

CustodiAR es una solución de escritorio orientada a la contención criptográfica local. Este documento describe los flujos operativos de inicialización, gestión de contenedores aislados y destrucción segura de remanentes digitales.

01. INICIALIZACIÓN Y ASISTENTE DE CONFIGURACIÓN

Al ejecutar la aplicación por primera vez en el entorno local, se despliega de forma automática el asistente guiado de inicialización para garantizar un despliegue seguro sin filtraciones previas:

- Verificación de Entorno:** Resumen de los pilares del software: arquitectura de cifrado en capas (Envelope Encryption), cifrado autenticado en bloque (AES-256-GCM) y soberanía de almacenamiento (cero persistencia en nube o servidores de telemetría).
- PIN de Aplicación (Opcional):** Barrera de acceso rápido previa al motor de baúles. Permite restringir la apertura de la interfaz gráfica ante accesos físicos no autorizados en el equipo. Seleccione "Omitir este paso" si prefiere delegar toda la seguridad exclusivamente en las llaves del baúl.
- Aprovisionamiento del Primer Baúl:**
 - Identificador (Nombre):** Etiqueta semántica (ej. `Laboral`, `Finanzas`, `Forense`).
 - Ruta de Persistencia:** Directorio físico donde se almacenarán las estructuras cifradas (por defecto: `~/CustodiAR_Vaults/<Nombre>`).
 - Contraseña Maestra y Entropía:** Defina la clave que derivará la KEK (Key Encryption Key). El indicador de entropía en tiempo real valida longitud, distribución y resistencia contra ataques de diccionario.
 - Compromiso Criptográfico:** Confirmación cruzada de clave para evitar bloqueos por fallas de tipeo. Haga clic en **Finalizar y Abrir CustodiAR**.

02. ARQUITECTURA DE MÚLTIPLES BAÚLES (MULTI-VAULT)

Cada baúl opera bajo una barrera de aislamiento criptográfico estricto, con sales independientes y derivación de llaves no vinculadas entre sí.

Aprovisionar Baúl Adicional

Desde el control lateral `+ Nuevo Baúl`, configure nuevos contenedores asignando directores de disco independientes y contraseñas maestras completamente distintas.

Vincular Contenedor Existente

Mediante `📁 Abrir Existente...`, cargue baúles portados desde unidades USB o unidades de almacenamiento secundarias seleccionando el archivo cabecera `vault.meta`.

Control de Estado y Ciclo de Vida de Claves

- Desbloqueo Seguro:** Ingrese la contraseña maestra del baúl específico y presione `Enter` o `🔓 Desbloquear Baúl`. La clave DEK se descifra exclusivamente en la memoria volátil (RAM).
- Bloqueo Individual:** En la cabecera del panel del baúl activo, accione `🔒 Bloquear Baúl` para purgar la llave DEK activa y desvincular el acceso a los descriptores de archivo.
- Protocolo de Pánico ("Bloquear Todo"):** Situado al pie del panel de navegación lateral. Elimina instantáneamente de la memoria RAM todas las claves de baúles montados y bloquea todas las sesiones activas en un único ciclo de reloj.
- Temporizador de Inactividad (Auto-Lock):** Configurable en 5, 10 (valor estándar), 15, 30 minutos o Desactivado. Si no se detectan eventos de entrada de puntero o teclado, se activa automáticamente la purga de memoria de los baúles abiertos.

03. MANEJO Y PROCESAMIENTO DE ARCHIVOS

CustodiAR gestiona el acceso a cada archivo mediante lecturas directas verificadas por firma criptográfica para impedir manipulación o lecturas parciales corruptas.

3.1 Ingesta de Archivos y Sanitización de Medios

Para ingresar información protegida al baúl activo:

1. Confirme que el baúl objetivo se encuentre en estado **Desbloqueado**.
2. Accione el botón de ingesta `+ Añadir Archivo(s)` y seleccione los ficheros mediante el explorador nativo.
3. Defina la política de integridad de los archivos originales según el nivel de aislamiento requerido:

OPCIÓN: TRITURADO SEGURO (DIGITAL SHREDDING)

Al seleccionar esta modalidad, tras confirmarse el cifrado atómico y validación de hash del nuevo bloque, el archivo original en el disco se destruye mediante sobrescritura física multipaso antes de su desvinculación en el sistema de archivos del sistema operativo.

4. Si selecciona **Conservar Originales**, el archivo quedará clonado bajo cifrado en el baúl y su original permanecerá inalterado en su ruta original.

3.2 Búsqueda Indexada

Filtro en tiempo real situado en el margen superior. Permite localizar archivos por nombre y metadatos sin necesidad de descryptar las cargas útiles en disco.

3.3 Extracción Autenticada

Al pulsar `↓ Extraer`, el sistema verifica primero el tag de autenticación **AEAD** y la suma de verificación **SHA-256**. Solo tras validar la autenticidad se genera el archivo descifrado en destino.

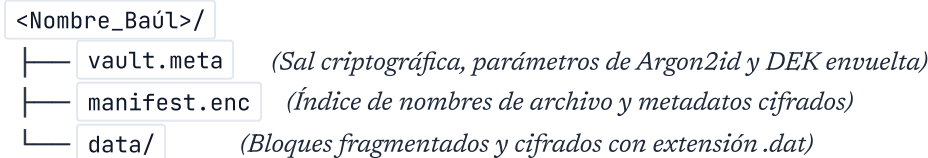
3.4 Eliminación Definitiva dentro del Baúl

Al eliminar un elemento del índice mediante el botón `🗑️ Borrar`, el bloque binario subyacente (`.dat`) es sobrescrito con patrones de ceros, unos y ruido pseudoaleatorio previo a su eliminación lógica del disco, impidiendo la recuperación de fragmentos residuales.

04. TOPOLOGÍA DE DATOS Y COPIAS DE SEGURIDAD (BACKUPS)

Los baúles de CustodiAR son contenedores portables atómicos. Cada directorio raíz de un baúl se compone de la siguiente estructura:

ESTRUCTURA DEL CONTENEDOR DE BAÚL



Estrategia de Backup: Para respaldar el contenido, simplemente copie la carpeta completa a un medio de almacenamiento externo o sincronícela con servicios en la nube comercial (Google Drive, Dropbox, OneDrive). Dado que la superficie de ataque está blindada con cifrado de extremo a extremo y nombres de archivo ofuscados en el manifiesto, los datos permanecen completamente inmunes a filtraciones de proveedores de almacenamiento.