|  |  |
| --- | --- |
| **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, a los [*Día en letras*] ([*Día en números*]) días del mes 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**), desde las instalaciones de la Entidad ubicadas en la carrera 13 # 27 – 00, piso 6, ala sur, donde se encuentra el Laboratorio de Informática Forense, y por comisión de la (del) *[ESCRIBIR LA DELEGATURA O SI FUE POR EL COORDINADOR]* procede a realizar el acompañamiento con el propósito de generar una copia forense y crear la correspondiente imagen de los mensajes de datos[[1]](#footnote-1) alojados en la(s) cuenta(s) de correo electrónico y/o cuenta(s) de almacenamiento en la nube, conforme a lo solicitado en el marco de la visita administrativa de inspección con expediente No. *[NÚMERO DE RADICADO*].

Dicha diligencia se realiza en cumplimiento del objeto establecido en la credencial de visita, la cual señala: “(…) *[ESCRIBIR EL OBJETO DE LA VISITA OBTENIDO DE LA CREDENCIAL DE VISITA TEXTUALMENTE] (…)”*, dirigida a la empresa *[NOMBRE EMPRESA O ENTIDAD]*.

1. **DESCRIPCIÓN DEL REQUERIMIENTO**

De conformidad con las facultades otorgadas a la **SIC**, en especial las previstas en los numerales 56, 57 y 58 del artículo 1 del Decreto 4886 de 2011, modificado por el Decreto 092 de 2022[[2]](#footnote-2), la (el) *[Coordinador del Grupo de Trabajo o Delegatura]* ha comisionado al (la) ingeniero(a)**[NOMBRE DEL INGENIERO(A) FORENSE]** para llevar a cabo la copia y creación de imagen forense de los mensajes de datos alojados en la(s) cuenta(s) de correo electrónico y/o cuenta(s) de almacenamiento en la nube, solicitados en el marco de la visita administrativa de inspección con expediente No. *[EN NÚMERO EL RADICADO]*.

Dado que el proceso de copia de la información desde el dispositivo de origen (servidor en la nube) podría superar el tiempo estimado para la presente diligencia, se ha contemplado esta alternativa como mecanismo para garantizar la continuidad del procedimiento, por lo anterior y para tal fin, la **SIC** dispone de una infraestructura adecuada, que incluye conexión segura y robusta a Internet, así como herramientas especializadas, licenciadas y avaladas para este tipo de procedimientos.

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

A continuación, se relacionan las herramientas de software y hardware empleadas durante la ejecución de la actividad de copia y creación de la imagen forense de los mensajes de datos exportados, con el fin de garantizar la integridad, trazabilidad y validez técnica de los procedimientos realizados:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **SOFTWARE/HARDWARE** | **PROPÓSITO** | **NOMBRE** | **VERSIÓN** | **FABRICANTE** |
| [*Software o Hardware*] | [*Describir el propósito u objetivo de la herramienta utilizada*] | [*Nombre del software o placa SIC del hardware*] | [*Versión del software o modelo del hardware*] | [*Nombre del fabricante o marca*] |
| [*Software o Hardware*] | [*Describir el propósito u objetivo de la herramienta utilizada*] | [*Nombre del software o placa SIC del hardware*] | [*Versión del software o modelo del hardware*] | [*Nombre del fabricante o marca*] |

Tabla 1. Relación de herramientas de software y hardware utilizadas en la actividad.

1. **CORREOS ELECTRÓNICOS Y/O CUENTAS DE ALMACENAMIENTO EN LA NUBE SOLICITADOS**

De acuerdo con las autorizaciones otorgadas por el(la) representante legal o el(la) titular de la información, a continuación, se relaciona(n) la(s) cuenta(s) de correo electrónico y/o cuenta (s) de almacenamiento en la nube sobre las cuales se aplicó el procedimiento descrito en la presente acta:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **NOMBRE DEL PROPIETARIO** | **CARGO** | **CUENTA DE CORREO / USUARIO** | **SERVIDOR DE CORREO O PROVEEDOR DEL SERVICIO** | **TIPO DE EVIDENCIA DIGITAL** |
| [*Nombre de la persona dueña del correo*] | [*Cargo de la persona dueña del correo*] | [*Correo electrónico o cuenta*] | [*Servidor de correo electrónico o Proveedor de Almacenamiento en la Nube*] | [*Correo electrónico o Almacenamiento en la Nube*] |

Tabla 2. Listado del (los) correo(s) electrónico(s) y/o cuenta(s) de almacenamiento en la nube solicitada(s).

