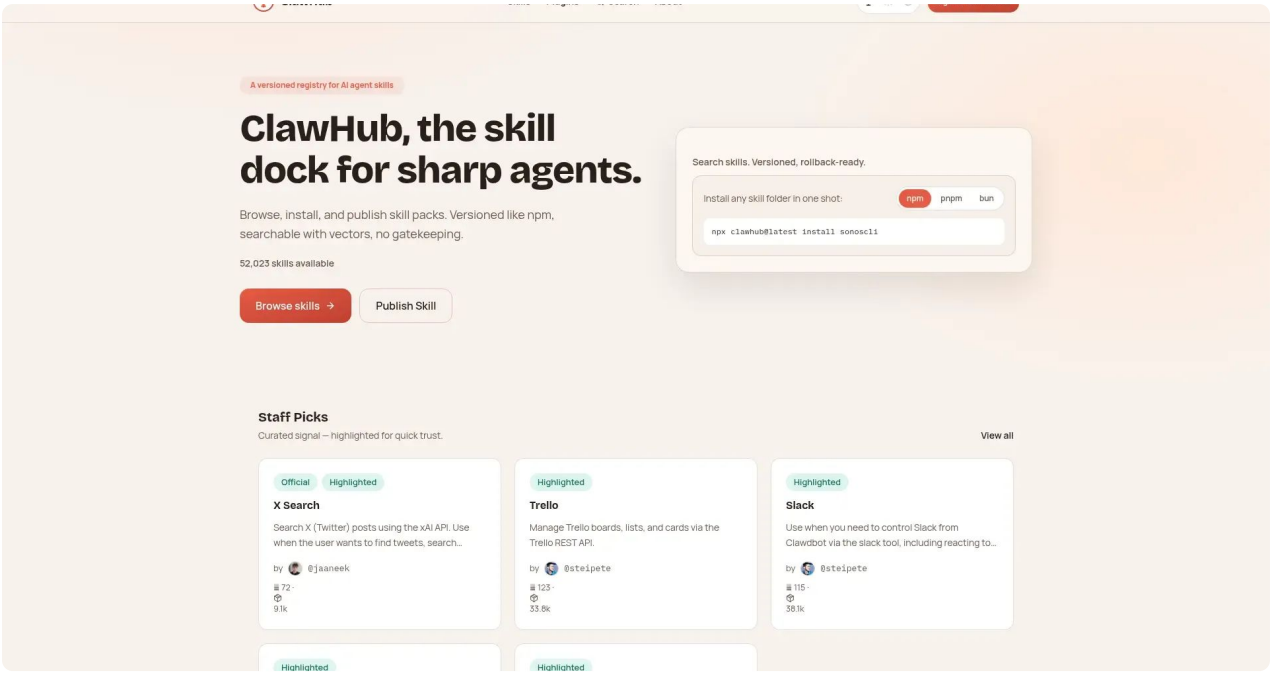

ClawHub.ai

Registro oficial de habilidades y plugins para el ecosistema OpenClaw, diseñado para desarrolladores y equipos de ingeniería que buscan expandir las capacidades de sus agentes de IA. Permite la automatización de tareas, integración con APIs y gestión de infraestructura mediante un repositorio centralizado y versionado. Es ideal para profesionales que operan con modelos locales y necesitan un sistema de extensibilidad basado en Markdown para desplegar funciones sin reescribir código.

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

Contenido del Dossier

INFORMACIÓN DE LA HERRAMIENTA

Qué y para quién es
ClawHub.ai es el registro oficial de habilidades (skills) y plugins para el ecosistema OpenClaw, un agente de IA de código abierto. Funciona de manera análoga a lo que representan npm para Node.js o PyPI para Python, pero aplicado a capacidades de agentes inteligentes. Está diseñado para desarrolladores y empresas que buscan expandir las funciones de sus agentes de IA (como automatización de tareas, integración con APIs de terceros o gestión de infraestructura) sin reescribir código desde cero. En el ámbito profesional, se dirige a equipos de ingeniería, DevOps y arquitectura de IA que necesitan un repositorio centralizado y versionado de funcionalidades listas para desplegar.

Principal ventaja profesional
Permite la extensibilidad inmediata de agentes de IA locales mediante un sistema basado en Markdown (SKILL.md), lo que facilita la auditoría, personalización y despliegue de nuevas capacidades sin necesidad de compilaciones complejas.

