1. OBJETO:

Describir el proceso para el análisis, documentación, preservación y custodia de la evidencia digital recolectada, asegurando su integridad, autenticidad y disponibilidad para la investigación forense y respuesta a incidentes de ciberseguridad.

2. ALCANCE:

Este protocolo aplica a todos los funcionarios y contratistas involucrados en el análisis, preservación, custodia y reporte de evidencia digital en incidentes cibernéticos, tanto en entornos en la nube como en infraestructuras locales.

3. DEFINICIONES:

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

Artefacto Forense (Artifact): Son objetos que contienen información y pruebas de que «algo sucedió» en esa área del sistema, registrando y guardando las diversas acciones llevadas a cabo por el sistema operativo.

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.

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.

Malware: software diseñado para dañar, interrumpir o acceder a sistemas informáticos de manera no autorizada.

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.

Sanitización: Proceso de eliminar de manera segura y definitiva toda la información almacenada en un dispositivo digital.

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.

Volatilidad de los Datos: La susceptibilidad de los datos a ser alterados, perdidos o destruidos debido a factores como el tiempo, la temperatura o la manipulación inadecuada.

4. PRINCIPIOS FUNDAMENTALES

4.1. Custodia

Mantener un registro detallado de quién ha manejado la evidencia, cuándo y cómo se ha manipulado, esto es esencial para demostrar la autenticidad de la evidencia.

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.

4.3. Preservación de la originalidad

Siempre trabajar con copias de la evidencia y preservar los originales en su estado intacto. Esto asegura que la evidencia original no se vea comprometida.

4.4. Confidencialidad

Proteger la información contenida en la evidencia digital. Solo las personas autorizadas deben tener acceso a la evidencia y a la documentación relacionada.

4.5. 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
Análisis	DES: Soporte Técnico II Oficial de Seguridad	Realizar un análisis exhaustivo de la evidencia digital utilizando herramientas forenses para identificar, evaluar y extraer información relevante.
Preservación	DES: Oficial de Seguridad Jefe de Laboratorio Soporte Técnico II	Garantizar que la evidencia recolectada y adquirida sea preservada adecuadamente para su análisis futuro, asegurando la cadena de custodia.
Elaboración de informes	DES: Oficial de Seguridad Soporte Técnico II	Elaborar informes detallados sobre las evidencias recolectadas y analizadas, y los presenta al jefe de la Oficina TIC, la Dirección o autoridades pertinentes.
Supervisión	Jefe de Laboratorio	Supervisar el laboratorio forense, gestionando presupuesto y adquisición de herramientas cuando se requieran. Evaluar al equipo (DEFR y DES) para asegurar el cumplimiento de protocolos y normativas. Actuar como enlace con la alta dirección, entregando informes periódicos sobre incidentes y recomendaciones.

Fuente: Elaboración propia

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

6. PROTOCOLO DE ACTUACIÓN Y TAREAS

El protocolo para análisis, documentación y preservación de la evidencia digital se compone de cuatro fases: Análisis, Documentación, Preservación y Disposición final de la evidencia digital.

Ilustración 1. Fases del Protocolo análisis, documentación y preservación de la evidencia digital

Fuente: Elaboración propia

6.1. Fase: Análisis de la Evidencia

Se debe realizar un análisis exhaustivo y detallado de la evidencia digital en un entorno seguro, utilizando herramientas especializadas y documentando cada paso del proceso.

Para lo anterior realice:

A. Establezca un entorno de análisis forense seguro y aislado.
   - No conecte los equipos de análisis al dominio ni a ninguna red, salvo que sea estrictamente necesario para la investigación.
   - Utilice sandboxing o entornos aislados para prevenir cualquier riesgo de contaminación de la evidencia o del sistema de análisis.

B. Asegúrese de que las herramientas y software forense estén actualizados.
   - Realice un análisis exhaustivo de la evidencia digital utilizando herramientas adecuadas de acuerdo con las evidencias.

