CREARAGENTEIA.COM

GUÍA PRÁCTICA 2026

Guía fácil: crea tu primer agente de IA

El camino más corto para pasar de cero a tener un agente funcionando — aunque no sepas programar

Índice de contenidos

Sección 1

Qué vas a conseguir con esta guía

Esta guía es práctica. No es un ensayo filosófico sobre el futuro de la inteligencia artificial ni una tesis académica llena de términos que necesitan diccionario. Es una hoja de ruta directa para que, al terminar de leerla, tengas claro qué es un agente de IA, por qué te importa y, sobre todo, cómo construir el tuyo hoy mismo sin necesidad de saber programar.

Al terminar habrás conseguido:

1. Entender exactamente qué es un agente de IA y en qué se diferencia de un chatbot normal (spoiler: es una diferencia enorme).
2. Identificar cuál de los dos caminos principales —con código o sin código— encaja mejor con tu nivel y tu objetivo.
3. Tener un agente real funcionando, paso a paso, usando la ruta más sencilla disponible en 2026.
4. Saber qué modelo de IA elegir sin agobiarte con opciones y saber cuánto va a costarte, aproximadamente.
5. Conocer los errores típicos que comete todo el mundo al principio y cómo evitarlos.

Una advertencia previa: un agente de IA no es magia. Es una herramienta que puede hacer cosas extraordinarias cuando se diseña bien y cosas desastrosas cuando se diseña mal. Esta guía te da las bases para caer en el primer grupo.

Sección 2

Qué es un agente de IA (explicado fácil)

La analogía del asistente con poderes reales

Imagina que contratas a un asistente personal muy inteligente. Le dices: "Necesito un informe de las tres empresas de la competencia que más han crecido este trimestre, con sus precios y un resumen de sus reseñas de clientes."

Un asistente corriente te diría: "De acuerdo, ¿me pasas la información?"

Un asistente de IA generativo como ChatGPT a secas respondería con algo plausible basado en lo que sabe, pero sin buscar datos actuales ni acceder a nada en tiempo real.

Un **agente de IA** haría otra cosa: abriría su navegador, buscaría las empresas, accedería a las páginas de precios, leería las reseñas, organizaría los datos y te entregaría el informe. Por sí mismo. Sin que le vayas diciendo qué hacer en cada paso.

Esa es la diferencia esencial. **Un agente de IA no solo piensa: actúa.** Tiene un objetivo, tiene herramientas para trabajar con el mundo real y tiene la capacidad de seguir adelante hasta completar la tarea, tomando sus propias decisiones intermedias.

La definición técnica (sin jerga innecesaria)

Un agente de IA es un sistema que:

1. **Recibe un objetivo** ("investiga las tres empresas de la competencia").
2. **Planifica** cómo alcanzarlo ("primero voy a buscar en Google, luego a sus webs...").
3. **Usa herramientas** para actuar (buscadores, APIs, bases de datos, ejecutores de código).
4. **Observa el resultado** de cada acción y decide qué hacer a continuación.
5. **Repite el ciclo** hasta que el objetivo está cumplido.

El motor de razonamiento detrás de todo esto es un **modelo de lenguaje grande** (LLM por sus siglas en inglés), como Claude, GPT-5 o Gemini. Piensa en él como el cerebro que toma las decisiones. Las herramientas son las manos con las que el agente actúa.

El ciclo completo de un agente: percibir, razonar, actuar y observar el resultado.

