

RECOLECCIÓN Y ADQUISICIÓN DE EVIDENCIA DIGITAL FORENSE - CLOUD

1. OBJETO:

Describir el proceso para la identificación, recolección y adquisición de evidencia digital en entornos de infraestructura en nube que asegure su integridad y autenticidad, mitigando el riesgo de alteración para su posterior investigación y análisis forense para respuesta a incidentes de ciberseguridad.

2. ALCANCE:

El protocolo aplica para todos los funcionarios y contratistas involucrados en la recolección y adquisición de evidencias digitales en incidentes cibernéticos.

Este protocolo se aplica a entornos en la nube que la entidad tenga contratado.

3. DEFINICIONES:

Adquisición de evidencia digital: Consiste en generar una réplica exacta de datos dentro de un entorno previamente determinado.

Cadena de Custodia: El proceso de documentación que asegura el control, transferencia, análisis y disposición de la evidencia desde el momento de su recolección hasta su presentación en un proceso legal.

Copia Bit a Bit: Proceso de creación de una réplica exacta y completa de un dispositivo de almacenamiento, en el cual se copian todos los bits de datos, tanto asignados como no asignados. La copia bit a bit también se denomina copia física.

DEFR (Digital Evidence First Responder): Individuo que puede desempeñar las funciones de un DEFR y cuenta con conocimientos especializados, habilidades y capacidades para abordar una variedad de problemas técnicos.

DES (Digital Evidence Specialist): Individuo que puede desempeñar las funciones de un DEFR y cuenta con conocimientos especializados, habilidades y capacidades para abordar una variedad de problemas técnicos.

RECOLECCIÓN Y ADQUISICIÓN DE EVIDENCIA DIGITAL FORENSE - CLOUD

Embalado: Disponer en balas o colocar convenientemente dentro de cubiertas la evidencia digital que han de transportarse o almacenarse.

Evidencia Digital: Información o datos, guardados o transmitidos en formato binario, que pueden considerarse confiables como prueba.

Recolección: recolección de objetos físicos que contienen evidencia digital potencial.

Rotulado: Etiquetar cada dispositivo de manera clara, por medio del formato dispuesto, en el cual se incluye un identificador único que se refleje en la documentación de la cadena de custodia, fecha, hora, nombre del investigador, descripción de la evidencia.

Snapshot: Copia completa de solo lectura de un disco duro virtual (VHD).

Suma de Verificación (Valor Hash): Cadena única generada a partir de datos mediante una función hash criptográfica. Se utiliza para verificar la integridad de los datos.

Verificación de la Imagen: Verificar que la imagen adquirida sea una réplica exacta del dispositivo original comparando los valores hash.

4. PRINCIPIOS FUNDAMENTALES

4.1. Minimización del Manejo

La manipulación directa de dispositivos digitales originales debe ser mínima para prevenir alteraciones o daños a la evidencia. Siempre que sea posible, se deben utilizar copias forenses o bit a bit en lugar de los dispositivos originales.

4.2. Documentación Detallada

Todas las acciones, decisiones y observaciones realizadas durante el manejo de evidencia digital deben ser documentadas de manera exhaustiva y precisa. Esta documentación es crucial para garantizar la trazabilidad y la efectividad del análisis durante la respuesta a incidentes.

RECOLECCIÓN Y ADQUISICIÓN DE EVIDENCIA DIGITAL FORENSE - CLOUD

4.3. Consideraciones sobre la privacidad

No se debe realizar ningún procedimiento de recolección o análisis forense en instancias o servicios de nube pública que puedan comprometer la privacidad de otras entidades o usuarios que comparten la misma infraestructura.

Si existen indicios de posible evidencia digital decisiva en otros recursos de la nube y el incidente es grave o muy grave, se recomienda solicitar el apoyo de los involucrados o presentar una denuncia ante las autoridades competentes.

Las demás evidencias recopiladas deben ser entregadas como pruebas para respaldar la investigación.