C. Recolecte los artefactos relevantes, puede tener en cuenta, pero no limitarse a:
   - Registros de acceso, volúmenes de discos, logs de auditoría, snapshots de discos virtuales y cualquier otro artefacto digital relacionado. Use la tabla 3 como una guía.

D. Documente las marcas de tiempo relevantes (*timestamps*) de la evidencia digital.

E. Correlacione los eventos detectados en la evidencia digital con el incidente investigado, identificando puntos clave como la entrada del atacante si fuese el caso, la propagación, y actividades relevantes.

F. Identifique y registre cualquier anomalía o hallazgo relevante como accesos no autorizados, cambios inusuales en la configuración o actividad inusual de red, entre otros.

G. Realice análisis basados en firmas.

- Antimalware: Detección de patrones de *malware* conocido.
- Sandboxig o SIEM: Análisis de comportamiento (detección de actividades anómalas).

H. Con ayuda de los timestamps y los artefactos analizados, genere una línea de tiempo que presente el flujo de eventos de manera clara y en orden cronológico, lo que facilitará entender el flujo de actividades que llevaron al incidente.

TABLA 2 ARTEFACTOS FORENSES

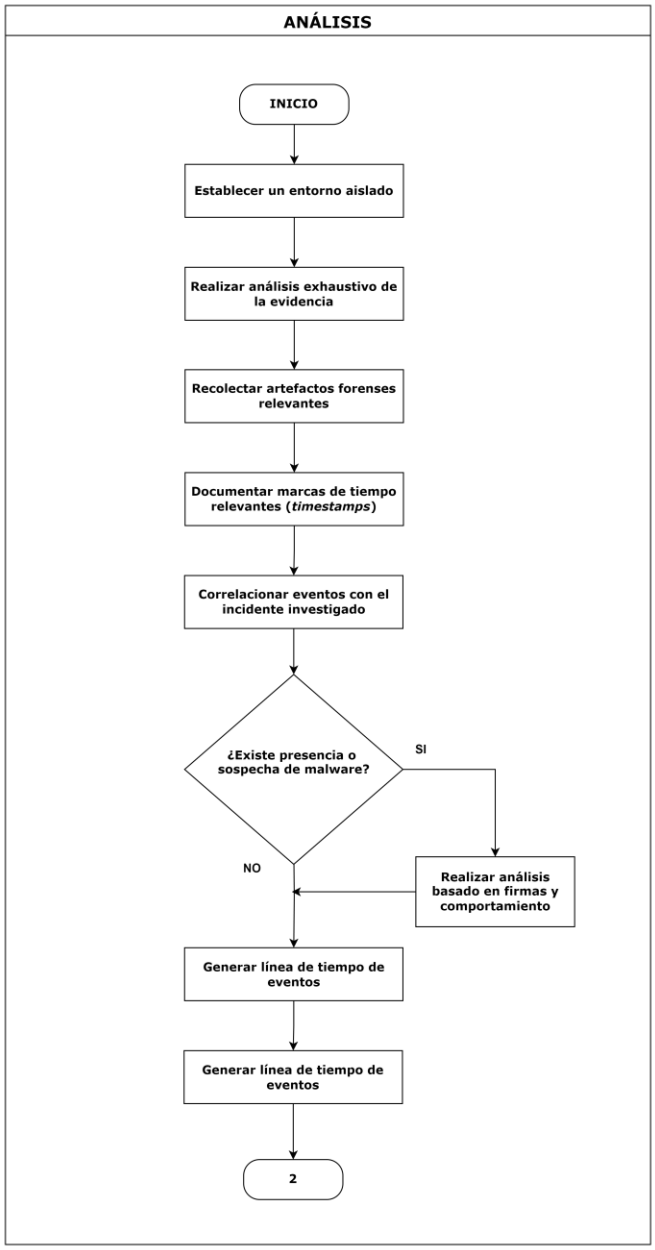
Tipo de Evidencia	Artefactos Importantes	Descripción
Memoria RAM	Contenidos de la memoria	Información volátil que incluye datos de programas en ejecución, contraseñas, y fragmentos de archivos.
	Datos de procesos e hilos	Información sobre los procesos activos y los hilos en ejecución.
	Información de red y conexiones	Datos sobre conexiones de red activas y no activas, puertos abiertos y sesiones de red actuales.
	Datos de registros del sistema operativo	Información sobre eventos del sistema y mensajes de error en tiempo real.
	Cachés de aplicaciones	Datos temporales almacenados por aplicaciones en ejecución.
Discos Físicos y Virtuales	Sistema de archivos	Estructura completa del sistema de archivos, incluyendo directorios y subdirectorios.
	Archivos y carpetas críticos	Documentos, bases de datos, archivos ejecutables, y otros archivos importantes.
	Snapshots	Imágenes del disco en puntos específicos en el tiempo.
	Metadatos de archivos	Información sobre la fecha de creación, modificación, y acceso de los archivos.
	Espacios no asignados	Áreas del disco que no están actualmente en uso, pero pueden contener datos residuales.