Sección 3

Agente vs chatbot vs automatización: las diferencias clave

El chatbot tradicional

Un chatbot responde preguntas. Puede tener personalidad, puede mantener el hilo de una conversación y puede ser muy útil para atención al cliente o soporte técnico. Pero solo genera texto. No puede abrir una pestaña del navegador, no puede modificar una hoja de cálculo, no puede enviar un correo por su cuenta. **Cuando acabas la conversación, el chatbot no ha cambiado nada en el mundo.**

La automatización clásica

Una automatización (Zapier, Make, un script) ejecuta una secuencia de pasos predefinida. Si llega un email con una factura adjunta, extrae el PDF, lo sube a Google Drive y lo añade a una hoja de cálculo. Funciona perfectamente para eso, pero solo para eso. Si el proceso cambia, alguien tiene que rediseñarlo manualmente. **No razona ni se adapta: ejecuta instrucciones fijas.**

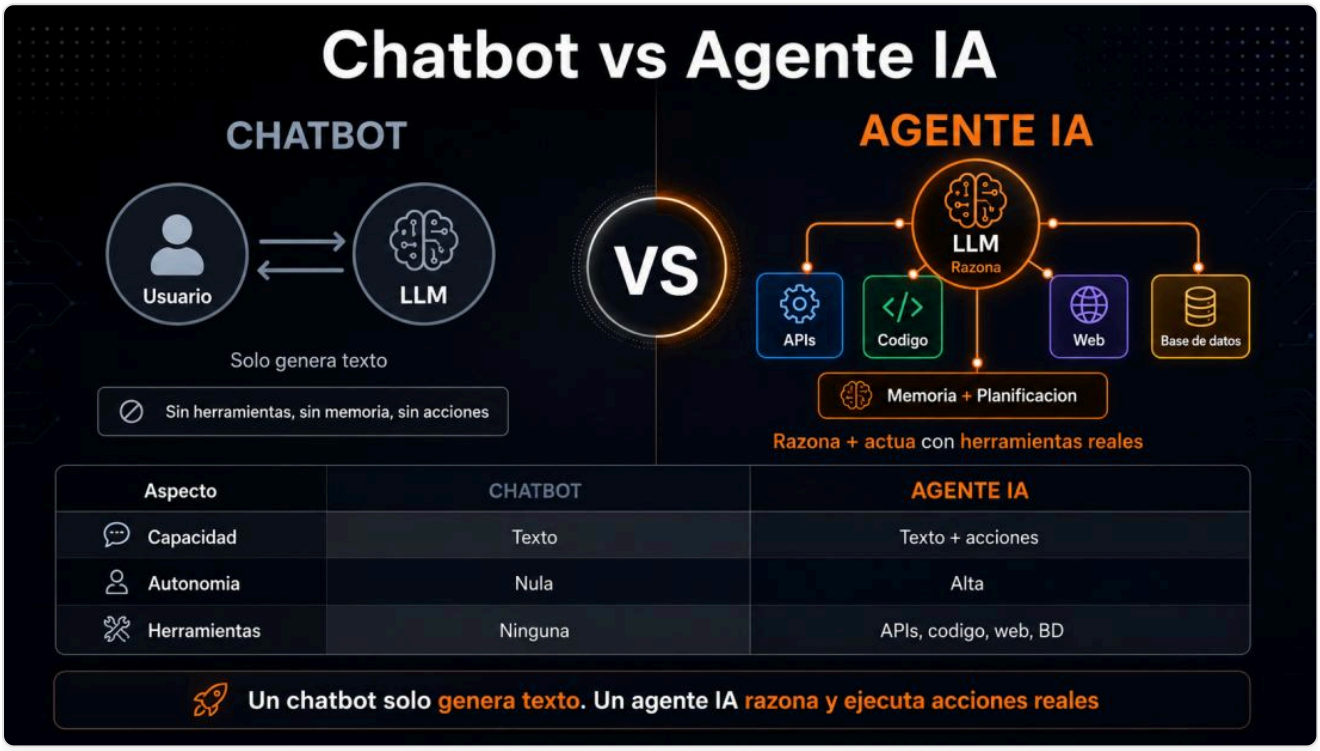
El agente de IA

Un agente combina lo mejor de los dos mundos y añade algo que ninguno de los dos tiene: **autonomía con razonamiento**. Puede mantener una conversación como un chatbot, puede ejecutar acciones como una automatización, pero además puede decidir por sí mismo qué pasos dar para alcanzar un objetivo que nadie le ha descrito paso a paso.