1. **DESCRIPCIÓN GENERAL DE LA ACTIVIDAD**

Se llevó a cabo la descarga de los mensajes de datos contenidos en la(s) cuenta(s) de correo electrónico y/o cuenta (s) de almacenamiento en la nube descritas en la sección anterior, desarrollando la actividad en [*Número en letras*] etapas, así:

1. **Selección de la fuente de extracción de los mensajes de datos de correos electrónicos:** Mediante el uso del software *[Escribir el software]*, se especificó el origen de los datos a respaldar, para este caso se seleccionó la opción: [Listar las opciones separadas por comas como aparece en el software, ejemplo: *Cloud-based formats: Microsoft 365, Outlook.com, Hotmail.com (vía graph API)]*, que permite conectar con el servidor de correo electrónico mediante el uso de las credenciales de inicio de sesión (usuario y contraseña) y doble factor de autenticación, si lo requiere la cuenta, evitando la perdida de la información del servidor.

Una vez culminado el proceso de copia del (los) buzón(es) de correo de la(s) cuenta(s),la herramienta de software *[Escribir el software]* genera el(los) informe(s) correspondiente(s), donde se consignan la hora de inicio, la duración de la actividad, los errores encontrados, y las estadísticas del proceso (elementos completados, procesados, filtrados, inválidos y no procesados), los cuales se encuentran alojados en el dispositivo de almacenamiento destino (*[Especificar tipo de dispositivo destino, ejemplo: disco duro externo]*) y en el Anexo *[Especificar número del anexo]* de la presente acta.

1. **(si aplica) Configuración de exportación de los mensajes de datos de correos electrónicos:** Se configuró el formato del archivo de salida de la copia del (los) buzón(es) de correo(s) electrónico(s) a un archivo compuesto tipo (**si aplica**) PST(Microsoft Outlook Personal Storage Table) que permite almacenar los correos electrónicos, contactos, calendarios y otros elementos en un solo archivo **u** (**si aplica**) OST (Offline Storage Table) que permite almacenar una copia local de los correos electrónicos, calendarios, contactos y otros elementos de la cuenta de correo electrónico.
2. **(si aplica) Selección de la fuente de extracción de los mensajes de datos de cuentas de almacenamiento en la nube:** Se utilizó el software *[Escribir el software]* para la copia de los mensajes datos desde cuentas de almacenamiento en la nube, conectando con el servidor correspondiente mediante credenciales de inicio de sesión.
3. **(si aplica) Configuración de exportación de los mensajes de datos de cuentas de almacenamiento en la nube:** Se configuró el formato de salida de la copia de los datos extraídos desde la(s) cuenta(s) de almacenamiento en la nube en formato [*Especificar Formato*], asegurando la integridad de la información.
4. **Adquisición de imagen forense:** Los mensajes de datos recopilados fueron transferidos a un dispositivo destino ([se especifica tipo de dispositivo destino, ejemplo: disco duro externo]) utilizando la herramienta de software [especificar software de copia, ejemplo: FastCopy] (ver informe de copia en el Anexo [especificar el número del anexo]), posteriormente, se realizó la adquisición de una imagen forense por cada uno de los buzón(es) de correo electrónico y/o cuenta(s) almacenamiento en la nube o mensajes de datos descargados. Esta imagen fue generada y verificada con el software **FTK Imager**, garantizando la integridad[[3]](#footnote-3) e inalterabilidad de los datos mediante la Huella HASH[[4]](#footnote-4). El desarrollo de esta actividad se detalla en las secciones siguientes de la presente acta.
5. **Análisis técnico del dispositivo de destino**: Se realizó la identificación del dispositivo contenedor de evidencia digital, en el cual reposarán los mensajes de datos compilados anteriormente. En esta etapa se realizan dos análisis: (i) **análisis físico**, en donde se identificaron las características físicas del contenedor de evidencia digital destino, es decir, el tipo de dispositivo, la marca, la capacidad, el embalaje, el serial físico y el estado físico. Y (ii) **análisis lógico**, en donde se identificaron las características lógicas del dispositivo contenedor de evidencia digital destino, es decir, la capacidad del dispositivo, el serial lógico, el número de archivos, las carpetas y el estado lógico. Para esta etapa se utilizaron la(s) herramienta(s) de software [*Listar las herramientas de software empleadas en esta etapa separadas por comas*], así como la(s) herramienta(s) de hardware [*Listar las diferentes herramientas de hardware empleadas durante esta etapa separadas por comas*].
6. **PROCEDIMIENTO FORENSE DE IDENTIFICACIÓN, PRESERVACIÓN Y ADQUISICIÓN DE IMAGEN FORENSE**