Tipo de Evidencia	Artefactos Importantes	Descripción
	Registros de eventos del sistema	Logs que capturan eventos del sistema operativo, como errores, inicios de sesión y cambios en la configuración.
Logs y Registros	Logs de acceso y autenticación	Registros de eventos de inicio de sesión, intentos fallidos, y autenticaciones exitosas.
	Logs de aplicaciones	Registros detallados de eventos y errores generados por aplicaciones específicas.
	Logs de sistema	Registros del sistema operativo incluyendo eventos del sistema, mensajes de error, y cambios de configuración.
	Logs de red	Registros de tráfico de red, conexiones entrantes y salientes, y actividades de red.
	Logs de bases de datos	Registros de consultas, transacciones, y errores en la base de datos.
Bases de Datos	Copias de seguridad de bases de datos	Backup completo de las bases de datos, incluyendo datos, esquemas y configuraciones.
	Registros de transacciones	Logs que registran todas las transacciones realizadas en la base de datos, incluyendo cambios y consultas.
	Metadatos de la base de datos	Información sobre la estructura de la base de datos, incluyendo tablas, índices, y relaciones.
	Historial de modificaciones	Registros de cambios en la estructura de la base de datos y sus elementos.
	Índices y estadísticas	Información sobre los índices utilizados y las estadísticas de rendimiento de la base de datos.

Fuente: Elaboración propia.

6.1.1. Diagrama

Ilustración 2 Diagrama de flujo - Fase de análisis



Fuente: Elaboración propia

6.2. Fase: Documentación

Es importante generar un informe completo que documente los hallazgos y el proceso seguido, asegurando que toda la evidencia, su manejo y los hallazgos estén claramente registrados.

Para lo anterior realice:

A. Elabore un informe detallado del análisis forense que incluya la metodología utilizada y los hallazgos.
B. Asegúrese de que el informe sea claro y comprensible, utilizando descripciones detalladas de los hallazgos y métodos, con registro fotográfico y capturas de pantalla para mayor claridad.
C. Incorpore una cronología de eventos clave o línea de tiempo basada en los artefactos recolectados, alineando los hallazgos con las marcas de tiempo relevantes.
D. Documente la integridad de la evidencia y cualquier incidente que pueda haber afectado su preservación, asegurando la trazabilidad de la cadena de custodia.
E. Adjunte anexos que incluyan la documentación del análisis, las herramientas utilizadas y cualquier información adicional relevante.

