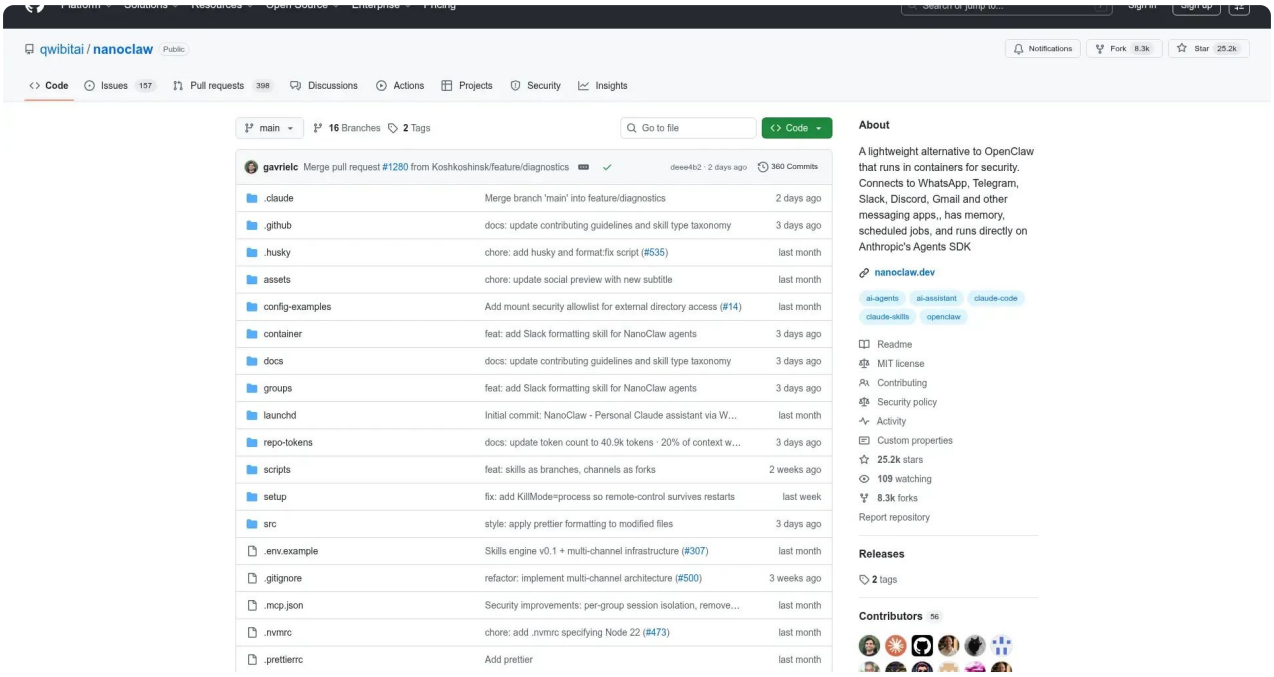

NanoClaw

NanoClaw es un asistente de IA personal de código abierto diseñado para profesionales con mentalidad self-hosted que buscan automatizar flujos de trabajo mediante mensajería. Permite conectar modelos como Claude con WhatsApp, Slack o Telegram para ejecutar comandos, gestionar archivos y realizar búsquedas web en entornos Linux aislados mediante Docker. Es ideal para desarrolladores y analistas que requieren un agente autónomo seguro, minimalista y capaz de realizar tareas programadas sin comprometer la privacidad del sistema anfitrión.

Visitar Sitio Oficial Preguntar a ChatGPT Preguntar a Claude Preguntar a Grok

Contenido del Dossier

- Información de la Herramienta
- Consejos de Implantación
- Preguntas Frecuentes
- Contratos y Condiciones

INFORMACIÓN DE LA HERRAMIENTA

Qué y para quién es
NanoClaw es un asistente de IA personal de código abierto diseñado para ejecutarse de forma local y segura. A diferencia de otras soluciones monolíticas, es una herramienta "AI-native" y minimalista (aprox. 15 archivos fuente) que conecta modelos de lenguaje (principalmente Claude) con aplicaciones de mensajería diarias.

