

# Guía de Procedimiento Pericial y Manual de Usuario



# eVidensTalk 2026

## CYBER FORENSIC SUITE

Herramienta: eVidensTalk - Cyber  
Forensic Suite

Fecha de Emisión: Febrero 2026



# Introducción y Validez Técnica

La presente guía establece el Procedimiento Operativo Estándar (SOP) para la extracción, preservación, análisis y reporte de evidencia digital proveniente de la aplicación de mensajería WhatsApp, utilizando la suite eVidensTalk.

El software ha sido desarrollado bajo estrictos principios de **Privacidad desde el Diseño** (Privacy by Design). A diferencia de las herramientas basadas en la nube, eVidensTalk asegura que el tratamiento, estructuración e indexación de los datos se realice de forma **100% local (On-Premise)** y descentralizada, procesando la información directamente en la memoria y almacenamiento del equipo del perito.

# Marco Normativo (República Argentina)

El diseño y flujo de trabajo de eVidensTalk cumple taxativamente con las siguientes normativas:

## Ley 25.326 de Protección de Datos Personales

El software no transmite información a servidores externos ni nubes de terceros, garantizando que el perito o investigador mantenga el control total como Responsable de Archivo.

## Ley 26.388 (Delitos Informáticos)

El procedimiento respeta la integridad de la prueba, operando sobre copias de trabajo y evitando la alteración de registros originales conforme a las exigencias procesales del Código Penal Argentino.

## Artículos 18 y 19 de la Constitución Nacional

Respeto absoluto a la inviolabilidad de las comunicaciones privadas, la intimidad y la privacidad.

# Garantía de Inalterabilidad

## (Hashing)

Para dar cumplimiento a los requisitos procesales periciales, eVidensTalk incorpora un motor de validación criptográfica. Al generar el reporte final, el sistema calcula de forma automatizada las firmas Hash **MD5** y **SHA-256** del archivo original procesado. Esto garantiza matemáticamente que la evidencia no ha sufrido alteraciones, modificaciones ni corrupciones desde su extracción hasta su presentación en el juzgado.

### "Doble Candado"

#### Hash MD5

La "**huella digital**" única e irrepetible de un archivo

#### SHA-256

"**huella digital**" ultra-segura de 64 caracteres, matemáticamente imposible de falsificar

# Protocolo de Cadena de Custodia

## y Flujo de Trabajo

### Fase 1: Aislamiento y Adquisición de la Evidencia

Aislamiento del Dispositivo: Asegurar el dispositivo móvil bajo custodia colocándolo en Modo Avión o, preferentemente, mediante el uso de bolsas de Faraday para evitar borrados remotos (wipes).

Extracción Lógica: Utilizar la función nativa de WhatsApp “Exportar chat”. Seleccionar la opción adecuada (con o sin archivos multimedia) según el alcance de los puntos de pericia.

Transferencia: Trasladar el archivo generado ([.txt](#) o [.zip](#)) a la estación de trabajo forense utilizando un medio de almacenamiento seguro e higienizado.

## **Fase 2: Ingesta Forense y Procesamiento**

Ejecutar eVidensTalk en la estación de trabajo local

Importar el archivo (.zip o .txt) directamente en la zona de carga del dashboard.

El software parseará y estructurará los metadatos (fechas, horas, emisores y cuerpo del mensaje) sin alterar el archivo fuente original.

## **Fase 3: Análisis, Discovery y Etiquetado**

Utilizar el motor de búsqueda global para identificar rápidamente términos clave ordenados por el juzgado o la fiscalía.

Identificar los mensajes relevantes y utilizar la función de etiquetado para marcarlos como "Evidencia Clave".

En caso de contar con audios transcritos mediante IA, revisar la coincidencia de texto en la visualización integrada.

## Fase 4: Generación de Entregables

Dirigirse a la sección de "Reportes" y verificar que los mensajes etiquetados sean los correctos.

Exportar el **PDF Forense**. El sistema compilará la información, los metadatos y estampará automáticamente los algoritmos Hash correspondientes para su presentación legal.

## Protocolo de Cadena de Custodia y Flujo de Trabajo

**METODOLOGÍA TÉCNICA:** Para la gestión, análisis y preservación de la evidencia digital, se ha utilizado la suite de auditoría forense eVidensTalk. Dicha herramienta opera bajo protocolos de "Procesamiento Local Estricto", garantizando que la información sensible no sea transmitida a servidores externos ni almacenada en nubes de terceros, cumplimentando con la Ley 25.326. El procesamiento de los datos se realizó manteniendo la integridad absoluta de los metadatos originales y asegurando la Cadena de Custodia digital requerida para la validez de la prueba en procesos judiciales en la República Argentina.

# Buenas Prácticas Periciales

## Recomendadas

**Air-Gapping:** Se recomienda operar la versión Enterprise de eVidensTalk en una estación de trabajo dedicada y desconectada de internet.

**Resguardo del Original:** El archivo extraído del dispositivo móvil debe conservarse siempre en su estado original (solo lectura) en un disco de resguardo o repositorio seguro.

### Soporte Técnico y Asistencia

Para consultas sobre licenciamiento, soporte técnico o reporte de incidencias operativas, contáctese de manera oficial a: [evidenstalk@gmail.com](mailto:evidenstalk@gmail.com)