# INFORME PROFESIONAL

Modo agente (ChatGPT)

Versión: 31 de agosto de 2025

## Resumen ejecutivo

El modo agente de ChatGPT permite que el asistente piense y actúe para completar tareas complejas de principio a fin usando un ordenador virtual propio. Integra navegación web, análisis de archivos, generación de entregables (hojas de cálculo y presentaciones), ejecución de código y conectores con servicios autorizados por el usuario. Es un despliegue progresivo disponible en planes de pago. La funcionalidad de Operator ha sido integrada en este modo.

## 1. ¿Qué es el modo agente?

Es la capacidad de ChatGPT para alternar razonamiento y acción, eligiendo de forma autónoma las herramientas adecuadas (navegación, lectura de archivos, código, etc.) hasta entregar un resultado. En la práctica, es como si el asistente dispusiera de un ordenador propio para trabajar bajo tu supervisión.

## 2. Disponibilidad y activación

• Disponible en planes de pago (Plus/Pro/Team/Enterprise/Edu) con despliegue gradual por oleadas.

• Operator está integrado en ChatGPT como “ChatGPT agent”; la web independiente se retira.

• Activación cuando esté disponible en tu cuenta: desde el desplegable del cuadro de mensaje eligiendo “Agent mode”.

• Deep research (agente de investigación multi■paso) está disponible para usuarios de pago y se integra en el flujo del modo agente.

• Los conectores (p. ej., Gmail, Google Calendar y Google Contacts) pueden usarse tras habilitarlos en la cuenta.

## 3. Capacidades principales (detalle)

### 3.1 Navegación y operaciones web

• Abre sitios, sigue enlaces, completa formularios y extrae información estructurada. • Puede adjuntar enlaces o capturas relevantes en sus respuestas cuando investiga.

### 3.2 Trabajo con archivos y entregables

• Lee y cruza información de archivos subidos o conectados. • Genera hojas de cálculo con limpieza/transformación de datos y crea presentaciones de resumen.

### 3.3 Ejecución de código

• Ejecuta código (como Python) en entorno aislado para analizar datos, convertir formatos o automatizar pasos auxiliares.

### 3.4 Conectores y cuentas

• Con autorizaciones explícitas, puede consultar conectores (Gmail, Calendar, Contacts, Drive empresarial, etc.) • Algunos conectores pueden utilizarse también dentro de deep research o en chat

según las notas de versión.

## 3.5 Agente de uso de ordenador (CUA)

• El modelo Computer■Using Agent (CUA) combina visión y razonamiento entrenados por refuerzo para interactuar con interfaces gráficas como lo haría una persona (clics, scroll, formularios).

## 3.6 Herramientas internas del agente

• Navegador visual: el agente interactúa con sitios web como un usuario (clics, scroll, formularios) y muestra una narración de lo que hace. Para inicios de sesión, te pedirá que completes las credenciales manualmente.

• Intérprete de código: permite ejecutar código (p. ej., para limpiar y transformar datos) dentro de un entorno aislado.

• Conectores (solo con tu permiso): Gmail, Google Calendar y Google Contacts, entre otros, para obtener contexto de lectura. No accede a tus archivos locales salvo que los subas.

• Entregables: puede crear/editar hojas de cálculo y presentaciones como parte del flujo, y adjuntar los archivos en el chat.

## 3.7 Flujo operativo real (paso a paso)

## 1) Arranque: activas “Agent mode” y defines la meta (qué quieres, con qué formato y criterios de éxito).

## 2) Ejecución: alterna planificación, acción y verificación (navega, extrae datos, transforma, revisa) con tu supervisión.

## 3) Permisos: solicita confirmación antes de acciones con consecuencias (envíos, formularios, etc.).

## 4) Entrega: adjunta resultados y enlaces/capturas a las fuentes consultadas.

## 5) Repetición (si está disponible): puedes programar la tarea para repetirla de forma periódica.

## 3.8 Qué sí puede y qué no

Sí puede: navegar sitios, rellenar formularios, leer/transformar archivos subidos, editar hojas y diapositivas, ejecutar código, usar conectores habilitados por ti, y citar fuentes.

No puede: acceder a tu equipo local sin que subas archivos, saltar bloqueos de sitios restringidos o suplantar tus credenciales; algunos recursos pueden no estar disponibles según plan y políticas.

## 3.9 Seguridad y datos

• Confirmaciones: pide permiso antes de pasos sensibles.

• Aislamiento: las acciones se realizan en un ordenador virtual seguro.

• Buenas prácticas: habilita solo los conectores necesarios; revisa siempre antes de confirmar operaciones; exige enlaces a fuentes cuando se usen datos públicos.

## 3.10 Relación con otros productos de OpenAI

• Operator: se integra dentro de ChatGPT como ‘ChatGPT agent’.

• Deep Research: agente de investigación multipaso que se combina con el modo agente para ejecutar acciones tras investigar.

• CUA (Computer■Using Agent): base técnica que permite interactuar con interfaces gráficas.

## 4. Cómo opera (alto nivel)

• Plan → Actúa → Verifica: alterna pasos de planificación, ejecución y comprobación hasta cumplir tu objetivo. • Control del usuario: puedes pausar o detener, y se solicitará confirmación antes de acciones sensibles. • Entorno aislado: las acciones ocurren en un ordenador virtual seguro.

## 5. Seguridad, privacidad y gobierno

• Confirmaciones previas a acciones de impacto (compras, reservas, envíos, etc.). • Aislamiento en ordenador virtual y defensas frente a ataques de inyección de prompts documentadas en la System Card. • En organizaciones, administradores pueden restringir capacidades y definir políticas.

## 6. Límites y estado de madurez

• Despliegue gradual: la presencia del menú en gris indica que tu cuenta aún no está activada. • Posibilidad de errores: aunque potente, requiere supervisión humana en tareas críticas. • Acceso a datos: solo a contenidos que subas o conectes de forma explícita.

## 7. Guía rápida de uso (cuando lo tengas activo)

## 1) Selecciona “Agent mode” en el menú del cuadro de mensaje. 2) Define la meta y los criterios de éxito (tablas/columnas, formatos, plazos, entregables). 3) Supervisa los permisos y corrige si se desvía. 4) Exporta el entregable (spreadsheet/diapositivas/informe) y valida.

## 8. Buenas prácticas

• Define objetivos medibles y formatos de salida desde el inicio.

• Divide en fases: primero recolecta y cita; luego transforma; finalmente presenta.

• Exige fuentes oficiales enlazadas cuando se trate de datos públicos.

• Revisa antes de ejecutar acciones con consecuencias.

• Documenta supuestos y limita el alcance cuando haya incertidumbre.

## 9. Preguntas frecuentes

¿Está disponible en cuentas gratuitas? — No, de momento solo en planes de pago.

¿Cita fuentes? — Sí: puede adjuntar enlaces o capturas en informes de investigación.

¿En qué dispositivos funciona? — Web, móviles (iOS/Android) y apps de escritorio (macOS/Windows).

¿Sustituye a Operator? — Sí, Operator se integra como ChatGPT agent y el sitio independiente queda descontinuado.

## 10. Nota contextual: “Agent mode” en otras plataformas (resumen breve)

En el ecosistema tecnológico, “modo agente” suele referirse a asistentes que ejecutan acciones por ti dentro de un IDE o una terminal. Aunque el presente informe se centra en ChatGPT, en el mercado existen aproximaciones similares para editores de código y terminales. Las capacidades, seguridad y disponibilidad varían por proveedor y suelen cambiar con frecuencia; consulta la documentación oficial de cada producto.