6.2.1. Informes

Para asegurar una correcta gestión y trazabilidad de la evidencia digital en las distintas fases del proceso forense, es importante el uso de instrumentos estandarizados. A continuación, se incluyen los instrumentos básicos con los elementos mínimos que debe incluir:

TABLA 3. INSTRUMENTOS MINIMOS NECESARIOS

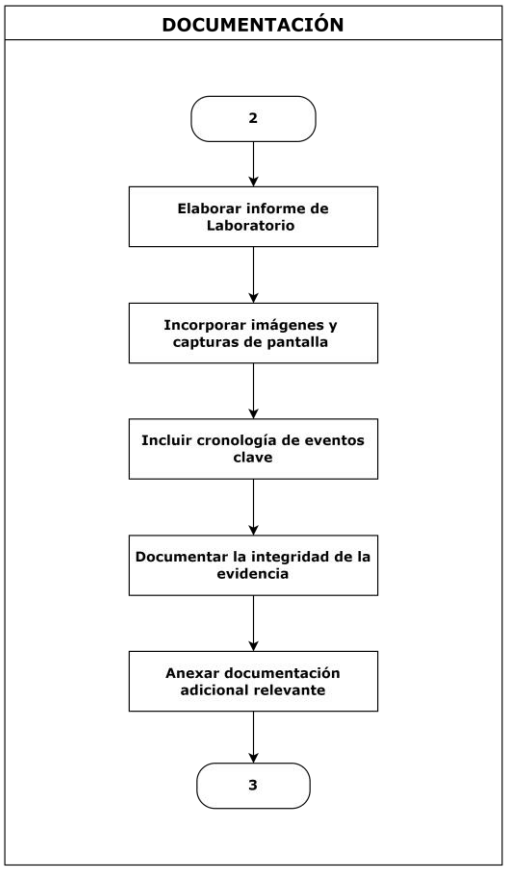
Instrumentos	Elementos Mínimos
Rótulo para Evidencia	Número de caso
	Número de identificación de la evidencia
	Descripción breve de la evidencia
	Fecha y hora de recolección
	Nombre del recolector
	Lugar de recolección
	Condiciones de la evidencia
	Firma del responsable
Cadena de Custodia y Registro de Continuidad	Número de caso
	Número de identificación de la evidencia
	Descripción de la evidencia
	Fecha y hora de transferencia
	Nombre de las personas involucradas
	Firma de la persona que recibe la evidencia

Instrumentos	Elementos Mínimos
	Propósito de la transferencia
	Ubicación de la evidencia
	Observaciones
Informe de Campo (Recolección o Adquisición)	Número de caso
	Número de identificación de la evidencia
	Fecha y hora del procedimiento
	Lugar del procedimiento
	Descripción de la evidencia recolectada
	Métodos utilizados para la recolección
	Nombre de los participantes
	Firmas de los responsables
	Observaciones
Informe de Laboratorio (Análisis)	Número de caso
	Número de identificación de la evidencia
	Fecha de recepción en laboratorio o espacio destinado a ello.
	Análisis realizados
	Cronología de eventos analizados (Línea de tiempo)
	Resultados obtenidos
	Conclusiones
	Firmas de los analistas
	Fecha de emisión del informe

Fuente: Elaboración propia

6.2.2. Diagrama de flujo

Ilustración 3 Diagrama de flujo - Fase Documentación



Fuente: Elaboración propia

6.3. Fase: Preservación y Custodia.

La Fase de Preservación y Custodia es crucial para mantener la integridad y autenticidad de la evidencia digital. Asegura que la evidencia no se altere ni se pierda y que sea válida en la investigación.

