

Lleve la IA a su laboratorio.

Con un registro fiable.

Un proxy autoalojado que guarda cada llamada de IA en un registro de auditoría que permite detectar manipulaciones, y solo deja pasar lo que usted autoriza.

Diseñado para dar soporte a flujos de trabajo GLP, 21 CFR Part 11 y EU GMP Annex 11.

 ChatGPT Claude Copilot

Su infraestructura. Sus políticas. Su control.

Usted decide qué información puede enviarse a los proveedores externos de IA.

El reto

Los asistentes de IA empiezan a consultar directamente sistemas de laboratorio y de gestión mediante el Model Context Protocol (MCP). En entornos regulados y de investigación, cada acción debe ser trazable. Pero un log normal se puede modificar o borrar sin que nadie lo note, y a menudo ni existe.



¿Qué se llamó, cuándo y qué se hizo?



¿Puede demostrar que el registro está intacto?



¿Puede frenar al asistente cuando no debe actuar?

Cómo funciona

1

Conectar



Sitúe el proxy entre su asistente de IA y sus sistemas (vía MCP). Un asistente de instalación lo configura y comprueba la configuración.

**2**

Comprobar y registrar



Se registra cada llamada: qué, cuándo y con qué herramienta. Lo no permitido se bloquea, y el bloqueo queda registrado.

**3**

Verificar



Cada entrada se encadena por hash con la anterior. La verificación muestra si algo se ha modificado o borrado.

Ventajas clave



Traza completa y automática

Qué, cuándo y con qué herramienta, sin esfuerzo manual.



Detección de manipulaciones

Cualquier modificación o borrado del registro se puede detectar.



Solo lectura por defecto

Con lista de permitidas: el resto se bloquea y cada bloqueo se registra.



Sin fricciones

Nunca hace esperar a nadie ni modifica el contenido de los mensajes.



Autoalojado, sin phone-home

El registro se queda en su propia infraestructura.



Empiece gratis

Edición Community de código abierto (MIT), disponible ya.

La misma IA. Cada llamada, registrada.

Un proxy autoalojado entre su IA y sus sistemas, trazable para sus equipos.

Dónde se sitúa



En qué se diferencia

	Sin auditoría	Logs genéricos	mcp-glp-audit-proxy
Registra cada llamada de la IA	✗ No	– Según la configuración	✓ Sí: qué, cuándo, con qué
Detecta modificaciones o borrados	✗ No	✗ No es su objetivo	✓ Cadena de hash + verificación
Solo pasan las llamadas aprobadas	✗ No	✗ No, solo observan	✓ Solo lectura + permitidas
En su propia infraestructura	– n/a	– Depende	✓ Autoalojado, sin phone-home
Diseñado para dar soporte a flujos de trabajo GLP, 21 CFR Part 11 y EU GMP Annex 11	✗ No	✗ No	✓ Sí

A diferencia de las pasarelas de IA habituales, centradas en logs u observabilidad, mcp-glp-audit-proxy se basa en un registro encadenado por hash que permite detectar manipulaciones y está orientado a flujos GxP y de investigación.

Dos ediciones



Edición Community

DISPONIBLE YA

Gratuita, MIT, v0.3.0 · PyPI, MCP Registry, GitHub.

- ✓ Log JSONL encadenado por hash
- ✓ Verificación con anclaje (pinning)
- ✓ Lista de permitidas
- ✓ Asistente de instalación

```
pip install mcp-glp-audit-proxy
```



Edición Pro

PRÓXIMAMENTE

Para equipos regulados que necesitan más.

- ✳ Almacenamiento SQL/MSSQL y S3 Object Lock
- ✳ Informes PDF/CSV
- ✳ Valores antes/después
- ✳ Paquete de validación IQ/OQ



Diseñado para dar soporte a flujos de trabajo GLP, 21 CFR Part 11 y EU GMP Annex 11. Por sí solo no garantiza el cumplimiento normativo ni sustituye la validación.

Contacto / Solicite una demo

Pruebe gratis la edición Community o solicite una demostración para su laboratorio, empresa o universidad.

✉ [Escriba a antonio@castellon.ch](mailto:antonio@castellon.ch)

👤 Antonio Castellon · Castellon.CH

✉ antonio@castellon.ch

☎ +41 76 689 13 69

🌐 castellon.ch

📍 Biel/Bienne, Suiza