4.4. Transparencia

Todas las técnicas y procedimientos empleados en la recolección y adquisición de evidencia digital deben estar claramente documentados y ser accesibles, de manera que otros expertos puedan replicar el proceso y obtener los mismos resultados. Esto es especialmente crucial en situaciones donde una respuesta a incidentes derive en una investigación judicial, asegurando así la integridad y validez de las pruebas presentadas.

5. ROLES Y RESPONSABILIDADES

En el marco de investigación de incidentes de ciberseguridad es importante definir los roles mínimos necesarios para realizar las etapas de investigación forense, estos roles dependerán del conocimiento y capacidades.

TABLA 1 ROLES Y RESPONSABILIDADES

ETAPA	ROL	RESPONSABILIDADES
Notificación y Evaluación inicial	- Oficial de Seguridad de la Información. - Jefe Oficina TIC	Recibir la notificación del incidente y coordinar la evaluación inicial. Decidir si es necesario activar al DEFR y al DES.
Identificación	DEFR: Oficial de Seguridad y Soporte Técnico II	El Oficial de Seguridad debe coordinar con el administrador de infraestructura para identificar recursos y servicios relevantes en Azure.

RECOLECCIÓN Y ADQUISICIÓN DE EVIDENCIA DIGITAL FORENSE - CLOUD

ETAPA	ROL	RESPONSABILIDADES
Recolección	DEFR: Soporte técnico II	Ejecutar la recolección inicial y asegurar que los datos recolectados sean íntegros y almacenados en forma segura.
Adquisición	DEFR / DES: Oficial de Seguridad y Soporte Técnico II	Realizar la adquisición de la evidencia digital no volátil utilizando herramientas forenses, asegurando la integridad de esta.

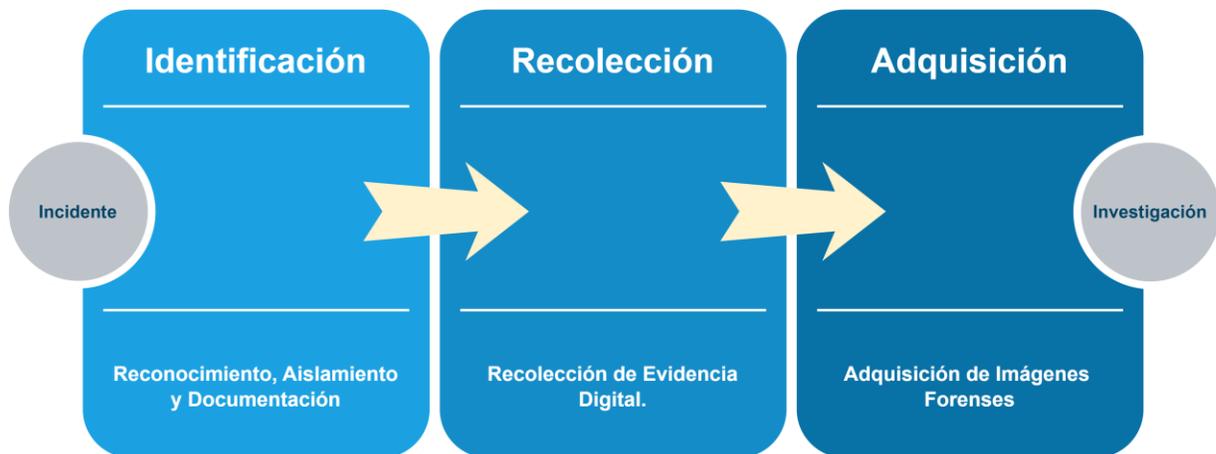
Fuente: Elaboración propia

Para entornos en la nube, la identificación debe realizarse entre el personal de soporte técnico nivel II o el administrador de infraestructura y el Oficial de Seguridad.

6. PROTOCOLO DE ACTUACIÓN Y TAREAS

El protocolo para gestión de Evidencia Digital Forense en la nube se compone de tres fases: Identificación, Recolección y Adquisición.