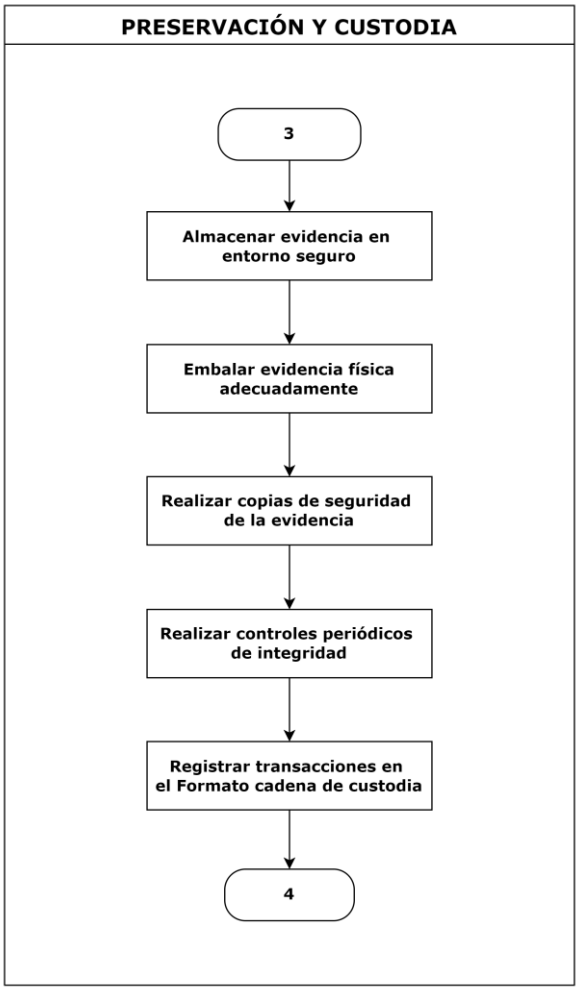
Para lo anterior realice:

A. Almacene la evidencia digital en un entorno seguro.
B. Las evidencias físicas deben embalarse en contenedores resistente a golpes y en caso de ser necesario usar bolsas Faraday para bloquear señales inalámbricas que pueda alterar la evidencia de forma remota.
C. Realice una copia de seguridad de la evidencia.

D. Realice controles periódicos para verificar la integridad de la evidencia.
E. Documente los resultados de las verificaciones de integridad.
F. Registre todas las transacciones relacionadas con la evidencia en el instrumento de cadena de custodia y registro de continuidad.

6.3.1. Diagrama de flujo

Ilustración 4 Diagrama de flujo - Documentación



Fuente: Elaboración propia

6.4. Fase: Disposición final

Esta fase tiene como objetivo definir los procedimientos para la disposición final de la evidencia digital, asegurando la integridad de los procesos hasta su eliminación o retención a largo plazo.

A. Conserve la evidencia digital recolectada por un periodo mínimo de seis (6) meses, a menos que el caso requiera un periodo de retención más largo.

B. Evalúe si la evidencia es necesaria para investigaciones en curso o futuras antes de que concluya el periodo de retención, o si puede eliminarse de forma segura.

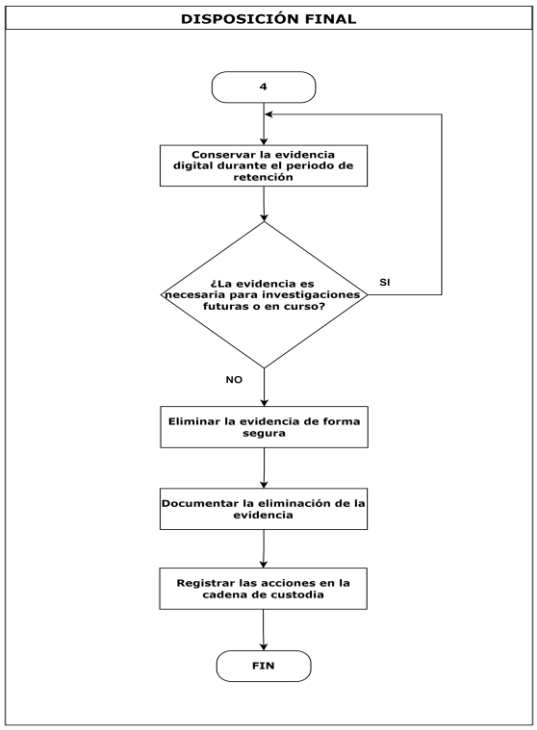
C. Elimine de forma segura la evidencia que no sea requerida después del periodo de retención, utilizando herramientas de borrado seguro (sanitización) como DBAN, FTK Imager o cualquiera disponible. Los dispositivos de almacenamiento sanitizados pueden ser usados en otros casos o investigación.

