

openclaw / openclaw-windows-node Public

Code Issues 29 Pull requests 43 Actions Security and quality Insights

master 165 Branches 36 Tags

Go to file Code

**About**  
Windows companion suite for OpenClaw - System Tray app, Shared library, Node, and PowerToys Command Palette extension  
Readme  
MIT license  
Security policy  
Activity  
Custom properties  
1.6k stars  
9 watching  
182 forks  
Report repository

**Releases** 28  
v0.6.3 (Latest)  
yesterday  
+ 27 releases

**Packages**  
No packages published

**Contributors** 26

File	Description	Last Commit
.agents/skills/autoreview	Fall back to Copilot for autoreview when Codex is unavailabl...	4 hours ago
.config	Bump gitversion.tool from 6.4.0 to 6.7.0 (#622)	4 hours ago
.github	build(deps): bump githubhigh-aw-actions from 0.74.4 to 0.77...	4 hours ago
docs	Consolidate setup UI into tray host (#690)	7 hours ago
scripts	Consolidate setup UI into tray host (#690)	7 hours ago
src	Use Arm64-aware wording when WSL reports virtualization ...	3 hours ago
tests	Use Arm64-aware wording when WSL reports virtualization ...	3 hours ago
tools	Make Inno the primary installer path	last week
.editorconfig	eng: enforce warning-clean builds	last week
.gitattributes	Add agentic workflow repo-assist	3 months ago
.gitignore	Add local Inno installer helper	last week
AGENTS.md	docs(agents): note --no-restore first-run golcha in test valida...	3 weeks ago
DEVELOPMENT.md	Address PR review feedback and add quoting proof	last week
GitVersion.yml	Preserve alpha release tags in GitVersion	last week
LICENSE	Initial commit: Moltbot Windows Hub monorepo	5 months ago
NuGet.Config	eng: handle repo-assist easy wins	2 months ago
README.md	docs: point setup at stable Windows Hub downloads	2 days ago
SECURITY.md	chore: add repo security workflows	last week

# OpenClaw Windows Node

*Suite nativa de acompañamiento para el asistente de IA OpenClaw que permite interactuar directamente con el sistema operativo Windows. Esta herramienta facilita a desarrolladores, administradores de sistemas y entusiastas de la productividad la ejecución de comandos PowerShell, capturas de pantalla y automatización de procesos locales. Ideal para profesionales técnicos que buscan un control total sobre su entorno de trabajo mediante agentes de IA locales con soberanía de datos absoluta.*

[Visitar Sitio Oficial](#) [Preguntar a ChatGPT](#) [Preguntar a Claude](#) [Preguntar a Grok](#)

## Contenido del Dossier

- [Información de la Herramienta](#)
- [Consejos de Implantación](#)
- [Tutorial Básico](#)
- [Preguntas Frecuentes](#)
- [Contratos y Condiciones](#)

## INFORMACIÓN DE LA HERRAMIENTA

Qué y para quién es

OpenClaw Windows Node (conocido internamente como "Molty") es la suite de acompañamiento nativa de **OpenClaw**, un asistente de IA personal de código abierto diseñado para ejecutarse localmente. Esta herramienta transforma un PC con Windows en un "nodo" activo que permite al asistente de IA no solo responder preguntas, sino **interactuar directamente con el sistema operativo** (capturar pantalla, usar la cámara, ejecutar comandos de PowerShell o mostrar notificaciones).

Está dirigido a **profesionales técnicos, desarrolladores y entusiastas de la productividad** en España que buscan un asistente de IA con control total sobre su entorno de trabajo, priorizando la ejecución local y la soberanía de los datos.

Principal ventaja profesional

En mi opinión profesional, la razón definitiva para elegir esta herramienta es su **capacidad de "Node Mode"**. A diferencia de otros asistentes que viven solo en un chat, este permite que la IA ejecute tareas reales en tu máquina (como automatizar procesos mediante scripts o monitorizar el estado del sistema) de forma segura y supervisada, integrándose perfectamente en el flujo de trabajo de Windows a través de la bandeja del sistema y PowerToys.

Para quién no es

Tras probar la lógica de configuración, considero que **no es para usuarios finales sin conocimientos técnicos** o perfiles de administración que busquen una solución "clic y listo". Aquellos que prefieran asistentes en la nube tipo SaaS (como ChatGPT Plus o Copilot estándar) encontrarán la configuración de nodos, la gestión de tokens y la aprobación de dispositivos demasiado farragosa para un uso casual.

funcionalidades clave

- **Node Mode (Agent Control)**: Permite que el asistente OpenClaw ejecute comandos en el PC (notificaciones, ejecución de scripts, capturas de pantalla).
- **Integración con PowerToys**: Extensión para la Command Palette de Windows que permite lanzar comandos de la IA rápidamente (Win+Alt+Space).
- **Molty Tray App**: Aplicación en la bandeja del sistema con diseño Windows 11 para monitorizar sesiones, canales (Telegram/WhatsApp) y costos de proveedores de IA en tiempo real.
- **Embedded Web Chat**: Ventana de chat integrada basada en WebView2 para interactuar con la IA sin abrir el navegador.
- **Protocolo de Seguridad MXC**: Integración profunda con Windows para la ejecución contenida y segura de comandos.
- **Deep Links**: Soporte para el esquema openclaw://, permitiendo automatizaciones desde scripts externos o navegadores.

Precios

La herramienta es **Open Source (Gratuita)** bajo licencia MIT, aunque su uso profesional depende de los modelos de IA que conectes.