Ilustración 1 Fases del Protocolo de gestión de la evidencia digital en Nube



Fuente: Elaboración Propia

6.1. Fase: Identificación de la Evidencia

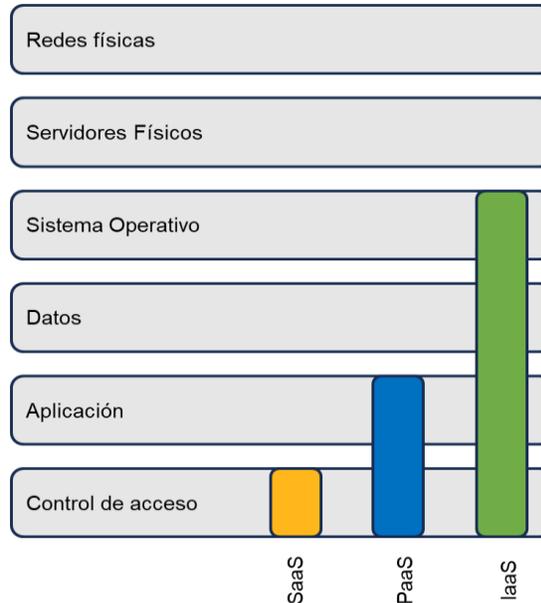
Para entornos Cloud o nube, se debe determinar qué elementos deben ser preservados como evidencia y evaluar su relevancia en el contexto del incidente cibernético.

Para lo anterior realice:

RECOLECCIÓN Y ADQUISICIÓN DE EVIDENCIA DIGITAL FORENSE - CLOUD

A. Identifique el nivel de acceso o control sobre el modelo de servicio en la nube de acuerdo con el siguiente gráfico.

Ilustración 2 Control en los modelos de servicio en nube



Fuente: Elaboración Propia

B. Según el modelo de servicio en la nube, elabore una lista de los elementos relevantes, sin limitarse únicamente a estos:

TABLA 2 GUÍA DE ELEMENTOS RELEVANTES DE NUBE

Datos	SaaS	PaaS	IaaS
Registros de acceso y actividad	Incluye logs de acceso, registros de auditoría, y detalles de la actividad de los usuarios dentro del software.	Logs de acceso a la plataforma y a las aplicaciones desplegadas en el entorno PaaS.	Logs de acceso al entorno de infraestructura, así como al sistema operativo, y servicios desplegados.
Metadatos de archivos	Información como fecha de creación, modificación y eliminación de archivos almacenados o manejados por el SaaS.	Metadatos relacionados con las aplicaciones desplegadas como registros de acceso y datos de rendimiento de la aplicación.	Metadatos del sistema operativo o de registros del sistema operativo.

RECOLECCIÓN Y ADQUISICIÓN DE EVIDENCIA DIGITAL FORENSE - CLOUD

Datos	SaaS	PaaS	IaaS
Configuraciones	Políticas y configuraciones de control de acceso aplicadas.	Aplicación: Detalles sobre la configuración de las aplicaciones, incluyendo control de versiones, despliegue, y acceso a APIs.	Red y Seguridad: Reglas de firewall, configuraciones de red, listas de control de acceso (ACLs).
Eventos y Estado	Autenticación: Registros de inicio y cierre de sesión, intentos fallidos, autenticaciones exitosas.	Aplicaciones: Información sobre la ejecución de aplicaciones, errores, y otras actividades de la aplicación.	Estado de las máquinas virtuales: Detalles sobre las instancias de máquinas virtuales (VMs), incluyendo snapshots y estados actuales.
Bases de Datos y Almacenamiento	N/A	Metadatos relacionados con bases de datos y almacenamiento manejado por la plataforma.	Metadatos, logs de transacciones, auditoría y acceso, estructura de la base de datos. Identificación de discos, sistemas de archivos y volúmenes de almacenamiento.

Fuente: Elaboración propia

6.1.1. Criterios de volatilidad.

En una investigación forense en la nube, es importante tener en cuenta que muchos de los datos pueden ser volátiles debido a la naturaleza dinámica del entorno y a los accesos constantes.

