexo*]*),* con la siguiente información detallada:

1. NÚMERO DEL DISPOSITIVO
2. ANÁLISIS FÍSICO:
	* Radicado del caso al que pertenece.
	* Ubicación exacta (cuaderno y folio) en el que reside el dispositivo.
	* Tipo de dispositivo.
	* Marca.
	* Serial físico.
	* Estado físico.
3. ANÁLISIS LÓGICO:
	* Capacidad total del dispositivo.
	* Espacio utilizado o tamaño.
	* Número de archivos que contiene el dispositivo.
	* Número de carpetas que se encuentran en el dispositivo.
	* Serial lógico.
	* Estado lógico.

A continuación, se adjunta un cuadro resumen del total de dispositivos copiados:

**(SÍ APLICA) CUADERNOS PÚBLICOS**

| **TIPO DE DISPOSITIVO** | **NÚMERO DE MENSAJES DE DATOS** | **NÚMERO DE IMÁGENES FORENSES** | **NÚMERO DE CARPETAS** | **TAMAÑO (GB)** |
| --- | --- | --- | --- | --- |
| **NÚMERO DE IMG** | **ARCHIVOS DE IMG** |
| (SEGÚN APLIQUE)[*Tipo de dispositivo*] | [*Identificar en valor numérico el total de archivos usando TreeSize*] | [*Identificar el total de archivos .ad1, L01. E01*] | [*Identificar el total de archivos ad, L y E sin tener en cuenta los .ad1, L01 y .E01*] | [*Identificar en valor numérico el total de carpetas usando TreeSize*] | [*Identificar el tamaño total de la información usando TreeSize*] |

Tabla 4 Total de dispositivos contenedores de evidencia digital copiados, pertenecientes a cuadernos públicos.

[*Emplear una fila por cada tipo de dispositivo*]

**(SÍ APLICA) CUADERNOS RESERVADOS**

| **TIPO DE DISPOSITIVO** | **NÚMERO DE MENSAJES DE DATOS** | **NÚMERO DE IMÁGENES FORENSES** | **NÚMERO DE CARPETAS** | **TAMAÑO (GB)** |
| --- | --- | --- | --- | --- |
| **NÚMERO DE IMG** | **ARCHIVOS DE IMG** |
| (SEGÚN APLIQUE)[*Tipo de dispositivo*] | [*Identificar en valor numérico el total de archivos usando TreeSize*] | [*Identificar el total de archivos .ad1, L01 .E01*] | [*Identificar el total de archivos ad, L y E sin tener en cuenta los .ad1, L01 y .E01*] | [*Identificar en valor numérico el total de carpetas usando TreeSize*] | [*Identificar el tamaño total de la información usando TreeSize*] |

Tabla 5. Total de dispositivos contenedores de evidencia digital copiados, pertenecientes a cuadernos reservados.

[*Emplear una fila por cada tipo de dispositivo*]

Se realiza la anotación de la actividad en la cadena de custodia de estos contenedores de evidencia digital que reposan en el [*Identificar cuaderno y número de folio*] del expediente. La información mantiene su integridad[[2]](#footnote-2) y validez probatoria mediante las imágenes forenses y huellas hash[[3]](#footnote-3) según lo indica el Articulo 11 de la Ley 527 de 1999

Los soportes técnicos de copia (Informe de copia completo y simple) de estos dispositivos se anexan a la presente acta *(Ver Anexo* [*Identificar si es físico o digital*][*Número secuencial de anexo*]*)*. La información mantiene su integridad y validez probatoria mediante las imágenes forenses y huellas hash según lo indica el artículo 11 de la ley 527 de 1999.

1. **ANÁLISIS TÉCNICO DE DISPOSITIVOS DE DESTINO**

**APLICA ÚNICAMENTE SI HAY UN SOLO DISPOSITIVO DESTINO**

El resultado de la copia realizada en la etapa anterior se almacena en un (01) dispositivo contenedor de evidencia digital ([*Describir los tipos de dispositivos de destino*]), **APLICA ÚNICAMENTE SI EL DESTINO ES UN DISCO DURO** debidamente esterilizado, el detalle del dispositivo de destino se adjunta a continuación:

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

Tabla 6 Características técnicas de contenedor de evidencia digital de destino.