Está dirigido a profesionales con mentalidad "self-hosted" que buscan un asistente autónomo con acceso a sus herramientas de trabajo, pero que no están dispuestos a comprometer la privacidad de sus datos o la seguridad de su sistema operativo.

Principal ventaja profesional
Seguridad por aislamiento real: cada sesión del agente se ejecuta en contenedores Linux independientes (Docker o Apple Container). Esto permite que la IA ejecute comandos, gestione archivos y acceda a la web en un entorno estanco, evitando que un error o una acción imprevista del modelo comprometa el equipo anfitrión.

Para quién no es
No es para usuarios que buscan una solución "Plug & Play" con interfaz gráfica (no tiene panel de control visual). Tampoco es adecuado para departamentos corporativos rigidly closed que prohíban el uso de terminales o la ejecución de Docker en puestos locales, ni para quienes no se sientan cómodos delegando la configuración en una línea de comandos (CLI).

funcionalidades clave
- **Multicanalidad:** Conexión directa con WhatsApp, Telegram, Slack, Discord y Gmail.
- **Aislamiento por Grupos:** Cada grupo de chat tiene su propia memoria (CLAUDE.md) y sistema de archivos aislado.
- **Tareas Programadas:** Capacidad para ejecutar trabajos recurrentes (ej. informes matutinos) y enviar los resultados por mensajería.
- **Acceso Web:** Búsqueda y extracción de contenido en tiempo real para investigación.
- **Swarms de Agentes:** Posibilidad de desplegar equipos de agentes especializados que colaboran para resolver tareas complejas.
- **Sistema de Skills:** Arquitectura modular donde las funciones nuevas (ej. soporte para Signal) se añaden como modificaciones de código asistidas por IA.

Precios
- **Versión Gratuita:** El software es Open Source bajo licencia MIT. No tiene coste de licencia por uso.
- **Coste Operativo:** Requiere una suscripción a Claude Code o el uso de una API Key de Anthropic (pago por uso de tokens).

Perfil del usuario
- Desarrolladores y DevOps que buscan automatizar flujos de trabajo personales.
- Analistas de datos que requieren resúmenes periódicos de fuentes externas.
- Emprendedores y perfiles técnicos en sectores de consultoría o IT.

Nivel técnico requerido
- **Uso:** Bajo-Medio. Se interactúa mediante lenguaje natural a través de apps de mensajería.
- **Instalación/Configuración:** Medio-Alto. Requiere manejo de terminal (CLI), Git y entornos de contenedores.
- **Conocimientos necesarios:** Familiaridad con Node.js, Docker y gestión de claves API.

Ejemplos de uso profesional
- **Resumen de Ventas:** "Envía un resumen del pipeline de ventas cada mañana a las 9:00 (accediendo a mi carpeta local de datos)".
- **Control de Repositorios:** "Revisa el historial de Git cada viernes y actualiza el README si hay discrepancias".
- **Monitorización de Noticias:** "Busca noticias sobre IA en portales especializados cada lunes y envíame un briefing por Slack".

Uso y distribución
- **CLI:** Interfaz de línea de comandos principal mediante Claude Code.
- **Integración con Mensajería:** Disponible vía WhatsApp, Telegram, Slack y Discord.
- **Entorno Ejecución:** Servidor local o VPS compatible con contenedores.

Open source
Licencia MIT. El proyecto incentiva el fork y la personalización del código fuente en lugar de la configuración por menús.

Integraciones
- **Integración Nativa:** Dispone de una arquitectura de "Skills" que permite añadir servicios (Gmail, Slack, etc.) mediante comandos asistidos por IA.
- **API Propia:** Basado en Claude Agent SDK.
- **Local Models:** Soporte para modelos locales a través de Ollama mediante proxies compatibles con la API de Anthropic.

Notas finales
información legal, licencias , contratos
El software se distribuye "tal cual" bajo la licencia MIT, lo que exime a los autores de responsabilidad por el uso de la herramienta. La privacidad total depende de la configuración del usuario y del proveedor del modelo (Anthropic).