Es crucial que nunca se apague una máquina virtual ni se altere su estado, ya que esto podría provocar la pérdida de información valiosa. En su lugar, aíse la máquina y realice un snapshot para preservar su estado en el momento de la investigación.

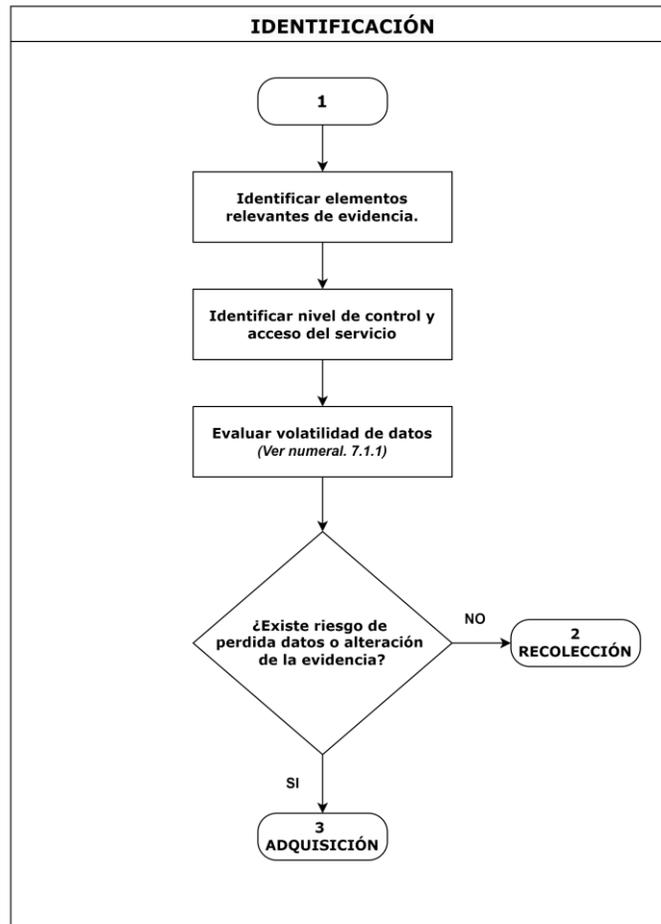
Siga los pasos recomendados por el proveedor, por ejemplo:

RECOLECCIÓN Y ADQUISICIÓN DE EVIDENCIA DIGITAL FORENSE - CLOUD

<https://learn.microsoft.com/en-us/azure/virtual-machines/snapshot-copy-managed-disk?tabs=portal>

6.1.2. Diagrama

Ilustración 3 Diagrama de flujo Fase Identificación



Fuente: Elaboración propia

6.2. Fase: Recolección

A diferencia de entornos tradicionales OnPremise, un proceso de informática forense en la nube está limitado por el proveedor de servicios por lo que la recolección se hace directamente desde interfaces API, herramientas del proveedor o descargas de registros y snapshots.

Para lo anterior, considere realizar las siguientes actividades de acuerdo con la naturaleza del caso y la identificación de la fase anterior.

RECOLECCIÓN Y ADQUISICIÓN DE EVIDENCIA DIGITAL FORENSE - CLOUD

6.2.1. Consideraciones Generales

Aislamiento: Aísle los sistemas antes de la recolección para evitar cambios adicionales en los datos.

Integridad: Asegure la integridad de los datos recolectados utilizando herramientas que permitan realizar hash (SHA-256).

Para esto, use la interfaz de línea de comandos del proveedor de nube como por ejemplo Azure CLI o exporte las evidencias a un archivo local y use el comando sha256sum <snapshot-file>.

Documentación: Documente cada paso del proceso, incluyendo herramientas utilizadas, fechas y horas, y descripciones detalladas de los elementos recolectados.