Característica	Chatbot	Automatización	Agente IA
Genera texto	Sí	No	Sí
Ejecuta acciones reales	No	Sí (fijas)	Sí (adaptativas)
Razona y planifica	No	No	Sí
Se adapta a situaciones nuevas	No	No	Sí
Mantiene conversación	Sí	No	Sí
Trabaja de forma autónoma	No	Parcialmente	Sí

CONSEJO

No hay una herramienta mejor que otra en abstracto. Si solo necesitas responder preguntas frecuentes, un chatbot es más que suficiente. Si tienes un proceso de pasos fijos y bien definidos, una automatización es más fiable y barata. El agente tiene sentido cuando el problema es complejo, variable o necesita razonamiento real.



Chatbot vs agente de IA: las diferencias que importan en la práctica.

Sección 4

Los 3 ingredientes de todo agente

Todo agente de IA, sea simple o complejo, está hecho de tres ingredientes fundamentales. Entenderlos te ayuda a diseñar mejor desde el primer momento.

Ingrediente 1: El modelo (el cerebro)

El modelo de lenguaje grande es quien toma las decisiones. Cuando el agente recibe una tarea, es el modelo quien piensa: "Para hacer esto, primero necesito buscar X, luego calcular Y, luego escribir Z." El modelo no hace nada por sí solo; es como un director muy inteligente que da órdenes pero necesita personal que las ejecute.

Los modelos más usados en 2026 son Claude (de Anthropic), GPT-5 (de OpenAI) y Gemini (de Google). Cada uno tiene sus fortalezas. Los veremos en detalle en la Sección 7.

Ingrediente 2: Las herramientas (las manos)

Las herramientas son las acciones que el agente puede ejecutar en el mundo real. Sin herramientas, el agente solo puede pensar pero no actuar, lo que lo convierte básicamente en un chatbot muy elaborado.

Ejemplos de herramientas habituales:

- **Búsqueda web:** el agente puede buscar información actual en internet.
- **Ejecución de código:** puede escribir y ejecutar código Python para calcular, analizar datos o transformar información.
- **Lectura y escritura de archivos:** puede leer documentos, generar PDFs o actualizar hojas de cálculo.
- **Llamadas a APIs:** puede interactuar con servicios externos como tu CRM, tu sistema de pedidos o tu correo.
- **Bases de datos:** puede consultar y modificar registros en bases de datos.

Cuantas más herramientas tenga el agente, más cosas puede hacer. Pero también más superficie de error hay. Para empezar, lo mejor es un agente con pocas herramientas bien definidas.

Ingrediente 3: La memoria (el contexto)

Los modelos de lenguaje son, por naturaleza, desmemoriados: cada vez que los llamas empiezan desde cero. La memoria del agente es lo que permite que recuerde qué ha hecho antes, qué ha aprendido sobre el usuario o el problema, y cómo estaba el estado de la tarea cuando se interrumpió.

Hay dos tipos:

- **Memoria de corto plazo:** lo que cabe en la conversación actual. Los modelos modernos como Claude Opus 4.7 o GPT-5.5 tienen ventanas de contexto de hasta 1 millón de tokens, equivalente a

leer varios libros seguidos.

- **Memoria de largo plazo:** una base de datos externa donde el agente guarda información entre sesiones.

Para tu primer agente, no necesitas preocuparte por la memoria de largo plazo. La de corto plazo es suficiente para empezar.

Los tres componentes fundamentales de cualquier agente de IA.

Sección 5

Elige tu camino: con código o sin código

Antes de ponerte a construir nada, la pregunta más importante que puedes hacerte es: **¿necesito escribir código?**

La respuesta honesta es: probablemente no, al menos para empezar.