Para quién no es
No es para usuarios finales que buscan una aplicación SaaS de "clic y listo" sin conocimientos técnicos. Profesionales que prefieren entornos cerrados y propietarios (como GPTs de OpenAI exclusivamente) o que no tienen experiencia mínima con líneas de comandos (CLI) pueden encontrar la curva de aprendizaje o la gestión de la infraestructura propia innecesariamente compleja.

funcionalidades clave
- Registro público de más de 5.700 habilidades desarrolladas por la comunidad.
- Búsqueda semántica integrada basada en embeddings (vector search) para localizar herramientas por intención, no solo por palabras clave.
- Gestión de versiones mediante SemVer (Semantic Versioning) con registro de cambios (changelog).
- Sistema de instalación ligero mediante CLI que sincroniza archivos directamente en el espacio de trabajo local.
- Moderación comunitaria con sistema de reportes y ocultación automática de habilidades sospechosas.
- Soporte para metadatos, etiquetas y señales de uso (estrellas/descargas) para evaluar la fiabilidad de las habilidades.

Precios
- Versión gratuita: El acceso al registro, la descarga de habilidades y el uso de la CLI son gratuitos bajo el modelo de código abierto.
- Rango de precios: 0€ (Software libre).
- Publicación: Es gratuita, aunque requiere una cuenta de GitHub con una antigüedad mínima de una semana para evitar spam y abusos.

Perfil del usuario
- Empresas que operan con modelos de IA locales (Ollama, Llama) por razones de privacidad y cumplimiento.
- Departamentos de IT que automatizan flujos de trabajo internos (gestión de calendarios, backups, despliegues).
- Desarrolladores de aplicaciones que integran capacidades de razonamiento de LLMs con ejecución de herramientas bash o APIs externas.

Nivel técnico requerido
- Nivel técnico de uso: Medio (Manejo de consola/terminal y configuración de archivos .env o Markdown).
- Nivel técnico de instalación: Medio (Requiere Node.js y conocimiento de gestión de paquetes con npm/pnpm).
- Necesidades de soporte: Equipos de desarrollo o administración de sistemas para la configuración del Gateway de OpenClaw.
- Competencias necesarias: Familiaridad con el protocolo MCP (Model Context Protocol) y lenguajes de marcado como Markdown.

Ejemplos de uso profesional
- Automatización de procesos DevOps: Instalación de una skill para gestionar backups de bases de datos PostgreSQL mediante comandos de lenguaje natural.

- Soporte técnico automatizado: Integración de habilidades de búsqueda en documentación técnica para que el agente responda consultas en Slack o Discord.
- Gestión de infraestructura: Uso de skills para monitorizar servicios en la nube y ejecutar comandos bash de autoreparación ante alertas.

Uso y distribución
- Versión web: Portal de descubrimiento y exploración de habilidades en clawhub.ai.
- CLI: Herramienta de línea de comandos oficial instalable vía npm (npm i -g clawhub).
- Integraciones: Nativa con OpenClaw y compatible con Claude Code mediante el protocolo MCP.

Open source
El proyecto es de código abierto con licencias permisivas (MIT/Apache 2.0 según el componente), gestionado por la comunidad OpenClaw.

Integraciones
- Facilidad de integración: Low code para instalación de skills; Full code para creación de plugins complejos.
- Servidor MCP: Totalmente compatible con el Model Context Protocol para conectar las habilidades de ClawHub con otros clientes de IA como Claude Desktop.
- Integraciones nativas: Conexión con más de 50 canales (WhatsApp, Slack, Discord, Microsoft Teams, Telegram).

Notas finales
información legal, licencias , contratos
El uso del registro está sujeto a las condiciones de servicio de ClawHub.ai. Al ser un registro abierto donde los usuarios suben contenido, la responsabilidad de la seguridad recae en el usuario final. Se recomienda auditar el archivo SKILL.md antes de cada ejecución, especialmente tras incidentes de seguridad reportados en el pasado (como el ataque de cadena de suministro ClawHavoc).