6.2.2. Priorización.

Para la recolección de evidencia, es fundamental priorizar según la volatilidad de los datos, siguiendo estas consideraciones:

TABLA 3 NIVELES DE VOLATILIDAD DE LA EVIDENCIA DIGITAL

Volatilidad	Elementos
Alto	Memoria RAM, Logs de autenticación y acceso, registros de aplicaciones.
Medio	Snapshots de sistemas operativos y bases de datos.
Bajo	Datos exportados, copias de seguridad.

Fuente: Elaboración propia

6.2.3. Modelo IaaS

TABLA 4 ACCIONES DE RECOLECCION DE EVIDENCIA EN SERVICIOS IAAS

Infraestructura Como Servicio IaaS			
Elemento	Acciones	Herramientas Sugeridas	Consideraciones
Máquina Virtual (VM)	Realizar snapshot	Veeambackup Azure CLI, AWS CLI, GCP CLI	No apagar ni reiniciar la VM. Aislar la VM antes del snapshot.
Volúmenes de Almacenamiento	Clonar o snapshot del volumen	Veeambackup Azure Disk Snapshot, AWS	Asegurar la integridad de los volúmenes antes de

RECOLECCIÓN Y ADQUISICIÓN DE EVIDENCIA DIGITAL FORENSE - CLOUD

Infraestructura Como Servicio IaaS			
Elemento	Acciones	Herramientas Sugeridas	Consideraciones
		EBS Snapshot	la clonación.
Logs del Sistema Operativo	Descargar y exportar logs	Syslog, Azure Monitor, AWS CloudWatch	Priorizar los logs de autenticación y actividad reciente.
Bases de Datos	Exportar y respaldar bases de datos	mysqldump, pg_dump, Azure SQL Backup	Recolectar tanto datos como metadatos de la base de datos.

Fuente: Elaboración propia

De acuerdo con los recursos y servicios desplegados en la nube, puede considerar usar herramientas externas para la recolección.

6.2.4. Modelo PaaS.

TABLA 5 ACCIONES DE RECOLECCION DE EVIDENCIA EN SERVICIOS PAAS

Plataforma Como Servicio PaaS			
Elemento	Acciones	Herramientas Sugeridas	Consideraciones
Logs de Aplicación	Descargar registros de la aplicación	Azure App Service Logs, AWS CloudTrail	Identificar y priorizar los eventos críticos de seguridad.
Configuraciones de Servicio	Exportar configuraciones	Azure Resource Manager, AWS CloudFormation	Documentar versiones y cambios recientes en la configuración.
Snapshots de Aplicación	Crear snapshot o backup de la aplicación	VeeamBackup, Azure Backup, AWS Backup	Realizar pruebas de consistencia o integridad del snapshot.

Fuente: Elaboración propia

6.2.5. Modelo SaaS.

TABLA 6 ACCIONES DE RECOLECCION DE EVIDENCIA EN SERVICIOS SAAS

Infraestructura Como Servicio IaaS			
Elemento	Acciones	Herramientas Sugeridas	Consideraciones
Registros de Autenticación y Acceso	Descargar registros de acceso	Herramientas del propio SaaS, API de Auditoría.	Revisar los términos de servicio para la disponibilidad y

