

Antes de conectar un agente

Elegí una tarea concreta. Respondé estas preguntas con el diseño real, no con lo que esperás configurar después.

1. ¿Qué información necesita leer? Anotá la fuente y quién la autoriza.
2. ¿Puede crear, modificar, enviar o borrar algo? Separá cada acción y su consecuencia.
3. ¿Qué permisos sobran para esta tarea? Empezá con el alcance mínimo.
4. ¿Qué acción requiere que una persona vea exactamente lo que ocurrirá y apruebe antes de ejecutarla?
5. ¿Qué registro permitiría reconstruir qué hizo, con qué dato, con qué permiso y con qué resultado?

Mi decisión inicial:

- ☐ Seguir diseñando sin conectar datos ni acciones reales.
- ☐ Probar en un entorno aislado con datos ficticios.
- ☐ Solicitar revisión de permisos, datos y aprobación humana antes de avanzar.

Una respuesta afirmativa no demuestra que un control esté implementado. Para una revisión más amplia, el curso Agentes seguros trabaja 15 controles y su evidencia.