Manual de Usuario - Secure Password Vault

1. Introducción

Bienvenido a **Secure Password Vault**, su gestor de contraseñas personal, seguro y auto-hospedado. Esta aplicación ha sido diseñada con la privacidad y la seguridad como prioridades absolutas, utilizando cifrado de nivel militar para proteger sus credenciales.

Características Principales

- **Arquitectura de Conocimiento Cero (Zero-Knowledge):** Su contraseña maestra nunca se almacena. Solo usted tiene la llave para descifrar sus datos.
- **Organización Jerárquica:** Gestione sus contraseñas mediante **Categorías** (ej. Trabajo, Personal) y **Aplicaciones** (ej. Gmail, Slack).
- **Seguridad Robusta:** Cifrado AES-256-GCM para todos los campos sensibles.
- **Interfaz Moderna:** Una aplicación web rápida e intuitiva para gestionar todo desde su navegador.
- **Portabilidad:** Herramientas de importación y exportación fáciles de usar.

---

2. Instalación y Requisitos

Requisitos Previos

Para ejecutar Secure Password Vault, necesita tener instalado:

1. **Docker**
2. **Docker Compose**

Pasos de Instalación

1. **Descargar el proyecto:** Asegúrese de tener los archivos fuente en su carpeta local.

   Iniciar la aplicación: Abra una terminal (PowerShell o CMD) en la carpeta del proyecto y ejecute:

   ```
   bash docker-compose up -d --build
   ```

   Este comando descargará las dependencias necesarias y levantará los servicios (base de datos y aplicación web).

Verificar el estado: Una vez finalizado el comando anterior, la aplicación estará disponible en su navegador.

---

3. Configuración Inicial

Acceso por Primera Vez

1. Abra su navegador web y vaya a: **http://localhost:8001**
2. Verá una pantalla de bienvenida solicitándole configurar su **Contraseña Maestra**.

Creación de la Contraseña Maestra

> [!IMPORTANTE] **La Contraseña Maestra es la única llave para sus datos. Si la olvida, perderá el acceso a todas sus contraseñas para siempre.** No hay función de "¿Olvidó su contraseña?" porque el sistema no la conoce ni la almacena.

1. Introduzca una contraseña fuerte y única.
2. Confírmela en el segundo campo.
3. Haga clic en **"Inicializar Bóveda"**.

¡Listo! El sistema cifrará su base de datos con esta llave y le llevará al panel principal.

---

4. Guía de Uso

Interfaz Principal

La interfaz se divide en dos áreas principales: 1. **Barra Lateral (Izquierda):** Muestra sus **Categorías** y **Aplicaciones**. Use el buscador en la parte superior para filtrar rápidamente sus cuentas. 2. **Panel Principal (Derecha):** Muestra los detalles de la aplicación seleccionada y la lista de contraseñas asociadas.

Gestión de Categorías

Las categorías le ayudan a agrupar sus aplicaciones (ej. "Finanzas", "Redes Sociales").

- **Crear:** Haga clic en el botón **"+"** junto al título "Categories" en la barra lateral.

  Editar/Eliminar: Use los iconos de lápiz (editar) o basura (borrar) que aparecen junto al nombre de la categoría al pasar el ratón.

- *Nota: Borrar una categoría eliminará también todas las aplicaciones y contraseñas contenidas en ella.*

Gestión de Aplicaciones

Las aplicaciones representan un servicio específico (ej. Netflix, Banco X).

- **Crear:** Haga clic en el botón **"+"** que aparece a la derecha del nombre de una Categoría.
- **Navegar:** Haga clic en el nombre de la aplicación para ver sus detalles en el panel principal.

Gestión de Contraseñas

Dentro de una aplicación, puede tener múltiples credenciales (ej. "Cuenta Personal", "Cuenta Compartida").

- **Añadir Contraseña:** Use el botón **"Add Password"** en la esquina superior derecha del panel principal.
- **Ver Contraseña:** Las contraseñas están ocultas por defecto (****). Haga clic en el icono del** "Ojo"** para revelarlas temporalmente.
- **Copiar:** Haga clic en el icono de **"Copiar"** para guardar la contraseña en su portapapeles.

---

5. Funciones Avanzadas

Copias de Seguridad (Importar/Exportar)

En la parte inferior de la barra lateral encontrará los botones para gestionar sus datos en lote:

Export Data: Descarga un archivo JSON con toda su base de datos.

- *Precaución: El archivo exportado contendrá sus datos sensibles. Guárdelo en un lugar seguro.*

- **Import Data:** Le permite restaurar una copia de seguridad previa desde un archivo JSON, recuperando todas sus categorías y contraseñas.

Generación de Datos de Prueba

Si es un desarrollador probando la aplicación, puede usar los scripts incluidos para generar datos masivos: * `seed_data.py`: Crea categorías y aplicaciones de ejemplo. * `seed_passwords.py`:

Genera contraseñas aleatorias para las aplicaciones existentes.

---

6. Seguridad

Para su tranquilidad, así es como protegemos sus datos bajo el capó:

- **Algoritmo de Hashing (Argon2id):** Utilizamos Argon2id, el ganador de la Password Hashing Competition, para derivar las claves de cifrado de su Contraseña Maestra. Esto hace que los ataques de fuerza bruta sean extremadamente costosos y lentos.
- **Cifrado Simétrico (AES-256-GCM):** Todos los campos sensibles (`username`, `password`, `url`, `notes`) se cifran individualmente usando AES-256 en modo GCM (Galois/Counter Mode), que garantiza tanto confidencialidad como integridad.
- **Vectores de Inicialización (IV) Únicos:** Cada campo cifrado utiliza un IV único, asegurando que guardar la misma contraseña varias veces resulte en datos cifrados completamente diferentes.

Generado automáticamente por Asistente IA - 2025