Para más información:
- Sitio web oficial
- Github
- Documentación

CONSEJOS DE IMPLANTACIÓN

Aplicación profesional
- **Tipos de empresa:** Startups de base tecnológica, agencias de desarrollo de software, consultoras IT y departamentos de ciberseguridad que gestionan datos sensibles.
- **Presupuesto:** Bajo en licencias (Open Source), medio en infraestructura y consumo de API. El gasto principal deriva del consumo de tokens de Anthropic (Claude) y el coste/hora del personal técnico para su despliegue inicial.
- **Puntos clave:** Automatización de flujos de trabajo mediante agentes autónomos en entornos estancos y seguros (Sandbox). Centralización de la operativa en aplicaciones de mensajería (WhatsApp, Slack, Discord).

Madurez digital requerida
- **Usuarios:** Nivel medio-bajo para el uso diario (interacción por chat), pero con mentalidad de "early adopter".
- **Equipo de implementación:** Nivel alto. Se requiere experiencia técnica sólida en entornos de contenedores y desarrollo backend.
- **Empresa:** Debe disponer de políticas de uso de IA claras y permitir la ejecución de Docker/contenedores en servidores locales o VPS controlados.

Plan orientativo de implantación
Pasos necesarios y estimaciones
- **Tiempo estimado de despliegue:** 1 a 2 semanas para una configuración estable y personalizada.
- **Fase 1: Evaluación (2-3 días):** Inventario de casos de uso (filtros de noticias, resúmenes de archivos, reportes) y definición de permisos de acceso a datos locales.
- **Fase 2: Infraestructura (1-2 días):** Configuración del entorno de ejecución (Docker o Apple Container), obtención de API Keys de Anthropic y configuración de pasarelas de mensajería (Bots en Telegram/Slack).
- **Fase 3: Implementación y Skills (3-5 días):** Despliegue del núcleo NanoClaw, configuración del aislamiento de grupos y desarrollo/ajuste de "Skills" específicas mediante Claude Code.
- **Fase 4: Piloto (1 semana):** Pruebas de ejecución en un entorno controlado por un equipo reducido para validar el comportamiento del agente y el consumo de tokens.

Necesidades de formación del equipo
- **Administradores:** Gestión de contenedores Docker, actualización de prompts de sistema y monitorización de costes de API.
- **Usuarios finales:** Instrucción en la redacción de prompts efectivos para interactuar con el agente y comprensión de las limitaciones del contexto (memoria del grupo).

Perfiles necesarios
- **Perfiles técnicos:** Ingeniero DevOps o Desarrollador Backend (Node.js) para la configuración y personalización del código.
- **Personal externo:** Opcionalmente, consultores en IA para el diseño de flujos de trabajo (Swarms) complejos.
- **Responsable de seguridad:** Para auditar los permisos de acceso de los contenedores a los sistemas de archivos locales.

Retorno de la inversión
- **Tiempos:** Reducción inmediata en tareas de recopilación de información y mantenimiento de documentación tras la fase de ajuste (2-4 semanas).
- **Cómo medirlo:** Comparativa de horas hombre dedicadas a tareas repetitivas (ej. resúmenes de informes) frente a la supervisión de los outputs del agente. Control de latencia en la ejecución de comandos automatizados.

Otros
- **Escalabilidad:** Al ser modular y basado en archivos de texto (CLAUDE.md) para la memoria, permite una escalabilidad horizontal sencilla replicando instancias para diferentes departamentos.
- **Privacidad Local:** Es posible apuntar el sistema hacia modelos locales mediante Ollama, eliminando la dependencia de nubes externas si la privacidad absoluta es el requisito principal, aunque con una degradación potencial en la capacidad de razonamiento frente a los modelos Claude 3.5.

PREGUNTAS FRECUENTES

¿Qué es NanoClaw y cuál es su arquitectura técnica?

NanoClaw es un asistente de IA de código abierto con una arquitectura minimalista y nativa para IA, diseñado para ejecutarse localmente. A diferencia de las plataformas monolíticas, utiliza un sistema de archivos reducido con aproximadamente 15 archivos fuente, conectando modelos de lenguaje avanzados con aplicaciones de mensajería cotidianas.