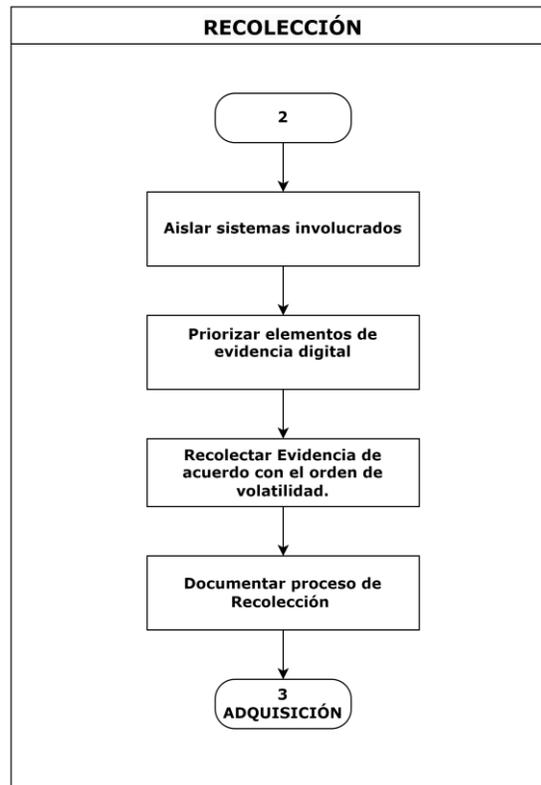
RECOLECCIÓN Y ADQUISICIÓN DE EVIDENCIA DIGITAL FORENSE - CLOUD

Infraestructura Como Servicio IaaS			
Elemento	Acciones	Herramientas Sugeridas	Consideraciones
			retención de logs.
Datos Exportados	Exportar datos críticos (ej. correos, archivos)	APIs del SaaS, herramientas de exportación.	Asegurar que la exportación cumpla con las políticas de retención y privacidad.
Configuraciones de Usuario	Descargar configuraciones y permisos	Herramientas del propio SaaS, API de Gestión.	Documentar cualquier cambio reciente en permisos y configuraciones.

Fuente: Elaboración propia.

6.2.6. Diagrama

Ilustración 4 Diagrama de flujo - Fase Recolección



Fuente: Elaboración propia

RECOLECCIÓN Y ADQUISICIÓN DE EVIDENCIA DIGITAL FORENSE - CLOUD

6.3. Fase: Adquisición

El proceso de adquisición implica la copia de la evidencia digital, junto con la documentación detallada de los métodos y procedimientos utilizados. Estos procesos varían según el modelo de servicio en la nube. Por ello, es importante llevar a cabo las siguientes actividades basadas en la naturaleza del caso y la identificación realizada en las fases previas. Asegúrese de proceder desde los elementos más volátiles hacia los menos volátiles, siguiendo el orden de volatilidad establecido.

6.3.1. Adquisición de Memoria RAM (Modelo IaaS)

- A. Conectar un disco virtual que contenga las herramientas portables necesarias para la adquisición de la memoria RAM a la máquina virtual.
- B. Conectar un disco virtual adicional destinado a almacenar las evidencias adquiridas, como la imagen de memoria RAM.
- C. Ingresar a la máquina virtual investigada, identifique la zona horaria y documente la fecha y hora respectiva.
- D. Ejecutar la herramienta de adquisición de memoria RAM, almacene la imagen generada en el disco virtual destinado al almacenamiento de evidencias.
- E. Generar y documentar la suma de verificación o valor hash de la imagen de memoria RAM para garantizar la integridad de la evidencia.
- F. De ser posible, tome una segunda copia sobre la primera y compruebe el hash.

6.3.2. Adquisición de Discos Virtuales (Modelo IaaS)

- A. Crear un disco administrado a partir del Snapshot generado en la fase de recolección. Este disco debe almacenarse en un grupo de recursos diferente al de la máquina original para proteger la evidencia.

RECOLECCIÓN Y ADQUISICIÓN DE EVIDENCIA DIGITAL FORENSE - CLOUD

- B. Conectar el disco administrado a otra instancia o máquina virtual que actúe como estación forense para realizar la adquisición.
- C. Utilizar herramientas de adquisición forense para crear una imagen forense del disco montado.
- D. Generar y documentar la suma de verificación o valor hash de la imagen forense del disco.
- E. Montar el disco virtual de almacenamiento de evidencias (donde se almacenó la imagen de memoria RAM) en la máquina virtual con rol de estación forense.
- F. Documentar cada paso de la adquisición de evidencia.
- G. De ser posible, tome una segunda copia sobre la primera y compruebe el hash.