La tabla de decisión

Pregunta	Sin código	Con código
¿Sabes programar?	No importa	Ayuda mucho
¿Cuánto tiempo tienes para el primer agente?	20-60 minutos	1-3 días
¿El agente necesita integraciones con apps conocidas?	Sí, ideal	También, más trabajo
¿Necesitas lógica de negocio muy específica?	Limitado	Sin límites
¿El agente va a manejar miles de usuarios al día?	Depende de la plataforma	Más control
¿Necesitas que los datos no salgan de tu servidor?	Complicado	Posible
¿Quieres control total sobre errores y comportamiento?	Limitado	Total

El camino sin código

Plataformas como **n8n**, **Make**, **Flowise** y los **Custom GPTs de ChatGPT** te permiten construir agentes funcionales arrastrando y conectando bloques visuales. Sin escribir una sola línea de código. Son ideales para automatizar flujos de trabajo con aplicaciones que ya usas, crear asistentes especializados para tu equipo y prototipar una idea rápidamente. Cubren el **80% de los casos de uso habituales**.

El camino con código

Python con frameworks como **LangChain**, **CrewAI** o el **Claude Agent SDK** te da control total sobre cada aspecto del agente. Es el camino correcto cuando necesitas integrar sistemas propietarios, el proceso de negocio es muy específico o quieres construir un sistema multi-agente.

> **CONSEJO**
>
> Si no tienes experiencia programando, empieza sin código. No lo estás haciendo "mal"; lo estás haciendo inteligentemente. Muchos agentes en producción en empresas reales están construidos con n8n o plataformas similares. El código viene después, si lo necesitas.

Las dos rutas principales para construir tu primer agente de IA.

Sección 6

Tu primer agente SIN código en 20 minutos

Vas a construir un agente real ahora mismo. Dos opciones según lo que tengas disponible: un **Custom GPT en ChatGPT** (el camino más rápido) y un **agente en n8n** (más potente y gratuito). Elige la que mejor encaje con tu situación.

Opción A: Custom GPT en ChatGPT (10-15 minutos)

Requisito: cuenta de ChatGPT Plus (actualmente 20 USD al mes). Si no la tienes, salta a la Opción B.

1. **Accede al GPT Builder.** Entra en chatgpt.com con tu cuenta Plus. En el panel izquierdo, haz clic en "Explorar GPTs" y luego en el botón "Crear" en la esquina superior derecha.
2. **Describe tu agente en lenguaje natural.** El GPT Builder te preguntará para qué quieres que sirva tu GPT. Escribe una descripción clara del objetivo, el tono y las limitaciones.
3. **Afina las instrucciones en la pestaña "Configurar".** Edita las instrucciones manualmente, sube documentos de conocimiento (PDFs, Word, hasta 20 archivos) y activa capacidades como búsqueda web.
4. **Prueba antes de publicar.** Usa el panel de preview para hablar con tu agente. Hazle preguntas difíciles, incluyendo casos límite y preguntas que debería rechazar.
5. **Publica y comparte.** Haz clic en "Guardar" y elige el nivel de visibilidad: solo tú, cualquiera con el enlace, o público.

> **CONSEJO**
>
> Escribe las instrucciones como si le explicaras el trabajo a una persona nueva que no conoce nada de tu negocio. Sé explícito. No asumas que el agente "ya sabe" cosas evidentes para ti.

El proceso completo de creación de un Custom GPT en ChatGPT.

Opción B: Agente con n8n (20-30 minutos, gratuito)

n8n es una plataforma open-source de automatización con IA. En su versión self-hosted es completamente gratuita. Tiene más de 400 integraciones nativas y permite conectarse a cualquier LLM.