A continuación, se describe cronológicamente el procedimiento forense realizado para la identificación, recolección, preservación y adquisición de la imagen forense de los mensajes de datos contenidos en la(s) cuenta(s) de correo electrónico y/o cuenta(s) de almacenamiento en la nube previamente mencionadas.

**[EN ESTA SECCIÓN DE DEBEN LISTAR LAS ACTIVIDADES REALIZADAS CRONOLÓGICAMENTE]**

A las XX:XX:XX horas del (si aplica) *[mismo día]* o [*Día en letras*] ([*Día en números*]) de [*Mes en letras*] del año [*Año en letras*] ([*Año en números*]), se *[inicia la configuración de, realiza la configuración de, configura, etc.…]* la herramienta de software *[****Escribir el software******en negrilla****]* para *[iniciar, realizar, proceder con, etc.…]* la copia exacta del buzón de correo electrónico asociado a la cuenta *[identificar la cuenta de correo electrónico o almacenamiento en la nube].*

***(Si aplica)* En la copia del correo electrónico de la cuenta [*cuenta de correo electrónico o almacenamiento en la nube*] se presenta un error por [describir la causa: falta de internet, fallo en la autenticación, etc.], por lo cual se procede a [*describir las acciones correctivas tomadas*].**

Siendo las XX:XX:XX horas del mismo día, se configura nuevamente la herramienta *[****Escribir el software******en negrilla****]* para *[iniciar, realizar, proceder con, etc.…]* con la copia exacta del buzón de correo electrónico asociado a la cuenta *[identificar la cuenta de correo electrónico o almacenamiento en la nube]*.

***(Si aplica)* Durante el proceso la copia del correo electrónico de la cuenta *[cuenta de correo electrónico o almacenamiento en la nube],* se presentó un inconveniente relacionado con *[describir la causa, si aplica],* por ende, se adoptaron las siguientes medidas[*describir las acciones correctivas tomadas*].**

**(si aplica) [PÁRRAFO SI EL PROCESO DE COPIA FINALIZA DURANTE EL TRANSCURSO DEL DÍA ANTES DE SUSPENDER ACTIVIDADES]**

A las XX:XX:XX [Referenciar la hora de inicio de adquisición de la imagen forense] horas del mismo día, una vez finalizado el proceso de *[****Escribir el software******en negrilla****]* para *[identificar la cuenta de correo electrónico o almacenamiento en la nube]*, se procede con la creación de la imagen forense correspondiente utilizando el software *[****Escribir el software de adquisición de imágenes forenses******en negrilla, e.g., FTK Imager****]*, que finaliza el mismo día a las XX:XX:XX [Referenciar la hora de finalización de la adquisición de la imagen forense] horas.

La imagen forense, en formato .AD1, fue verificada con éxito y se compone de: (i) un archivo digital de imagen forense .AD1, segmentado en *[Cantidad de archivos .AD en letras]* (*[Cantidad de archivos .AD en números]*) parte(s); (ii) un archivo digital en formato de texto .TXT; y (iii) un archivo digital en formato de valores separados por comas .CSV. A continuación, se presenta el informe técnico de adquisición de la herramienta forense:

|  |
| --- |
| *[Poner el informe de adquisición de la herramienta FTK-Imager]* |

Log de Adquisición 1. Informe técnico generado por la herramienta FTK Imager para la imagen forense denominada [nombre la imagen forense].

**(si aplica) [PÁRRAFO PARA SUSPENSIÓN TEMPORAL]**

Siendo las XX:XX horas del [*Día en letras*] ([*Día en números*]) de [*Mes en letras*] del año [*Año en letras*] ([*Año en números*]), se suspenden las actividades en el Laboratorio de Informática Forense de la **SIC**, para continuar el día siguiente.

