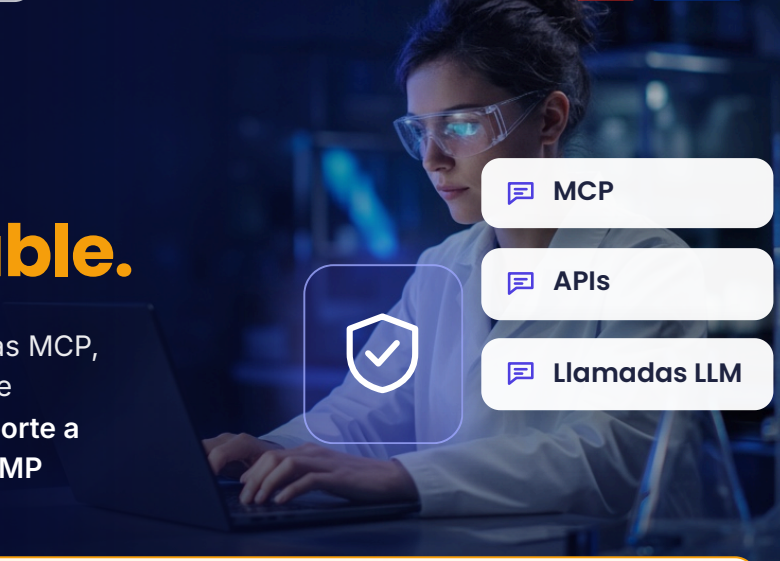
Castellon.CH | GxP Gateway Audit

PARA LABORATORIOS, LIFE SCIENCE Y UNIVERSIDADES

Lleve la IA a su laboratorio. Con un registro fiable.



Una pasarela autoalojada que guarda las llamadas MCP, API y LLM en un registro de auditoría que permite detectar manipulaciones. **Diseñada para dar soporte a flujos de trabajo GLP/GxP, 21 CFR Part 11 y EU GMP Annex 11.**

Su infraestructura. Sus políticas. Su control.
Usted decide qué información puede enviarse a los proveedores externos de IA.

El reto

Asistentes de IA, agentes y scripts acceden ya a sistemas de laboratorio y de gestión mediante MCP, APIs HTTPS, pasarelas y llamadas a LLM. En entornos regulados cada acción debe ser trazable, pero un log normal se puede modificar o borrar sin que nadie lo note.

- **¿Qué llamada se hizo, cuándo y qué se hizo?**
- **¿Puede demostrar que no se ha modificado ni borrado nada?**
- **¿Puede frenar una llamada que no debe pasar?**

Cómo funciona

1 Conectar
Funciona como proxy inverso con TLS. El cliente solo cambia la URL base. Flujos: mcp2mcp, mcp2api, api2mcp, api2api, mcp2llm, api2llm.

→

2 Comprobar y registrar
Cada llamada queda en un registro encadenado por hash. Autenticación mTLS y/o token; cuerpo: solo hash (por defecto), redactado o completo.

→

3 Verificar
Fail-closed: si se borra un registro o se rompe la cadena, se detiene y avisa de qué registro y cuándo.

Ventajas clave

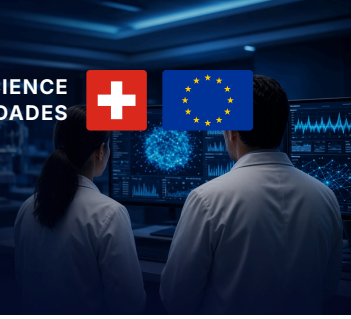
- **MCP y HTTPS**
  Una sola capa de auditoría para MCP, APIs, pasarelas y LLM.
- **Detecta manipulaciones**
  Un registro roto o borrado la detiene y genera una alerta.
- **Usted decide qué se guarda**
  Solo hash por defecto, o cuerpo redactado o completo.
- **Sin reescribir clientes**
  Proxy inverso: el cliente solo cambia la URL base.
- **Informe regulatorio offline**
  Normativas por tipo y país, y si su configuración las soporta.
- **Empiece gratis**
  Edición Community, código abierto (MIT), 240 tests.

Al dorso: en qué se diferencia, ediciones y contacto →

info@castellon.ch castellon.ch

Castellon.CH | GxP Gateway Audit

PARA LABORATORIOS, LIFE SCIENCE Y UNIVERSIDADES



Misma IA, mismas APIs. Todo, registrado.

Complementa el registro de auditoría de sus propios sistemas.

Dónde se sitúa

Clientes
(solo cambia la URL base)

- Asistentes de IA
- Agentes y scripts
- Aplicaciones

GxP Gateway Audit
proxy inverso autoalojado · TLS

MCP/HTTPS

Sus sistemas y servicios
(MCP o HTTPS)

- Servidores MCP
- APIs HTTPS
- Pasarelas
- Endpoints LLM

En qué se diferencia

	Sin auditoría	Logs genéricos	GxP Gateway Audit
Registra llamadas MCP, API y LLM	✗ No	– Según config.	✓ **Sí, los seis flujos**
Detecta modificaciones o borrados	✗ No	✗ No es su objetivo	✓ **Hash + alerta fail-closed**
Decide qué cuerpos se guardan	✗ No	– Depende	✓ **Hash, redactado o completo**
Indica qué normativas soporta	✗ No	✗ No	✓ **Informe regulatorio offline**
Diseñado para flujos GLP/GxP, 21 CFR Part 11 y EU GMP Annex 11	✗ No	✗ No	✓ **Sí**

A diferencia de las pasarelas de IA habituales, centradas en logs, GxP Gateway Audit se basa en un registro encadenado por hash y fail-closed, como complemento al de sus sistemas.

Dos ediciones

Edición Community

DISPONIBLE YA

Gratuita, MIT, v0.4.0 · PyPI, GitHub.

- ✓ Cadena de hash, esquema 1.3.0
- ✓ Manifiestos, revisión
- ✓ mTLS y/o token
- ✓ Informe regulatorio offline

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

Edición Pro

DEMO BAJO PETICIÓN

Edición de pago para equipos regulados.

- Registros firmados
- WORM, SIEM
- SSO, aprobaciones
- Informes, paquete IQ/OQ

Diseñado para dar soporte a flujos de trabajo GLP/GxP, 21 CFR Part 11 y EU GMP Annex 11. Complementa el registro de auditoría de sus sistemas; por sí solo no garantiza el cumplimiento normativo ni sustituye la validación.

Contacto / Solicite una demo

Pruebe gratis la edición Community o solicite una demo de Pro para su laboratorio, empresa o universidad.

Escriba a info@castellon.ch

Antonio Castellon · Castellon.CH
info@castellon.ch
+41 76 689 13 69
castellon.ch
Biel/Bienne, Suiza

GxP Gateway Audit (paquete mcp-glp-audit-proxy). Los registros de la edición Community permiten detectar manipulaciones (encadenados por hash), pero no están firmados. github.com/antonio-castellon/mcp-glp-audit-proxy · pypi.org/project/mcp-glp-audit-proxy