1. **Arranca n8n.** Ejecuta en tu terminal: `npx n8n`. Esto instala n8n automáticamente y lo levanta en `http://localhost:5678`. Alternativamente, activa la prueba gratuita de 14 días en n8n.io.
2. **Crea un nuevo flujo de trabajo.** Haz clic en "New workflow" en el panel principal. Verás un lienzo vacío donde vas a conectar nodos.
3. **Define el trigger.** Usa el nodo "Chat Trigger" para una primera prueba. En producción el trigger puede ser un email, un mensaje de Slack, un webhook o un horario programado.
4. **Añade el nodo "AI Agent".** Este nodo implementa el bucle completo de razonamiento. Elige el modelo de IA (Claude Haiku 4.5 o GPT-5.4 mini para empezar) y escribe el system prompt que define el comportamiento del agente.
5. **Conecta herramientas (opcional).** Puedes añadir herramientas en la sección "Tools" del nodo AI Agent: HTTP Request, Calculator, Code, Google Sheets, etc.
6. **Prueba el agente.** Haz clic en "Test workflow". Observa el log de cada paso para entender cómo razona el agente y ajusta el system prompt si algo no funciona.
7. **Activa el flujo.** Cuando estés satisfecho, activa el flujo con el botón "Active". n8n lo mantendrá corriendo permanentemente.

> **CONSEJO**
>
> En la primera semana, revisa el historial de ejecuciones todos los días. n8n guarda el log completo de cada ejecución. Es la herramienta más valiosa para entender por qué el agente hace lo que hace.

Un agente construido en n8n: el nodo AI Agent conectado al trigger y las herramientas.

Sección 7

Qué modelo elegir (resumen práctico 2026)

La regla del 80/20

Para el 80% de los casos de uso de agentes, cualquier modelo bueno de nivel intermedio es más que suficiente. La diferencia entre modelos se nota en tareas muy específicas: razonamiento matemático complejo, código avanzado, análisis de documentos largos. Para un agente de atención al cliente, de generación de contenido o de automatización de procesos, la diferencia práctica entre los mejores modelos es pequeña.

Los tres grandes proveedores en 2026

Proveedor	Modelo	Contexto	Precio (entrada/salida por M tokens)	Mejor para
Anthropic	Claude Sonnet 4.6	1M tokens	$3 / $15	Agentes de uso general, escritura, análisis
Anthropic	Claude Haiku 4.5	200K tokens	$1 / $5	Tareas rápidas y alto volumen
Anthropic	Claude Opus 4.7	1M tokens	$5 / $25	Tareas muy complejas, razonamiento avanzado
OpenAI	GPT-5.4 mini	1M tokens	~$0,25 / $2	Volumen alto, coste bajo
OpenAI	GPT-5.5	1M tokens	$5 / $30	Tareas de alta precisión
Google	Gemini 3.5 Flash	1M tokens	$1,50 / $9	Velocidad, multimodalidad
Google	Gemini 3.1 Pro	2M tokens	$2 / $12	Contextos muy largos, documentos extensos

Nota sobre "tokens": un token equivale aproximadamente a tres cuartos de una palabra en inglés. Un millón de tokens son aproximadamente 750.000 palabras, equivalente a unos 6-8 libros de longitud media.

¿Y los modelos gratuitos?

- **Gemini Flash-Lite de Google:** tiene un tier gratuito reducido, suficiente para experimentar.
- **Mistral Small 4 y DeepSeek V4 Flash:** opciones económicas con muy buena relación calidad-precio.

- **Modelos locales con Ollama:** instala Llama o Mistral en tu ordenador. Gratis pero requiere GPU.

La recomendación para empezar

- **Con Custom GPT de ChatGPT:** el modelo está incluido en el plan Plus, no tienes que elegir nada.
- **Con n8n:** empieza con **Claude Haiku 4.5** (rápido y económico) o **GPT-5.4 mini** (muy barato).

> **CONSEJO**
>
> El modelo no es lo más importante de tu agente. Las instrucciones (el system prompt) y las herramientas disponibles tienen más impacto en la calidad del resultado que la diferencia entre un modelo bueno y uno muy bueno. Empieza con algo económico y optimiza después.

Panorama de los modelos LLM disponibles para agentes en mayo de 2026.

Sección 8

Cuánto cuesta (rangos realistas y cómo no gastar de más)

El coste de un agente de IA tiene dos componentes principales: la **plataforma** (si usas una) y el **modelo de lenguaje** (el uso de la API).

