novaeon

LA CHECKLIST · 40 PUNTOS DE CONTROL

Llevar agentes de IA a producción

Novaeon Studio · Maik Buchenau · Versión de noviembre de 2026

Un agente de IA actúa dentro de finanzas, RR. HH., compras o ventas, con autorizaciones reales y consecuencias reales. Esta checklist trata cada agente como cualquier otro cambio en SAP: inventariado, evaluado, probado, aprobado, supervisado y reversible, igual que un transporte. Sirve para agentes de SAP Joule (el ejemplo que se usa a lo largo del documento), agentes propios en SAP BTP y agentes de otros proveedores que acceden a sus datos SAP. 40 puntos de control en 9 bloques. Márquelos, señale las carencias y asigne un responsable a cada uno.

> Nota: SAP está desarrollando Joule y Joule Studio a gran velocidad. Antes de tomar cualquier decisión, verifique fechas, precios y disponibilidad (GA/EA/roadmap) con la documentación actual de SAP y con su propio contrato. Información general, no asesoramiento jurídico. Redactado con ayuda de IA.

1 Inventario y responsabilidades

- [ ] Cada agente tiene un **responsable de negocio** (responsabilidad sobre el proceso) y un responsable técnico (operación).
- [ ] Cada agente figura en **un único inventario**, incluidos los modelos, skills, subagentes y servidores MCP que utiliza. En entornos SAP, este inventario es el **SAP AI Agent Hub** (de LeanIX), que también recoge agentes de otros proveedores.
- [ ] Finalidad, proceso, sistemas afectados y categorías de datos están documentados en una frase («¿Qué puede hacer este agente y qué no?»).
- [ ] Los agentes fuera de SAP que acceden a datos SAP (Copilot, agentes propios vía A2A/MCP) figuran en el mismo inventario.

2 Riesgo y autonomía

- [ ] Cada agente tiene una clasificación de riesgo (p. ej., bajo / medio / alto) según su impacto: dinero, personas, clientes, cumplimiento normativo.
- [ ] El **nivel de autonomía** es una decisión consciente: solo sugerir · actuar con aprobación · actuar de forma autónoma.
- [ ] El **human-in-the-loop** está configurado para cada paso de alto riesgo (una persona aprueba; no basta con una entrada en el log).
- [ ] Comprobado si el caso de uso entra en el **Anexo III del EU AI Act** (p. ej., contratación, promoción, evaluación del desempeño). Las obligaciones para sistemas de alto riesgo se aplican a partir del 2 de diciembre de 2027.

3 Identidad y autorizaciones

- [ ] El agente actúa solo con los permisos del usuario que lo invoca (intersección de usuario y agente); los agentes autónomos tienen su **propia identidad técnica**.
- [ ] Los roles y autorizaciones del agente están descritos en el concepto de autorizaciones y aprobados. Nada de «SAP_ALL para el bot».
- [ ] Las conexiones salientes (destinos, OAuth) siguen el patrón client credentials (máquina a máquina) o JWT bearer (propagación del usuario); ningún secreto en el código.
- [ ] Los agentes propios que se ejecutan en BTP Cloud Foundry están protegidos con IAS. De lo contrario, son accesibles desde internet por defecto.
- [ ] En producción solo se invocan **servidores MCP verificados**.

4 Datos y grounding

- [ ] Documentos de grounding cargados revisados: en Joule son visibles para **todos los usuarios del tenant** (sin permisos por documento). No cargue nada confidencial.
- [ ] Evaluada la calidad de los datos maestros del proceso (un agente que trabaja con datos deficientes solo toma decisiones erróneas más rápido).
- [ ] Decisión tomada sobre el uso de los datos del cliente por parte del proveedor (en SAP: opt-out en SAP for Me); opt-in de logging configurado de forma consciente.
- [ ] Protección de datos: registro de actividades de tratamiento, EIPD cuando proceda y región del centro de datos (p. ej., EU Access) documentados.