6.3.3. Adquisición de Logs y Registros (Modelos IaaS, PaaS y SaaS)

- A. Descargar los registros de acceso, logs de auditoría y actividades relevantes utilizando herramientas como Azure Monitor o Azure Activity Logs.
- B. Exportar logs de configuraciones críticas, incluyendo políticas de acceso y cambios recientes en la configuración, usando Azure Resource Manager.
- C. Documentar cada paso del proceso de exportación de logs, especificando fechas, herramientas y responsables.
- D. Generar un hash de los archivos exportados para garantizar su integridad, utilizando algoritmo SHA-256.
- E. Verificar la consistencia de los logs exportados y almacenarlos en un disco administrado junto a las demás evidencias recolectadas.
- F. De ser posible, tome una segunda copia sobre la primera y compruebe el hash.

6.3.4. Adquisición de Bases de Datos (Modelo IaaS y PaaS)

- A. Realizar una copia de seguridad completa de las bases de datos relevantes.

RECOLECCIÓN Y ADQUISICIÓN DE EVIDENCIA DIGITAL FORENSE - CLOUD

Utilice las herramientas nativas de la nube como Azure, como Azure SQL Database backup o Azure Blob Storage, para realizar copias de seguridad completas, o con las herramientas que disponga el desarrollador o infraestructura. Esto garantiza que se capture la información más reciente

- B. Capturar los metadatos relevantes de la base de datos, incluyendo la estructura, logs de transacciones y auditoría.

Realice una visualización del listado de esquemas y objetos de la base de datos de acuerdo con las sentencias que utilice el motor de base de datos involucrado.

- C. Generar un hash de la base de datos exportada para asegurar su integridad, empleando el algoritmo SHA-256.

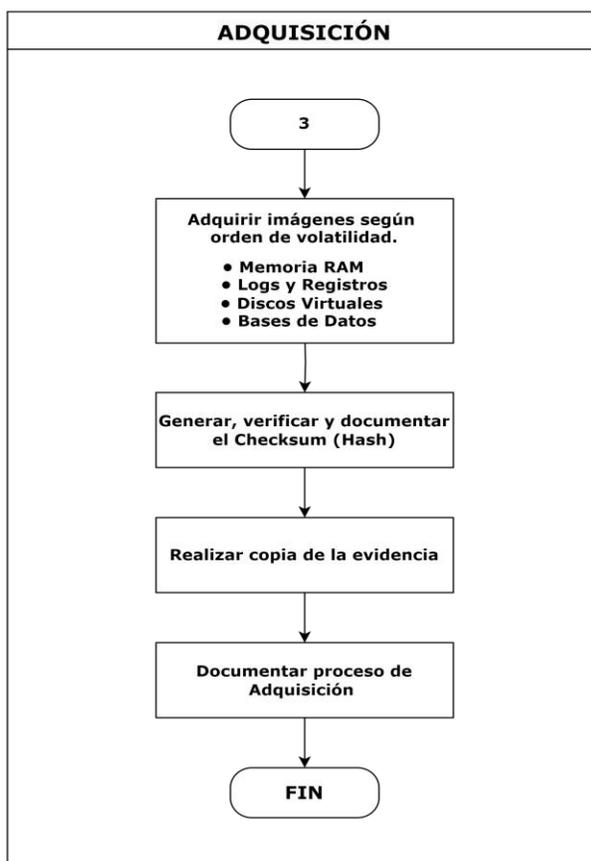
Instrucción en powershell / CLI: `Get-FileHash -Algorithm SHA256 "ruta\del\archivo"`

- D. Almacenar la copia de seguridad de la base de datos en un entorno aislado y seguro.

6.3.5. Diagrama

RECOLECCIÓN Y ADQUISICIÓN DE EVIDENCIA DIGITAL FORENSE - CLOUD

Ilustración 5 Diagrama de flujo - Fase Adquisición



Fuente: Elaboración propia

7. HERRAMIENTAS

Para la adquisición, considere usar las herramientas descritas en el protocolo de Recolección y Adquisición de Evidencia digital forense – Onpremise, herramientas propias de los entornos cloud si dispone de ellas o la que mejor se adapte a la situación.

8. CONTROL DE CAMBIOS

TABLA 7 CONTROL DE CAMBIOS

Versión	Fecha	Descripción de la modificación
01		Creación del documento