

Agentes de IA programados: cómo trabajan solos sin descontrolarse



¿Cómo se construye un agente de IA que trabaje solo cada día de forma segura? Lo que exploraste, resumido para que lo conserves, lo imprimas y lo uses.

Lo esencial

1. Una automatización con agentes es un agente que se activa solo según un horario cron y deja un registro de cada ejecución.
2. Agente, entorno y sesión son las tres piezas: qué sabe hacer, dónde corre y cada ejecución concreta.
3. Los horarios necesitan zona horaria: conviene evitar la franja de 1 a 3 a. m. local o usar UTC, y esperar una pequeña demora aleatoria.
4. La memoria se monta como una carpeta: solo lectura para lo que el agente no debe cambiar, y lectura y escritura solo donde haga falta.
5. Las claves van en bóvedas: el agente solo ve un marcador y el secreto real sale únicamente hacia los servidores permitidos.
6. Un presupuesto en centavos limita el gasto por ejecución; al alcanzarlo, la sesión queda en pausa y puede pasarse un poco del tope.
7. Estas funciones están en beta: conviene revisar la documentación oficial antes de construir.

Lo que muestran las ayudas visuales

Una ejecución programada. Pasos de una ejecución programada de un agente: el horario cron la dispara, se crea una sesión, el agente trabaja, se guarda el historial y queda un registro.

Cambios de hora y cron. Qué pasa con una ejecución programada cuando adelantan o atrasan el reloj, y cómo evitar que se omita o se repita.

Los límites de la memoria. Límites de los almacenes de memoria de los agentes: tamaño de cada memoria, cantidad por almacén, almacenes por sesión y días que se conservan las versiones.

El viaje de un secreto. Cinco pasos de una credencial guardada en una bóveda: se guarda, se asocia a la sesión, el agente ve un marcador, el secreto sale solo a servidores permitidos y se renueva o archiva.

Hasta dónde llega el gasto. Escala del gasto de una sesión frente a un tope de 50 centavos: por debajo sigue trabajando, al llegar se pausa y la última petición puede pasarse un poco.

Mito o realidad. Cinco afirmaciones sobre agentes programados: el lector decide si son mito, realidad o depende, y compara con la documentación oficial.

Explóralas en <https://grafimaticadigital.com/explorables/agentes-de-ia-programados-como-trabajan-solos-sin>

Para pensar y conversar

- ¿Qué podría salir mal si un agente se ejecuta solo y nadie revisa lo que hace?

- ¿Por qué conviene darle al agente la menor cantidad de permisos posible?

-
-
- ¿Qué tareas de tu colegio o de tu casa te gustaría automatizar, y qué límites le pondrías?
-
-

- ¿Por qué una sesión pausada por presupuesto no es lo mismo que una ejecución fallida?
-
-

Actividad

Diseña en papel una automatización para tu colegio, por ejemplo un resumen semanal de las tareas pendientes. Paso 1: escribe qué lugares leería (solo lectura) y en qué único lugar podría escribir. Paso 2: define el horario y la zona horaria, y evita las horas que se repiten o no existen. Paso 3: lista qué claves necesitaría y quién las guardaría. Paso 4: fija un tope de gasto en centavos y decide qué pasaría al alcanzarlo. Paso 5: intercambia tu diseño con un compañero y busquen fallos.

Fuentes

1. **Claude Managed Agents overview.** Anthropic (documentación de la Claude Platform), 2026. <https://platform.claude.com/docs/en/managed-agents/overview>
2. **Scheduled deployments.** Anthropic (documentación de la Claude Platform), 2026. <https://platform.claude.com/docs/en/managed-agents/scheduled-deployments>
3. **Memory stores.** Anthropic (documentación de la Claude Platform), 2026. <https://platform.claude.com/docs/en/managed-agents/memory>
4. **Vaults and credentials.** Anthropic (documentación de la Claude Platform), 2026. <https://platform.claude.com/docs/en/managed-agents/vaults>
5. **Session budgets.** Anthropic (documentación de la Claude Platform), 2026. <https://platform.claude.com/docs/en/managed-agents/budgets>