Para más información:
- Sitio web oficial: https://clawhub.ai
- Documentación oficial: https://open-claw.bot/docs/es/tools/clawhub/
- Github: https://github.com/openclaw-community/openclaw-hub

CONSEJOS DE IMPLANTACIÓN

Este informe técnico detalla el protocolo de implantación y seguridad para **ClawHub.ai** en el ecosistema **OpenClaw (MCP)**. Debido a que esta herramienta otorga capacidades de ejecución de código y acceso al sistema a agentes de IA, su despliegue debe seguir estrictos criterios de seguridad para evitar incidentes como el ataque de cadena de suministro ClawHavoc.

Aplicación profesional
- **Tipos de empresa:** Equipos de ingeniería, departamentos de DevOps, Arquitectos de IA y empresas con políticas de privacidad estrictas que ejecutan LLMs locales (Ollama, Llama 3).
- **Presupuesto:** 0€ (Software libre). Requiere inversión en horas de preventa técnica y auditoría interna.
- **Puntos clave:** Centralización de habilidades via MCP (Model Context Protocol), extensibilidad inmediata mediante archivos Markdown y automatización de infraestructura mediante lenguaje natural.

Madurez digital requerida
- **Usuarios:** Desarrolladores o administradores de sistemas con capacidad para auditar scripts Bash/Python y manejar entornos Node.js.
- **Empresa:** Debe contar con una política de gestión de secretos y contenedores (Docker/Podman), así como protocolos de seguridad para IAs agénticas.

Plan orientativo de implantación
Pasos necesarios y estimaciones
- **Evaluación inicial (1-2 días):** Definición de "Trusted Boundaries". Decidir en qué máquina se ejecutará el Gateway de OpenClaw (se recomienda VPS aislado o Raspberry Pi, nunca el equipo principal).
- **Instalación y Configuración (1 día):** Despliegue de OpenClaw via CLI (npm i -g clawhub) y configuración del archivo openclaw.json.
- **Hardening de Seguridad (Fase Crítica):**
- Configurar el Gateway en modo loopback (127.0.0.1) para evitar exposición a internet.
- Implementar **Tailscale** para acceso remoto seguro sin abrir puertos públicos.
- Ejecutar openclaw security audit --deep para detectar vulnerabilidades iniciales.
- **Prueba de Concepto (1 semana):** Instalación de skills específicas (ej. búsqueda técnica o gestión de backups) y verificación en un entorno "sandbox".
- **Puesta en producción:** Despliegue en contenedor Docker con privilegios limitados (cap-drop ALL, read-only).

Necesidades de formación del equipo
- Capacitación en el protocolo **MCP** (Model Context Protocol) para entender cómo se comunican las habilidades con el modelo.
- Formación en **Prompt Injection Defense**: entender que las habilidades de ClawHub son "instrucciones Markdown" que pueden ser manipuladas por entradas maliciosas.

Perfiles necesarios
- **Ingeniero DevOps/SRE:** Para la configuración de la red segura y el despliegue de contenedores.
- **Auditor de Seguridad:** Imprescindible para revisar el archivo SKILL.md de cada plugin antes de su instalación profesional.
- **Desarrollador Backend:** Para la creación de habilidades personalizadas que conecten con APIs privadas de la empresa.

Retorno de la inversión (ROI)
- **Tiempos:** Reducción drástica en el tiempo de desarrollo de conectores de IA (de semanas a minutos mediante el uso de skills pre-existentes).
- **KPIs:** Número de tareas manuales automatizadas por el agente, reducción de errores en despliegues DevOps y latencia en la resolución de consultas técnicas internas.

Otros: Medidas de seguridad críticas tras ClawHavoc
- **Auditoría de Skills:** Tras detectarse más de 300 habilidades maliciosas en el registro, es obligatorio usar openclaw security audit --fix.
- **Aislamiento de Archivos:** Configurar fs: { workspaceOnly: true } en el archivo de configuración para que el agente no pueda salir de su carpeta asignada ni leer claves SSH o /etc/.

- **Human-in-the-loop:** Configurar ask: "always" para herramientas sensibles (shell, borrado de archivos), obligando a una aprobación humana antes de ejecutar cualquier comando detectado por la IA.
- **Redacción de logs:** Activar logging.redactSensitive: "tools" para evitar que las API Keys queden impresas en los archivos de registro de la sesión.

PREGUNTAS FRECUENTES

¿Qué es exactamente ClawHub.ai y cuál es su función en el ecosistema de IA?