Costes de plataforma

Plataforma	Tier gratuito	Primer tier de pago	Notas
n8n self-hosted	Gratis	Gratis	Solo pagas el servidor (~5-10 USD/mes) y la API del LLM
n8n cloud	14 días de prueba	20 USD/mes	2.500 ejecuciones al mes incluidas
Make	1.000 operaciones/mes	9 USD/mes	Bueno para empezar
Flowise self-hosted	Gratis	Gratis	Open-source, mismo esquema que n8n
ChatGPT Plus (Custom GPTs)	No	20 USD/mes	El modelo está incluido; no pagas tokens adicionales
Zapier AI	5 automatizaciones gratis	19,99 USD/mes	Más limitado para agentes

Costes del modelo de IA (por uso)

Se paga por "tokens procesados": cada llamada al agente consume tokens de entrada (el contexto, el system prompt, el historial) y genera tokens de salida (la respuesta).

Ejemplo real con Claude Sonnet 4.6 ($3 entrada / $15 salida por millón de tokens):

- Un agente de atención al cliente con conversaciones de longitud media (500 tokens entrada + 200 tokens salida): **~0,005 USD por conversación.**
- Para 1.000 conversaciones al mes: unos **5 USD** en tokens.
- Para 10.000 conversaciones: unos **50 USD** en tokens.

¿Cómo no gastar de más?

1. **Empieza con modelos económicos:** Claude Haiku 4.5 o GPT-5.4 mini cuestan entre un 70% y un 90% menos que los modelos flagship.

2. **Controla el tamaño del contexto:** un system prompt de 5.000 tokens que se repite en cada llamada multiplica los costes. Escríbelo conciso.
3. **Pon límites al agente:** configura un número máximo de pasos por tarea (por ejemplo, no más de 10 iteraciones).
4. **Monitoriza desde el día uno:** revisa el dashboard de uso cada semana al principio para detectar consumos anómalos.
5. **Usa caché:** los proveedores como Anthropic ofrecen descuentos del 90% en tokens repetidos (el system prompt, por ejemplo).

¿Cuánto esperar pagar para un primer agente?

- **Custom GPT de ChatGPT:** 20 USD al mes (todo incluido).
- **n8n cloud + Claude Haiku:** 20-25 USD/mes (plataforma) + 5-20 USD en tokens.
- **n8n self-hosted + cualquier modelo:** 5-10 USD/mes en servidor + coste de tokens.
- **Completamente gratuito:** n8n en local + modelo local con Ollama = 0 USD (requiere GPU).

Los componentes de coste de un agente de IA y cómo controlarlos.

Sección 9

Errores típicos de principiante y cómo evitarlos

Estos son los errores que comete casi todo el mundo la primera vez. Leerlos ahora te ahorra horas de frustración.

Error 1: Un system prompt vago

"Eres un asistente útil" no es un system prompt: es una instrucción sin valor. El modelo no sabe quién eres, qué hace tu empresa, cuál es el tono correcto, qué puede y qué no puede hacer.

Cómo evitarlo: escribe el system prompt como si fuera el primer día de trabajo de un empleado nuevo. Incluye: quién es el agente, qué empresa representa, qué puede hacer, qué no puede hacer, cómo debe responder cuando no sabe algo y qué tono debe mantener.

Error 2: Dar demasiadas herramientas a la vez

Conectar el agente a 15 herramientas desde el primer día hace que el modelo se confunda y elija las herramientas equivocadas con más frecuencia.

Cómo evitarlo: empieza con una o dos herramientas. Cuando el agente las use correctamente de forma consistente, añade más.

Error 3: No probar con casos difíciles

Probar el agente solo con las preguntas "felices" es insuficiente. En producción, los usuarios van a hacer preguntas extrañas, escribir con errores y preguntar cosas fuera del alcance del agente.

