

Guía de integración API y tokens — StateFlowAI

Esta guía está pensada para equipos que necesitan conectar StateFlowAI con otros sistemas, automatizar tareas o incorporar resultados de la plataforma dentro de un flujo operativo más amplio.

El objetivo no es solo explicar que existe una API. El objetivo es ayudarte a integrarla con una lógica sana, de forma que la automatización no termine introduciendo más riesgo del que resuelve.

Cuándo conviene usar la API

La API tiene sentido cuando necesitas algo más que uso manual desde el portal. Por ejemplo:

- automatizar consultas o ejecuciones recurrentes,
- integrar StateFlowAI con backend propio o herramientas internas,
- incorporar resultados en un dashboard, workflow o sistema tercero,
- correr jobs programados,
- mantener trazabilidad técnica de un proceso que no debería depender de una sesión humana.

Si la necesidad es ocasional, exploratoria o de validación rápida, muchas veces conviene empezar por el portal. Si la necesidad es repetible, sistemática o parte de una cadena operativa, la API suele ser la mejor capa.

Formas habituales de autenticación

En términos prácticos, hay dos caminos frecuentes:

- **sesión humana autenticada**, útil para exploración, administración o uso interactivo,
- **app tokens**, pensados para integraciones, automatización y servicios.

La regla general es evitar usar una sesión humana para un proceso que debería ser estable y repetible. Cuando una integración depende de una sesión personal, tarde o temprano aparecen problemas de rotación, trazabilidad o permisos.

Cómo pensar una integración antes de implementarla

Antes de escribir una línea de código, conviene responder estas preguntas:

1. **qué decisión o proceso se quiere automatizar,**
2. **qué modelo o recurso interviene,**
3. **qué tenant debe quedar aislado,**
4. **qué permisos mínimos necesita esa integración,**
5. **qué pasa si la integración falla o devuelve algo inesperado.**

Una integración bien planteada empieza por alcance y responsabilidad, no por copiar un ejemplo rápido.

Recomendaciones para trabajar con tokens

Los tokens son útiles, pero conviene tratarlos como credenciales operativas sensibles. Las prácticas recomendadas son:

- crear un token por integración o servicio, no uno “global para todo”,
- otorgar únicamente los scopes necesarios,
- limitar el acceso al tenant o al recurso que corresponda cuando aplique,
- registrar quién creó el token y con qué objetivo,
- rotarlo cuando cambie el servicio, el proveedor o la responsabilidad,
- retirarlo cuando ya no sea necesario.

Qué patrón suele funcionar mejor

Un patrón sano de implementación normalmente se ve así:

1. definir el caso de uso y el resultado esperado,
2. identificar el tenant y el modelo implicados,
3. crear un token con permisos mínimos,
4. probar la integración en un contexto controlado,
5. validar respuestas, errores y supuestos,
6. recién después incorporarla a un flujo más estable.

Este orden importa. Saltarse pasos suele generar integraciones que “funcionan” en una prueba, pero quedan frágiles cuando se vuelven parte de una operación real.

Casos típicos de integración

Sin entrar en detalle de endpoints concretos, los casos más habituales suelen ser:

- consultar estado o métricas de modelos,
- ejecutar predicciones o secuencias,
- incorporar resultados a otro sistema,
- automatizar procesos internos que requieren una decisión o señal del modelo,
- ordenar cargas, entrenamientos o feedback dentro de un workflow controlado.

Para el detalle puntual de contratos y endpoints, lo correcto es complementar esta guía con la referencia técnica del proyecto.

Errores comunes que conviene evitar

Los problemas más frecuentes no suelen venir de la API en sí, sino de cómo se la usa. Por ejemplo:

- dar más scopes de los necesarios,
- mezclar tenants o entornos sin querer,
- automatizar sin validar el contexto correcto,
- usar un token humano en lugar de uno de aplicación,
- no definir qué hacer ante errores, timeouts o respuestas incompletas,
- promover a producción una integración que solo fue probada “a mano”.

Checklist antes de pasar a algo estable

Antes de dar una integración por válida, conviene revisar esto:

- el caso de uso está bien delimitado,
- el token tiene alcance mínimo,
- el tenant correcto está validado,
- hay forma de rotar o revocar la credencial,
- existe trazabilidad suficiente para soporte,
- el comportamiento esperado frente a errores está definido.

Recomendación práctica final

Una buena integración con StateFlowAI no se reconoce por la cantidad de código, sino por la claridad del contrato operativo.

Si está claro quién usa qué, con qué alcance, sobre qué tenant y para qué decisión, la API suele encajar muy bien. Si eso no está definido, integrar antes de ordenar el problema solo traslada la confusión a producción.