**(si aplica) [PÁRRAFO PARA REANUDACIÓN DE ACTIVIDADES]**

A las XX:XX horas del [*Día en letras*] ([*Día en números*]) de [*Mes en letras*] del año [*Año en letras*] ([*Año en números*]), se reanudan las actividades de apoyo remoto desde el Laboratorio Forense de la **SIC**.

**[PÁRRAFO SI EL PROCESO DE COPIA FINALIZA DURANTE LA NOCHE]**

A las XX:XX:XX horas del [*Día en letras*] ([*Día en números*]) de [*Mes en letras*] del año [*Año en letras*] ([*Año en números*]), tras verificar que el proceso de *[****Escribir el software******en negrilla****]* para la cuenta *[identificar la cuenta de correo electrónico o almacenamiento en la nube]* culmina con éxito y posterior al traslado de la descarga al dispositivo destino [Si aplica], se procede con la creación de la imagen forense correspondiente utilizando el software *[****Escribir el software de adquisición de imágenes forenses******en negrilla, e.g., FTK Imager****]*, que finaliza el mismo día a las XX:XX:XX horas.

La imagen forense, en formato .AD1, fue verificada con éxito y se compone de: (i) un archivo digital de imagen forense .AD1, segmentado en *[Cantidad de archivos .AD en letras]* (*[Cantidad de archivos .AD en números]*) parte(s); (ii) un archivo digital en formato de texto .TXT; y (iii) un archivo digital en formato de valores separados por comas .CSV. A continuación, se presenta el informe técnico de adquisición de la herramienta forense:

|  |
| --- |
| *[Poner el informe de adquisición de la herramienta FTK-Imager]* |

Log de Adquisición 2. Informe técnico generado por la herramienta FTK Imager para la imagen forense denominada [nombre la imagen forense].

Siendo las XX:XX horas del [*Día en letras*] ([*Día en números*]) de [*Mes en letras*] del año [*Año en letras*] ([*Año en números*]), se da por terminado el apoyo técnico remoto para la empresa/entidad/asociación **[PONER NOMBRE DE LA EMPRESA ENTIDAD O ASOCIACIÓN]**.

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

Todos los mensajes de datos recaudados y las imágenes forenses adquiridas en el presente radicado se almacenan en [*Cantidad de contenedores en letras*] ([*Cantidad de contenedores en números*]) contenedor(es) de evidencia digital ([Tipo de dispositivos]) con las siguientes características técnicas:

**DISPOSITIVO [Poner número de dispositivo, si son más de uno listar varios cuadros]**

|  |  |  |
| --- | --- | --- |
|  |  | **DISPOSITIVO DESTINO** |
| **ANÁLISIS FÍSICO** | **Radicado** | [Diligenciar este campo] |
| **Ubicación** | [Diligenciar este campo] |
| **Tipo de Dispositivo** | [Disco Duro Externo / USB/DVD/CD -Escoger el tipo de dispositivo] |
| **Marca** | [Diligenciar este campo] |
| **Serial Físico** | [Diligenciar este campo] |
| **Estado Físico** | [óptimo / Deteriorado / roto, entre otros] |
| **ANÁLISIS LÓGICO** | **Capacidad total** | [Diligenciar este campo] |
| **Espacio utilizado o tamaño** | [Diligenciar este campo] |
| **Número Archivos** | [Diligenciar este campo] |
| **Número Carpetas** | [Diligenciar este campo] |
| **Serial Lógico** | [Diligenciar este campo] |
| **Estado Lógico** | [Óptimo / Con Errores] |

Tabla 3. Resumen de información contenedor de evidencia digital “[Poner número del radicado]”.