Cómo evitarlo: antes de lanzar, prueba con al menos 20 casos distintos, incluyendo preguntas capciosas, preguntas sin respuesta y casos límite.

Error 4: No poner límites de iteración

Un agente sin límites puede entrar en un bucle infinito intentando completar una tarea imposible, consumiendo tokens y dinero sin parar.

Cómo evitarlo: configura siempre un número máximo de pasos. Para tareas simples, 5-10 pasos es suficiente; para tareas complejas, 20-30.

Error 5: Lanzar sin monitorización

Un agente en producción puede empezar a fallar silenciosamente: responder incorrectamente, no usar las herramientas cuando debería o consumir más tokens de lo esperado. Sin monitorización, no te enteras hasta que el daño está hecho.

Cómo evitarlo: activa las notificaciones de error desde el primer día. Revisa el historial de ejecuciones periódicamente. Configura alertas de gasto en el dashboard del proveedor del LLM.

Error 6: Confundir el agente con un oráculo infalible

Los modelos de lenguaje alucinan: a veces inventan información con total confianza. Un agente puede devolver una respuesta incorrecta, especialmente en dominios muy específicos.

Cómo evitarlo: diseña el agente para que indique cuándo no tiene información suficiente ("No tengo datos sobre eso") en lugar de inventar.

> **CONSEJO**
>
> Un agente que sabe decir "no sé" es infinitamente más valioso que uno que inventa. Instruye explícitamente al agente para que reconozca sus límites.

Sección 10

Seguridad básica: qué NO hacer

Un agente mal diseñado puede causar problemas reales: enviar información confidencial a quien no debe, ejecutar acciones irreversibles por error o ser manipulado por un usuario malintencionado. Estas reglas básicas aplican desde el primer día.

Regla 1: Permisos mínimos

Tu agente solo debe poder hacer lo que necesita para su tarea. Si el agente de atención al cliente solo necesita leer pedidos, no le des acceso para modificarlos o borrarlos. La pregunta correcta es: "¿Qué es lo mínimo que este agente necesita para hacer su trabajo?"

Regla 2: Nunca incrustes credenciales en el system prompt

Las claves de API, contraseñas o tokens de acceso no deben aparecer jamás en el system prompt. Usa las variables de entorno o los sistemas de gestión de secretos que ofrece la plataforma.

Regla 3: Confirmación humana para acciones irreversibles

Si el agente puede borrar datos, enviar emails masivos, hacer pagos o publicar contenido, añade un paso de confirmación humana antes de ejecutar la acción. Un "¿Estás seguro?" puede evitar desastres.

Regla 4: Mantén un registro de lo que hace el agente

Activa los logs de todas las acciones. Debes poder responder: ¿qué hizo el agente? ¿Cuándo? ¿Con qué datos? ¿Cuál fue el resultado? Esto es esencial para depurar errores y cumplir con el GDPR.

Regla 5: Cuidado con el "prompt injection"

El prompt injection es una técnica por la que un usuario malintencionado intenta hacer que el agente ignore sus instrucciones. **Cómo mitigarlo:** instrúyele explícitamente en el system prompt para que no revele sus instrucciones ni siga peticiones que contradigan su función.

Regla 6: No conectes el agente a datos sensibles sin protección

Si el agente tiene acceso a datos de clientes, información financiera o datos de salud, asegúrate de que la conexión está cifrada, que solo el agente tiene acceso y que cumples con la normativa aplicable (GDPR en Europa).

Las principales amenazas de seguridad en agentes de IA y cómo mitigarlas.

Sección 11

Siguientes pasos: cómo seguir aprendiendo

Tienes tu primer agente funcionando. El camino natural después es profundizar en tres direcciones según lo que necesites.

Si quieres más potencia sin código

Explora las funciones avanzadas de n8n: memoria persistente con Redis, integración con bases de datos propias y configuración de múltiples agentes que se pasan trabajo entre ellos.

En crearagenteia.com tienes: guía completa de n8n con casos de uso avanzados y guía de Custom GPTs con Actions y conocimiento personalizado.