D. Documente cada eliminación de evidencia digital, incluyendo la herramienta utilizada, el método de destrucción y cualquier información relevante, y adjunte esta documentación al expediente del caso.

E. Registre toda decisión relacionada con la disposición final de la evidencia, así como las acciones realizadas, en la cadena de custodia para garantizar la trazabilidad del proceso.

6.4.1. Diagrama de flujo

Ilustración 5 Diagrama de flujo - Disposición final



Fuente: Elaboración propia

7. HERRAMIENTAS PARA ANÁLISIS

La selección de la herramienta adecuada dependerá de la investigación, el dispositivo, la experiencia del investigador y los recursos. Si la UAESP adquiere software comercial, se podrá ampliar el conjunto de herramientas disponibles, incluyendo software comercial especializado.

A continuación, se listan las herramientas para análisis opensource que puede ser usadas para el análisis de incidentes de ciberseguridad.

TABLA 4 HERRAMIENTAS PARA ADQUISICIÓN

Herramienta	Sitio Oficial	Sistema Operativo	Propósito Principal	Dispositivos
Autopsy	https://www.autopsy.com/	Multiplataforma (Linux, Windows, macOS)	Interfaz gráfica para TSK, facilitando el análisis y visualización de datos, incluyendo	Memoria RAM Dispositivos USB Imágenes de discos HDD y SSD

Herramienta	Sitio Oficial	Sistema Operativo	Propósito Principal	Dispositivos
			volátiles.	
Volatility	https://volatilityfoundation.org/	Multiplataforma (Linux, Windows, macOS)	Análisis de datos volátiles, recuperación de contraseñas, investigación de incidentes en tiempo real.	Memoria RAM
LiME	https://github.com/504ensicsLabs	Windows	Análisis de volátiles, enfoque en sistemas Linux, complemento para Volatility.	Memoria RAM
RegRipper	https://github.com/keydet89/RegRipper3.0	Multiplataforma (Linux, Windows, macOS)	Análisis de registros de Windows	Registros windows
Mobile Verification Toolkit (MVT)	https://docs.mvt.re/en/latest/	Multiplataforma (Linux, Windows, macOS)	Verificación de dispositivos móviles, extracción de datos, análisis inicial	Dispositivos móviles (Android, iOS)

Fuente: Elaboración propia

Es fundamental contar con un repositorio de imágenes del software utilizado o asegurarse de descargarlo directamente desde los sitios oficiales, para garantizar la autenticidad, integridad y seguridad del software.

Si se considera necesario, utilice otras herramientas o compendio de estas de acuerdo con la necesidad específica del caso, por ejemplo:

- SIFT WorkStation (SANS Institute): Distribución Linux que posee un conjunto gratuito de herramientas de código abierto para respuesta a incidentes y análisis forense.

  Página oficial: https://www.sans.org

- CAINE: Distribución de Linux que proporciona un ambiente para investigación forense.

Página oficial: https://www.caine-live.net/

- Paladin Edge: Herramienta gratuita basada en Ubuntu que permite simplificar la tarea del informático forense.

  Página oficial: https://sumuri.com/

8. CONTROL DE CAMBIOS

TABLA 5 CONTROL DE CAMBIOS

Versión	Fecha	Descripción de la modificación
01	18/10/2024	Creación del documento

Fuente: UAESP

9. AUTORIZACIONES

TABLA 6 AUTORIZACIONES

	NOMBRE	CARGO	FIRMA
Elaboró	Juan Sebastián Perdomo Méndez	Profesional Universitario Oficina TIC	
Revisó	Jorge Alexis Rodriguez Meza	Jefe Oficina TIC	
Aprobó	Luz Mary Palacios	Jefe Oficina Asesora de Planeación (E)