Informe del Gestor de Contraseñas

Tecnologías empleadas
- Lenguaje: C# (.NET 8)
- Criptografía: PBKDF2 (Rfc2898DeriveBytes), AES-GCM (System.Security.Cryptography), RSA (2048, OAEP-SHA256)
- Almacenamiento: archivo binario con metadata JSON + blob cifrado
- CLI: aplicación de consola

URL del repositorio
- URL: <completar una vez publicado>

Capturas de pantalla
- Agregar capturas de `add`, `list`, `remove`, `genpass`, `genkeys`, `export`, `import`.

Funcionalidad principal
- Vault cifrado con AES-GCM; clave derivada de contraseña maestra con PBKDF2.
- Verificación de contraseña con HMAC-SHA256 sobre salt derivado.
- CRUD de entradas, generador de contraseñas, exportación/importación con RSA.

Decisiones técnicas relevantes
- AES-GCM por autenticidad e integridad (AEAD) y nonce de 12 bytes.
- Iteraciones PBKDF2 = 210k para endurecer ataques de fuerza bruta.
- Formato del vault: `magic(4)+version(1)+len-json(4)+metadata-json+blob-cifrado`.
- Import re-genera Id para evitar colisiones.

Cómo ejecutar
- Ver `README.md`.