Si quieres pasar al código

El paso siguiente natural es aprender Python básico y los frameworks de agentes más usados:

- **LangChain:** el más popular, con una documentación extensa y una comunidad enorme.
- **CrewAI:** diseñado para sistemas multi-agente donde varios agentes con roles distintos colaboran.
- **Claude Agent SDK:** el SDK oficial de Anthropic para construir agentes con Claude de forma estructurada.

Si quieres entender los modelos en profundidad

El sitio tiene una sección dedicada a cada modelo: Claude, GPT-5, Gemini y las alternativas de código abierto como DeepSeek y Mistral. Con análisis de precios, capacidades y casos de uso ideales para cada uno.

Recursos en crearagenteia.com

- **/que-es-un-agente-ia/** — Referencia completa sobre qué es un agente, tipos y componentes.
- **/como-crear-agente-ia/** — Hub central con todos los métodos de creación.
- **/como-crear-agente-ia/sin-codigo/** — Comparativa completa de plataformas no-code.
- **/como-crear-agente-ia/n8n/** — Tutorial completo de n8n con casos de uso avanzados.
- **/frameworks/** — Comparativa de todos los frameworks de agentes.
- **/frameworks/selector/** — Quiz interactivo: responde 6 preguntas y descubre tu framework.
- **/modelos/** — Análisis de todos los modelos LLM para agentes en 2026.

CONSEJO

El aprendizaje más efectivo en este campo es construir cosas reales. No leas 10 tutoriales antes de intentar nada. Construye algo pequeño, fállalo, arréglalo y repite. El conocimiento que se queda es el que se gana con las manos.

El ecosistema completo de los agentes de IA: conceptos, herramientas y rutas de aprendizaje.

Sección 12

Checklist final imprimible

Usa esta lista antes de declarar que tu agente está listo para producción. Marca cada punto cuando esté resuelto.

FASE 1 — DISEÑO

- [ ] He definido claramente el objetivo del agente (una tarea específica, no "todo").
- [ ] He identificado quiénes son los usuarios del agente y qué esperan.
- [ ] He decidido si necesito código o si el no-code es suficiente.
- [ ] He elegido la plataforma adecuada para mi caso de uso.
- [ ] He elegido el modelo de IA y tengo una estimación de costes.

FASE 2 — CONSTRUCCIÓN

- [ ] El system prompt es específico, claro y define el tono, las capacidades y los límites.
- [ ] Las herramientas conectadas son las mínimas necesarias para la tarea.
- [ ] He configurado un límite máximo de iteraciones para evitar bucles infinitos.
- [ ] No hay credenciales ni datos sensibles en el system prompt ni en campos de texto visibles.
- [ ] Las acciones irreversibles requieren confirmación antes de ejecutarse.

FASE 3 — PRUEBAS

- [ ] He probado con al menos 20 casos distintos, incluyendo casos límite y preguntas fuera del alcance.
- [ ] He verificado que el agente sabe decir "no sé" cuando no tiene información suficiente.
- [ ] He intentado hacer "prompt injection" y el agente lo ha resistido.
- [ ] He revisado los logs de las pruebas y no hay comportamientos inesperados.
- [ ] He estimado el coste real por conversación con los datos de las pruebas.

FASE 4 — LANZAMIENTO Y MONITORIZACIÓN

- [ ] Los logs están activos y puedo consultar el historial de ejecuciones.

- [ ] Tengo alertas de gasto configuradas en el dashboard del proveedor del LLM.
- [ ] Tengo una forma de recibir feedback de los usuarios.
- [ ] He documentado cómo funciona el agente para poder mantenerlo en el futuro.
- [ ] Tengo un plan para actualizar el agente cuando cambien las necesidades.

Esta guía es un recurso vivo. Si algo ha cambiado desde que la descargaste, la versión más actualizada de cada tema está en crearagenteia.com.

Mayo 2026 | crearagenteia.com