1. **OBSERVACIONES**
2. [Ejemplo: Todos los mensajes de datos fueron alojados y custodiados en [cantidad de dispositivos destino en letras] (cantidad de dispositivos destino en número) [Tipo de dispositivo destino, ejemplo: disco(s) duro(s) externo(s)] con S/N: [Poner serial físico del o los dispositivos destino(s) de soporte remoto], junto con sus respectiva(s) cadena(s) de custodia, la(s) cual(es) es(son) entregada(s) en el proceso de unificación del presente radicado y reposará(n) en el expediente.
3. [ejemplo: Se envía desde la cuenta lifsic@sic.gov.co correo de terminación de la actividad a cada una de las cuentas de correo electrónico o almacenamiento en la nube objeto del procedimiento de adquisición y creación de imagen forense.]
4. **ANEXOS**

De acuerdo con las actividades realizadas anteriormente y el volumen de información, los anexos de la presente acta se entregan en un dispositivo óptico ([Especificar el dispositivo óptico empleado ejemplo: CD o DVD]) con las siguientes características técnicas:

|  |  |
| --- | --- |
| **DESCRIPCIÓN** | **INFORMACIÓN** |
| Marca | [Diligenciar este campo] |
| Capacidad | [Diligenciar este campo] |
| Tamaño | [Diligenciar este campo] |
| Serial Físico | [Diligenciar este campo] |
| Serial Lógico | [Diligenciar este campo] |
| Número de carpetas | [Diligenciar este campo] |
| Número de archivos | [Diligenciar este campo] |

Tabla 4. Características técnicas del dispositivo anexo al acta.

|  |  |  |  |
| --- | --- | --- | --- |
| **IDENTIFICADOR** | **DESCRIPCIÓN** | **CANTIDAD DE FOLIOS *(Anexo físico)*** | **RUTA *(Anexo Digital)*** |
| 1 | Informe(s) técnico(s) generado(s) por la herramienta de copia de correos electrónicos [NOMBRE DEL SOFTWARE] | X | No aplica |
| 2 | Informe(s) técnico(s) generado(s) por la herramienta de copia de las cuentas de almacenamiento en la nube [NOMBRE DEL SOFTWARE] | X | No aplica |
| 3 | Informe(s) generados por [NOMBRE DEL SOFTWARE], software usado para la copia de archivos y directorios. | X | No aplica |

Tabla 5. Resumen de los anexos del acta

A continuación, se presentan la estructura de archivos y carpetas del dispositivo, tomada con el software **TreeSize**:

|  |
| --- |
|  |

Imagen 1. Informe de estructura de archivos y carpetas del dispositivo óptico ([Tipo de dispositivo, ejemplo DVD o CD]) que contiene los anexos digitales de la presente acta, tomado con el software TreeSize. Captura de pantalla tomada con la herramienta recortes de Windows.

Asimismo, se adjunta el informe de funcionamiento del dispositivo óptico, generado con el software **VSO-Inspector**:

|  |
| --- |
|  |

Texto 1. Informe de correcto funcionamiento de dispositivos ópticos, tomado con el software VSO-Inspector.

La actividad y creación de la presente acta 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*] horas, firman los encargados de las actividades técnicas mencionadas y la revisión de la presente acta por parte del GTIFSD,

|  |  |
| --- | --- |
| **Realizado por:**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**NOMBRE**CC. CÉDULA de CIUDADServidor Público y/o Contratista Exterro ACE - AccessData Certified Examiner | **Revisado por:**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**NOMBRE**CC. CÉDULA de CIUDADServidor Público (Coordinador y grupo) y/o Contratista – Exterro 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)
2. D. 4886/2011, art. 1, numerales 56, 57 y 58 modificados por el art. 1 del D. 92 de 2022. *“La Superintendencia de industria y Comercio ejercerá las siguientes funciones. (. . .) 56. Realizar visitas de inspección, decretar y practicar pruebas y recaudar toda la información conducente, con el fin de verificar el cumplimiento de las disposiciones legales cuyo control le compete y adoptar las medidas que correspondan conforme a la ley. 57. Solicitar a las personas naturales y jurídicas el suministro de datos, informes, libros y papeles de comercio que se requieran para el correcto ejercicio de sus funciones. 58. Interrogar, bajo juramento y con observancia de las formalidades previstas para esta clase de pruebas en el Código General del Proceso. a cualquier persona cuyo testimonio pueda resultar útil para el esclarecimiento de los hechos durante el desarrollo de sus funciones*”. [↑](#footnote-ref-2)
3. Propiedad de salvaguardar la precisión y completitud de los recursos NORMA ISO 27001, Términos y definiciones. [↑](#footnote-ref-3)
4. 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/indexides-idphp.php [↑](#footnote-ref-4)