El resultado final del proceso se encuentra en el contenedor de evidencia digital anteriormente nombrado. Este contenedor tiene su correspondiente cadena de custodia que reposa en el expediente del caso. La información mantiene su integridad y validez probatoria mediante las imágenes forenses y huellas hash según lo indica el Articulo 11 de la Ley 527 de 1999.

**APLICA ÚNICAMENTE SI HAY MÁS DE UN DISPOSITIVO DESTINO**

El resultado del traslado realizado en la etapa anterior se almacena en [*Número en letras*] ([*Valor numérico*]) dispositivos contenedores de evidencia digital ([*Describir los tipos de dispositivos de destino*]). El detalle de dichos dispositivos ([*Describir los tipos de dispositivos copiados*]) de destino se anexa a la presente acta *(Ver Anexo* [*Identificar si es físico o digital*][*Número secuencial de anexo*]*)* con la siguiente información por cada dispositivo:

1. ANALISIS FISICO:
	* Radicado del caso al que pertenece.
	* Tipo de dispositivo.
	* Marca.
	* Serial físico.
	* Estado físico.
2. ANALISIS LOGICO:
	* Capacidad total del dispositivo.
	* Espacio utilizado o tamaño.
	* Número de archivos que contiene el dispositivo.
	* Número de carpetas que se encuentra en el dispositivo.
	* Serial lógico.
	* Estado lógico.

Se verifica el correcto funcionamiento de [*Número en letras*] ([*Valor numérico*]) dispositivos contenedores de evidencia digital de destino ([*Describir los tipos de dispositivos de destino*]) con el software [*Identificar las herramientas de software empleadas*]. Estos contenedores tienen su correspondiente cadena de custodia que reposa en el expediente del caso. La información mantiene su integridad y validez probatoria mediante las imágenes forenses y huellas hash según lo indica el Articulo 11 de la Ley 527 de 1999.

1. **OBSERVACIONES**
2. **ANEXOS**

De acuerdo a las actividades realizadas anteriormente y el volumen de información, los anexos de la presente acta se entrega un dispositivo ([*Describir los tipos de dispositivos*]) con las siguientes características técnicas:

|  |  |
| --- | --- |
| **DESCRIPCIÓN** | **INFORMACIÓN** |
| Marca | [*Describa marca*] |
| Capacidad | [*Describa capacidad*] |
| Serial Físico | [*Describa serial físico*] |
| Serial Lógico | [*Describa serial lógico*] |
| Número de carpetas | [*Describa número de carpetas*] |
| Número de archivos | [*Describa número de archivos*] |

Tabla 8 Características técnicas del dispositivo anexo al acta.

El cual contiene los siguientes anexos:

| **IDENTIFICADOR** | **DESCRIPCIÓN** | **CANTIDAD DE FOLIOS *(Anexo físico)*** | **RUTA *(Anexo Digital)*** |
| --- | --- | --- | --- |
| [*Número secuencial si aplica*] | Identificación y análisis de dispositivos [*Valor numérico*] contenedores de evidencia digital de origen  | [E*n valor numérico la cantidad de folios*] | [DESCRIBIR TIPO DE DISPOSITIVO]:\ANEXO [*Valor numérico*] – IDENTIFICACIÓN |
| [*Número secuencial si aplica*] | Cuadros resumen de identificación y copia de dispositivos de origen y destino | [E*n valor numérico la cantidad de folios*] | DESCRIBIR TIPO DE DISPOSITIVO]:\ANEXO [*Valor numérico*] – RESUMEN COPIA |
| [*Número secuencial si aplica*] | Paquete de informe de copia de [*Valor numérico*] contenedores de evidencia digital* + - 1. **(SÍ APLICA)** Informe de copia ejecutivo
			2. **(SÍ APLICA)** Informe de inspección del dispositivo de origen
			3. **(SÍ APLICA)** Informe de funcionamiento del dispositivo de origen
			4. **(SÍ APLICA)** Informe de inspección del dispositivo de destino
			5. **(SÍ APLICA)** Informe de funcionamiento del dispositivo de destino
			6. **(SÍ APLICA)** Informe de copia técnico
 | [E*n valor numérico la cantidad de folios*] | DESCRIBIR TIPO DE DISPOSITIVO]:\ANEXO [*Valor numérico*] – INFORMES DE COPIA |
| **TOTAL DE FOLIOS** | **[Totalizar** | **NO APLICA** |

Tabla 9 Cuadro resumen de anexos del acta.