5 Pruebas y evaluación

- [ ] Existen casos de prueba para los flujos principales **y** para casos límite (datos faltantes, instrucciones contradictorias, ejecuciones interrumpidas).
- [ ] Pruebas de seguridad: prompt injection, uso indebido de herramientas, fuga de datos a través de las respuestas.
- [ ] Escenarios de evaluación con resultados esperados; criterios de aceptación acordados de antemano (p. ej., tasa de acierto, tolerancia a errores).
- [ ] Las pruebas no solo comprueban que las herramientas se **descubren**, sino que realmente se **invocan** (descubrimiento ≠ invocación): que una herramienta aparezca en la lista no demuestra que el agente pueda llamarla, así que pruebe llamadas reales de extremo a extremo.
- [ ] Prueba de regresión planificada tras cada actualización de release de SAP y cada cambio en el agente.

6 Transporte y aprobación

- [ ] Entornos separados de desarrollo → test → producción; nada se construye directamente en producción.
- [ ] Ruta de transporte definida: Joule Studio clásico mediante **Cloud Transport Management** (MTA); el nuevo Joule Studio mediante despliegues basados en Git; agentes propios a través de su propio pipeline de CI/CD.
- [ ] Cada cambio (prompt, instrucciones, herramientas, cambio de modelo) está **versionado** y pasa por la misma aprobación que el código.
- [ ] Aprobación formal antes del go-live (solicitud de cambio, aprobador, fecha), p. ej., en **SAP Cloud ALM**.
- [ ] Dependencias de release aclaradas: las funciones de Joule solo llegan con las releases actuales. Su calendario de upgrades es su calendario de IA.

7 Operación y supervisión

- [ ] Supervisión continua: uso, tasa de errores, tiempos de respuesta, interrupciones (Agent Hub / Cloud ALM donde esté disponible).
- [ ] Trazabilidad: pista de auditoría por sesión que muestra quién desencadenó qué y con qué resultado.
- [ ] Desviaciones de comportamiento vigiladas (p. ej., process/agent mining en Signavio, controles puntuales por parte del responsable).
- [ ] Proceso de incidencias: una persona designada recibe la alerta cuando un agente actúa incorrectamente, y una persona designada (normalmente el responsable de negocio) está autorizada a desactivarlo.

8 Gastos

- [ ] Consumo estimado por agente: agentes de SAP **0,02 AI Units por acción del agente** (2026); agentes propios según el consumo de recursos.
- [ ] Fin del tiempo de ejecución gratuito para agentes de Joule propios (**31 de diciembre de 2026**) incluido en el presupuesto de 2027.
- [ ] Presupuesto **por agente**, no por usuario; umbral de aviso y límite máximo definidos (las AI Units caducan a los 12 meses).
- [ ] Condiciones contractuales negociadas: precio por AI Unit, volumen incluido, tarifa por exceso y si las unidades no utilizadas pueden trasladarse (por defecto caducan a los 12 meses).
- [ ] Pasos deterministas implementados como **skills** en lugar de pasos del agente (las skills de Joule no se cobran por llamada).

9 Representación de los trabajadores, rollback y retirada

- [ ] **Representación de los trabajadores** involucrada desde el principio cuando existan derechos de codecisión. En Alemania: § 90 BetrVG (cubre expresamente la IA) y § 87(1) no. 6 BetrVG (sistemas capaces de supervisar el comportamiento o el rendimiento). Normalmente esto requiere un acuerdo de empresa.
- [ ] Plan de rollback probado: restaurar la versión anterior o desactivar el agente sin detener el proceso (alternativa manual).
- [ ] Criterios de retirada definidos (valor, gasto, tasa de errores) y una fecha de revisión periódica fijada para cada agente.
- [ ] La retirada incluye la limpieza de: autorizaciones, destinos, entrada en el inventario, documentos de grounding.

Novaeon Studio — la gestión de releases y cambios en SAP se une a los agentes de IA.
¿Quiere revisar sus agentes con esta lista? Reserve una llamada de 30 minutos:
https://novaeon.studio/es/contact/ · office@novaeon.studio