¿Qué utilidad profesional ofrece en comparación con otros asistentes?

Sirve para automatizar tareas complejas, ejecutar comandos de sistema y gestionar flujos de trabajo profesionales de forma autónoma. Su valor diferencial reside en la capacidad de realizar tareas integradas en el entorno del usuario (como leer repositorios localmente o enviar informes por Slack) manteniendo la privacidad de los datos.

¿Cuál es el coste de implementación de la herramienta?

El software es gratuito bajo licencia MIT y no conlleva costes de licencia. Sin embargo, existen costes operativos variables asociados al consumo de tokens de las API de modelos de lenguaje (principalmente Anthropic/Claude) o al uso de Claude Code. El gasto final depende directamente del volumen de actividad y consultas realizadas.

¿Es posible utilizar NanoClaw de forma gratuita sin dependencias de API de pago?

Sí, aunque está optimizado para Claude, NanoClaw admite el uso de modelos locales a través de Ollama mediante proxies compatibles con la API de Anthropic. Esto permite una ejecución 100% gratuita y sin salida de datos a la nube, siempre que el hardware local tenga la capacidad de cómputo necesaria.

¿Dónde se puede descargar el código fuente?

Al ser un proyecto Open Source, el código fuente completo, los archivos de configuración y las instrucciones de despliegue están disponibles públicamente en su repositorio de GitHub (qwibitai/nanoclaw).

¿Cómo garantiza la seguridad del sistema operativo al ejecutar comandos?

NanoClaw utiliza un sistema de seguridad por aislamiento real a través de contenedores Linux (Docker o Apple Container). Cada sesión del agente opera en un entorno estanco, lo que impide que las acciones de la IA o posibles errores del modelo afecten o comprometan el sistema de archivos principal o la integridad del equipo anfitrión.

¿Cumple con la normativa española y europea de privacidad?

Al ser una herramienta autohospedada, el cumplimiento normativo (como el RGPD) recae en el usuario final y en el proveedor del modelo elegido. NanoClaw facilita la privacidad al procesar los datos localmente y permitir el aislamiento de memorias por grupos de chat mediante archivos independientes (CLAUDE.md).

¿Qué nivel de conocimientos técnicos se requiere para su configuración?

El perfil técnico requerido es medio-alto para la fase de instalación. Es necesario tener experiencia previa en el manejo de interfaces de línea de comandos (CLI), gestión de contenedores con Docker, uso de Git y configuración de entornos Node.js. No cuenta con una interfaz gráfica de usuario para su despliegue.

¿Qué aplicaciones y servicios profesionales se pueden integrar?

Dispone de integraciones nativas con canales de comunicación como WhatsApp, Telegram, Slack, Discord y Gmail. Además, su arquitectura flexible de 'Skills' permite añadir nuevos servicios o modificar las funcionalidades existentes mediante programación asistida por la propia IA.

¿Cómo gestiona la persistencia de datos y la memoria?

La herramienta implementa un sistema de aislamiento por grupos donde cada hilo de conversación posee su propio sistema de archivos y memoria persistente. Esto asegura que la información de un proyecto o departamento no se mezcle con otros, permitiendo un control granular de la información compartida con el agente.

CONTRATOS Y CONDICIONES

Princiaples recomendaciones
- Evaluar el riesgo de terceros: Al ser una herramienta que actúa como puente, el cumplimiento no depende solo de NanoClaw, sino de la configuración que hagas de las API de Anthropic (Claude) o proveedores de mensajería (WhatsApp/Telegram).
- Configuración de retención en Anthropic: Si usas la API de Anthropic, asegúrate de revisar si tus datos se usan para entrenar sus modelos. Para empresas, se recomienda usar el acceso vía API que, por defecto, suele tener condiciones de privacidad más estrictas que la versión comercial de chat.
- Control de acceso a contenedores: Aunque la ejecución es aislada (Docker), debes monitorizar qué permisos otorgas al agente sobre el sistema de archivos local para evitar fugas de información confidencial hacia la IA.
- Acuerdo de Encargado de Tratamiento (DPA): Si tratas datos de clientes mediante esta herramienta, debes verificar que tienes un contrato de tratamiento de datos con el proveedor del modelo de lenguaje (Anthropic) y con el hosting si usas un VPS externo.