La actividad termina el [*Día en letras*] ([*Valor* numérico]) 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 DE QUIEN REALIZA LA ACTIVIDAD*]**C.C [*CÉDULA*] [*CIUDAD*][*Identificar si es servidor o contratista*]ACE Accessdata Certified Examiner | **Revisado por:**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**[*NOMBRE DE QUIEN REVISA LA ACTIVIDAD*]**C.C [*CÉDULA*] de [*CIUDAD*][*Identificar si es servidor o contratista*]ACE Accessdata Certified Examiner |

1. **DISPOSITIVO N° 1.**

|  |  |  |  |
| --- | --- | --- | --- |
| **TIPO DE ANALISIS** | **CARACTERISTICA** | **DESCRIPCION****DISPOSITIVO ORIGEN** | **DESCRIPCION DE DISPOSITIVO DESTINO** |
| **ANÁLISIS FÍSICO** | Radicado | [*Indicar el número de radicado*] | [*Indicar el número de radicado*] **(SI APLICA)** |
| Ubicación | Cuaderno | [*Identificar si es público o reservado*] | [*Identificar si es público o reservado*] **(SI APLICA)** |
| Folio | [*Identificar folio*] | [*Identificar folio*] **(SI APLICA)** |
| Tipo de Dispositivo | [*Identificar tipo de dispositivo*] | [*Identificar tipo de dispositivo*] |
| Marca | [*Identificar marca*]  | [*Identificar marca*]  |
| Serial Físico | [*Identificar serial físico*]  | [*Identificar serial físico*]  |
| Estado Físico | [*Identificar el estado físico del dispositivo*] | [*Identificar el estado físico del dispositivo*] |
| **ANÁLISIS LÓGICO** | Capacidad total | [*Identificar en GB la capacidad del dispositivo*] | [*Identificar en GB la capacidad del dispositivo*] |
| Espacio utilizado o tamaño | [*Identificar en GB el espacio utilizado en el dispositivo*] | [*Identificar en GB el espacio utilizado en el dispositivo*] |
| Número Archivos | [*Cantidad de archivos*] | [*Cantidad de archivos*] |
| Número Carpetas | [*Cantidad de carpetas*] | [*Cantidad de carpetas*] |
| Serial Lógico | [*Identificar serial lógico*] | [*Identificar serial lógico*] |
| Estado Lógico | [*Identificar el estado lógico* (óptimo, malo)] | [*Identificar el estado lógico* (óptimo, malo)] |

**DISPOSITIVO 1**

1. **INFORME DE COPIA EJECUTIVO**

**INCLUIR INFORME DE COPIA EJECUTIVO**

1. **(SÍ APLICA) INFORME DE INSPECCIÓN DEL DISPOSITIVO DE ORIGEN**

|  |
| --- |
| [*Incluir el informe de inspección*] |

1. **(SÍ APLICA) INFORME DE FUNCIONAMIENTO DEL DISPOSITIVO DE ORIGEN**

|  |
| --- |
| [*Incluir el informe de funcionamiento*] |

1. **(SÍ APLICA) INFORME DE INSPECCIÓN DEL DISPOSITIVO DE DESTINO**

|  |
| --- |
| [*Incluir el informe de inspección*] |

1. **(SÍ APLICA) INFORME DE FUNCIONAMIENTO DEL DISPOSITIVO DE DESTINO**

|  |
| --- |
| [*Incluir el informe de funcionamiento*] |

1. **(SÍ APLICA) INFORME TÉCNICO DE COPIA DEL DISPOSITIVO DE ORIGEN AL DESTINO**

|  |
| --- |
| [*Incluir el informe de técnico*] |

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)
2. “Propiedad de salvaguardar la precisión y completitud de los recursos NORMA ISO 27001, Términos y definiciones.” [↑](#footnote-ref-2)
3. ” Es una operación que se realiza sobre un conjunto de datos de cualquier tamaño, de forma que el resultado obtenido es otro conjunto de datos de tamaño fijo, independientemente del tamaño original, y que tiene la propiedad de estar asociado unívocamente a los datos iniciales, es decir, es imposible encontrar dos mensajes distintos que generen el mismo resultado al aplicar la Función hash. Fuente: Agencia Española de Protección de Datos Personales: https://www.agpd.es/portalwebAGPD/canalresponsable/inscripcion\_ficheros/preguntas\_frecuentes/glosario/index-ides-idphp.php” [↑](#footnote-ref-3)