VaultLM

Resumen de seguridad de VaultLM

Flujo de datos y principios de seguridad para IA documental confidencial

QUÉ ES VAULTLM

Un espacio controlado entre documentos confidenciales e IA. VaultLM aplica permisos, enmascarado y seudonimización antes del procesamiento externo y devuelve respuestas con fuentes y pista de auditoría.

1. Documentos
Los originales entran en un vault gobernado con permisos y retención.

›

2. Proteger
Los identificadores sensibles se enmascaran y seudonimizan.

›

3. Minimizar
Solo se seleccionan fragmentos relevantes y permitidos.

›

4. Servicio de IA
El servicio externo elegido recibe el contexto protegido mínimo.

›

5. Evidencia
La respuesta vuelve con pasajes citados y uso registrado.

PERMANECE EN VAULTLM

Archivos originales, mapas de identidad, permisos y retención.

A PROCESAMIENTO DE IA

Solo fragmentos mínimos, permitidos y seudonimizados.

PRINCIPIOS DE SEGURIDAD

Ligado a permisos
El acceso mediante IA no supera el permiso para abrir la fuente.

Fail-closed
Si el enmascarado requerido no está disponible, la consulta se detiene.

Basado en documentos
Las consultas externas están ligadas a fuentes permitidas del vault.

Verificable
Fuentes, servicio utilizado y eventos de auditoría apoyan la revisión humana.

LÍMITES HONESTOS

El enmascarado reversible es seudonimización, no anonimización. La detección automática no es infalible y sigue siendo necesaria la revisión humana. VaultLM apoya la gobernanza y las evidencias, pero no garantiza automáticamente el cumplimiento legal.

CALENDARIO DE LA AI ACT

Desde el 2 de agosto de 2026 se aplican más disposiciones del AI Act. Las reglas para sistemas de alto riesgo tienen plazos posteriores: 2 de diciembre de 2027 para sistemas independientes y 2 de agosto de 2028 para sistemas integrados en productos