Ley de Inteligencia Artificial (AI Act)
- Clasificación de riesgo: Por su naturaleza de "Asistente de propósito general", se clasifica inicialmente como de riesgo bajo o mínimo, a menos que se use para fines críticos (recursos humanos, evaluación crediticia, etc.).
- Transparencia: Como empresa, estás obligado a informar a tus empleados o clientes si están interactuando con un sistema de IA generado por esta herramienta.
- Vigilancia humana: Al permitir que la IA ejecute comandos en contenedores, la Ley de IA exige que mantengas siempre el control y la capacidad de supervisar o detener las tareas automatizadas por el agente.

Privacidad y protección de datos
- Responsabilidades: Tu empresa actúa como Responsable del Tratamiento de los datos. NanoClaw, al ser software de código abierto ejecutado en tus servidores, es el medio técnico, pero la responsabilidad legal del uso es exclusivamente tuya.
- Ubicación de los datos: Si ejecutas NanoClaw en un servidor local en España, los datos residen en la UE. Sin embargo, el procesamiento del texto (tokens) ocurre en los servidores de Anthropic (generalmente en EE.UU.).
- Transferencia internacional: El uso de la API de Anthropic implica una transferencia internacional de datos. Debes verificar que la transferencia está amparada por las Cláusulas Contractuales Tipo o el Marco de Privacidad de Datos UE-EE.UU.
- Derechos ARCO: Tienes la ventaja de que, al gestionar tus propios archivos de memoria (CLAUDE.md), es más sencillo cumplir con las solicitudes de acceso, rectificación o supresión de los interesados.

Propiedad intelectual
- Propiedad de datos: Los datos de entrada (prompts) y los archivos de entrenamiento local siguen siendo propiedad de la empresa.
- Propiedad del resultado: Según la legislación española actual, las obras generadas íntegramente por IA sin intervención humana creativa no suelen ser objeto de propiedad intelectual (derechos de autor), aunque el software resultante de su uso sí puede estar protegido como secreto comercial o bajo contratos específicos.
- Licencia de software: NanoClaw usa la licencia MIT, lo que permite su uso comercial, modificación y distribución con muy pocas restricciones, siempre que se mantenga el aviso de copyright original.

Usos y prohibiciones
- Usos admitidos: Automatización de tareas administrativas, resúmenes de reuniones, gestión de repositorios de código y análisis de datos internos en entornos controlados.
- Usos prohibidos: No debe utilizarse para la toma de decisiones automatizadas que produzcan efectos jurídicos significativos sobre personas (según RGPD Art. 22) sin supervisión humana real. Está prohibido el uso para vigilancia masiva o extracción de datos personales de terceros de forma automatizada sin base legal.

Seguridad y certificaciones
- Seguridad: El aislamiento por contenedores (Docker/Apple Container) es una medida de seguridad técnica robusta que mitiga ataques de inyección de prompts que intenten acceder al sistema operativo base.
- Certificaciones: Al ser un proyecto de código abierto reciente, no cuenta con certificaciones tipo ISO 27001

o SOC2 de forma nativa. La responsabilidad de certificar el entorno de ejecución recae en el departamento de IT de tu empresa.

Otros
- Interconexión con apps de mensajería: El uso de WhatsApp o Telegram para enviar datos profesionales de clientes a través de un agente de IA puede vulnerar las políticas de uso de dichas plataformas y añadir riesgos de privacidad adicionales, ya que los datos pasan por los servidores de estas aplicaciones antes de llegar al usuario.

Fuentes consultada:
- Repositorio oficial de NanoClaw (Licencia y Código)
- Documentación técnica de NanoClaw
- Términos comerciales y de API de Anthropic
- Reglamento de Inteligencia Artificial de la UE
- Licencia MIT (Explicación)