ClawHub.ai es el registro central y oficial de habilidades (skills) y plugins diseñado específicamente para OpenClaw, un agente de IA de código abierto. Su funcionamiento es equivalente a gestores de paquetes como npm o PyPI, permitiendo a los profesionales localizar, versionar e instalar funcionalidades preconfiguradas para expandir las capacidades de razonamiento y ejecución de agentes inteligentes sin necesidad de desarrollar código desde cero.

¿Para qué sirve ClawHub.ai en un entorno empresarial?

Sirve para dotar a los agentes de IA locales de la capacidad de interactuar con el mundo real y herramientas técnicas. Permite automatizar flujos de trabajo de DevOps (como backups de bases de datos), gestionar infraestructura mediante comandos de lenguaje natural e integrar el agente con canales de comunicación corporativos como Slack, Microsoft Teams o Discord mediante el uso de habilidades ya testeadas por la comunidad.

¿Cuál es el coste de uso y publicación en la plataforma?

El acceso al registro, la descarga de habilidades y el uso de la herramienta de línea de comandos (CLI) son totalmente gratuitos bajo un modelo de software libre (0€). La publicación de habilidades también es gratuita, aunque exige como medida de seguridad activa que la cuenta de GitHub del colaborador tenga al menos una semana de antigüedad para mitigar el riesgo de spam.

¿Es ClawHub.ai de código abierto (Open Source)?

Sí, el proyecto forma parte del ecosistema OpenClaw y se gestiona de forma comunitaria bajo licencias permisivas como MIT y Apache 2.0. El código fuente de las herramientas y del registro es accesible para auditoría y contribución por parte de cualquier desarrollador.

¿Cómo se garantiza la seguridad ante posibles ataques de cadena de suministro?

ClawHub implementa un sistema de moderación comunitaria, reportes de usuarios y ocultación automática de entradas sospechosas. Sin embargo, al ser un registro abierto, la responsabilidad final recae en el profesional. Se recomienda encarecidamente auditar el archivo SKILL.md antes de su ejecución para verificar los comandos y permisos solicitados, especialmente tras incidentes históricos como ClawHavoc.

¿Qué normativa y protocolos de interoperabilidad sigue la tecnología?

La plataforma es totalmente compatible con el Model Context Protocol (MCP), un estándar de la industria que permite la interoperabilidad entre diferentes clientes de IA, como Claude Desktop, y las herramientas alojadas en ClawHub. Esto asegura que las habilidades no estén cautivas en un solo ecosistema y puedan ser utilizadas en diversos entornos profesionales.

¿Qué requisitos técnicos son necesarios para su instalación y uso?

A nivel de infraestructura, se requiere tener instalado Node.js y un gestor de paquetes (npm o pnpm). A nivel de competencia profesional, el usuario debe tener conocimientos medios en el manejo de terminal (CLI) y configuración de archivos de entorno (.env) o marcado (Markdown), ya que no es una herramienta orientada a usuarios finales sin perfil técnico.

¿Cómo aborda ClawHub la privacidad de los datos empresariales?

ClawHub facilita el uso de modelos de IA locales (como Llama u Ollama) al permitir que las habilidades se ejecuten directamente en la infraestructura del cliente. Al no requerir necesariamente el envío de datos a nubes propietarias para la ejecución de herramientas, se adapta a las necesidades de empresas que operan bajo estrictos marcos de cumplimiento y soberanía de datos.

¿Puedo descargar el código y las habilidades desde un repositorio central?

Sí, todas las herramientas y la lógica del registro son accesibles y gestionables a través de GitHub en la organización oficial de OpenClaw. La sincronización de archivos se realiza de forma transparente mediante la CLI de ClawHub, que descarga los activos necesarios directamente al espacio de trabajo local del desarrollador.

CONTRATOS Y CONDICIONES

Informe técnico descriptivo

Clasificación de la herramienta: Impacto legal Medio. El uso de repositorios de terceros de código abierto (estilo npm/PyPI) para ejecutar acciones en servidores o puestos de trabajo conlleva riesgos de seguridad y cumplimiento que deben ser mitigados por la empresa.

Principales recomendaciones
- Auditoría obligatoria de código: Al ser un registro donde cualquier usuario puede subir habilidades (skills), es imprescindible revisar el contenido del archivo SKILL.md y los scripts asociados antes de su ejecución para evitar ataques de cadena de suministro (como el incidente documentado ClawHavoc).
- Entornos aislados (Sandboxing): Se recomienda ejecutar los agentes que utilicen estas skills en contenedores o máquinas virtuales con privilegios limitados para evitar que una skill maliciosa acceda a archivos sensibles del sistema.
- Gestión de Secretos: No incluir claves personales, tokens de API o credenciales en los archivos de configuración de las skills. Usar variables de entorno gestionadas de forma segura.
- Verificación de Versiones: Fijar las versiones de las skills utilizadas en producción para evitar actualizaciones automáticas que puedan introducir cambios no deseados o código malicioso.

Ley de Inteligencia Artificial (AI Act)
- Clasificación de riesgo: El uso de ClawHub para automatizar tareas profesionales se clasifica generalmente como de "riesgo bajo" o "no clasificado", a menos que las habilidades específicas se utilicen para propósitos críticos (infraestructuras, recursos humanos, educación o vigilancia biométrica), en cuyo caso el riesgo aumentaría a "alto".
- Transparencia: Las empresas deben informar a los empleados o clientes si están interactuando con un agente de IA que utiliza estas automatizaciones.
- Responsabilidad del proveedor: Bajo el AI Act, la empresa española que integra estas habilidades asume la responsabilidad de supervisión del sistema de IA.

Privacidad y protección de datos
- Responsabilidades: La empresa usuaria actúa como Responsable del Tratamiento. ClawHub.ai es un mero repositorio (proveedor de infraestructura de software) y no accede a los datos que el agente procesa localmente.
- Ubicación de los datos: El registro reside en servidores externos, pero la ejecución de las habilidades y el procesamiento de los datos de la empresa se realiza de forma local o en el cloud privado de la empresa, lo que facilita el cumplimiento del RGPD.
- Transferencia internacional: No existe transferencia de datos personales a favor de ClawHub durante el uso técnico del CLI, salvo los metadatos de conexión técnica. No obstante, si una "skill" de terceros conecta con una API fuera de la UE, la empresa debe realizar una Evaluación de Impacto (EIPD).
- Derechos ARCO: La empresa debe garantizar que sus agentes de IA permitan el ejercicio de derechos (acceso, rectificación) sobre los datos que procesen mediante estas habilidades.

Propiedad intelectual
- Propiedad de datos: Los datos de entrada y los resultados generados por el agente pertenecen a la empresa usuaria.
- Propiedad de la herramienta: El software del registro y la CLI están protegidos mayoritariamente bajo licencias de código abierto (MIT / Apache 2.0).
- Propiedad del resultado: Los scripts y habilidades (skills) subidos por la comunidad mantienen la propiedad intelectual de sus autores originales, pero se distribuyen bajo licencias que permiten su uso profesional y modificación.

Usos y prohibiciones
- Usos prohibidos: Está prohibido usar ClawHub para crear habilidades destinadas a evasión de seguridad (CAPTCHA bypass), fraude, suplantación de identidad (clonación de voz/cara sin consentimiento), spam masivo o vigilancia invasiva.
- Usos admitidos: Automatización de flujos de trabajo internos, gestión de infraestructura (DevOps), integración de herramientas de soporte técnico y consultas de documentación mediante protocolos estándar (MCP).

Seguridad y certificaciones
- Seguridad: La plataforma utiliza un sistema de moderación comunitaria y reporte de habilidades sospechosas. Sin embargo, no ofrece una garantía de "zero-malware".
- Certificaciones: Al ser un proyecto de comunidad y código abierto, ClawHub no presenta certificaciones ISO 27001 o SOC2 de forma nativa. La responsabilidad de la certificación de seguridad recae sobre el entorno donde la empresa española despliegue la herramienta.

Otros
- Incidente ClawHavoc: Es importante recalcar que en febrero de 2026 se detectaron más de 300 habilidades maliciosas en el registro. Esto refuerza la necesidad de utilizar únicamente habilidades verificadas o con alta reputación (estrellas/descargas) y antigüedad.

Fuentes consultada:
- Contratos: https://open-claw.org/terms-of-service
- Condiciones: https://www.clawhub.ai/about
- Licencias: https://github.com/openclaw/clawhub/blob/main/LICENSE
- Documentación: https://open-claw.bot/docs/es/tools/clawhub/