- **Versión gratuita**: Completa y sin limitaciones de software. Al ser código abierto, puedes auditarla y modificarla.
- **Gastos operativos**: El coste dependerá de las API de los modelos de lenguaje (OpenAI, Anthropic, etc.) que configures en el Gateway central de OpenClaw.

Perfil del usuario

- **Desarrolladores de Software**: Para automatizar flujos de trabajo locales y depuración asistida por IA.
- **Administradores de Sistemas**: Para monitorizar infraestructuras desde un panel centralizado con notificaciones nativas en Windows.
- **Profesionales de Ciberseguridad**: Que requieran probar automatizaciones locales en entornos controlados.

Nivel técnico requerido

- **Para su uso**: Medio. Requiere familiaridad con el concepto de agentes de IA y gestión de tokens.
- **Para su instalación**: Alto. Requiere conocimientos de terminal (PowerShell), instalación de SDKs (.NET 10) y configuración de archivos JSON para políticas de seguridad.
- **Competencias necesarias**: Manejo de CLI, comprensión de WebSockets y gestión de servicios en

Windows.

Ejemplos de uso profesional

- **Automatización de reportes:** Indicar a la IA que capture una ventana específica de una aplicación de análisis y la envíe por Telegram como reporte diario.
- **Gestión de incidencias:** Crear notificaciones persistentes en Windows (Toast Notifications) que se disparen ante eventos específicos detectados por el asistente en otros canales de comunicación.
- **Control de flujos DevSecOps:** Ejecutar scripts de validación local de código mediante el comando `system.run` tras recibir una aprobación manual o automática.

Uso y distribución

- **Versión web:** Accesible a través del Dashboard central del Gateway.
- **Versión escritorio:** Aplicación nativa WinUI 3 para Windows 10/11.
- **Extensiones:** Integración nativa con PowerToys Command Palette.
- **CLI:** Herramienta de línea de comandos openclaw para gestión avanzada.

Open source

El proyecto es totalmente open source y se encuentra alojado en GitHub bajo la organización openclaw.

Integraciones

- **Facilidad de integración:** Nivel medio/alto (requiere configuración manual de políticas de ejecución).
- **API propia:** Utiliza un protocolo de Gateway basado en WebSockets.
- **Canales nativos:** Integración directa para gestionar estados de WhatsApp y Telegram desde el PC.

Notas finales

Veredicto técnico

Como profesional, valoro enormemente la **robustez técnica** de esta herramienta. No es un juguete; es una infraestructura seria de control para agentes de IA. **Vale totalmente la pena para empresas y perfiles técnicos** que quieran construir su propio ecosistema de productividad sin depender de las limitaciones impuestas por los grandes proveedores de nube. Su integración con el ecosistema de desarrollo de Microsoft (WinUI 3, .NET, PowerToys) la posiciona como la mejor suite de acompañamiento para IA en Windows a día de hoy.

información legal, licencias , contratos

- **Licencia:** MIT (permite uso comercial, modificación y distribución).
- **Propiedad Intelectual:** Los datos y la lógica de ejecución permanecen en el control del usuario (Self-hosted).

Otros

Quiero destacar que, aunque el proyecto ha evolucionado desde nombres como "Moltbot", su madurez actual en 2026 lo hace compatible con infraestructuras modernas de Windows, incluyendo soporte nativo para arquitectura ARM64.

Fuentes consultadas:

- [Sitio web oficial](#)
- [Github - Repositorio Principal](#)
- [Github - Windows Node](#)
- [Microsoft Windows Developer Blog](#)

## CONSEJOS DE IMPLANTACIÓN

### Aplicación profesional

Según mi experiencia, es necesario entender que esta herramienta no es un software de oficina convencional, sino una capa de infraestructura para automatización avanzada. El tipo de empresa que mejor puede aprovechar OpenClaw es aquella que cuenta con departamentos de desarrollo (DevOps) o equipos de ciberseguridad que gestionan datos sensibles y no pueden permitirse enviar telemetría de sus sistemas operativos a nubes de terceros. En mi opinión profesional, el presupuesto necesario es mínimo en cuanto a licencias (0€ al ser MIT), pero se requiere una inversión significativa en horas de ingeniería para la puesta a punto. Lo que más me gusta es que permite cerrar el círculo de la soberanía digital: controlas el hardware, el modelo (vía servicios tipo Ollama o LocalAI) y ahora, con este nodo, la ejecución en el sistema.

### Madurez digital requerida

- **Usuarios y equipo:** Se requiere un dominio avanzado de la administración de sistemas Windows. El equipo debe estar familiarizado con el uso de APIs, protocolos de comunicación como WebSockets y la gestión de permisos de ejecución en entornos corporativos. No es apto para entornos con baja competencia digital donde los usuarios dependen exclusivamente de interfaces gráficas simplificadas.

- **Empresa y departamentos:** La organización debe contar con una política clara de gobernanza de datos y ciberseguridad, ya que otorgar a una IA la capacidad de ejecutar comandos de PowerShell y capturar pantalla implica riesgos si no se gestiona bajo los protocolos MXC que ofrece la herramienta.

### Plan orientativo de implantación

#### Pasos necesarios y estimaciones

- **Tiempos estimados de despliegue:** Entre 2 y 4 semanas para un despliegue estable en un entorno profesional controlado.

- **Evaluación inicial y recursos:** Auditoría de los flujos de trabajo que se pretenden automatizar. Es vital verificar que las máquinas cumplen con los requisitos de .NET 10 y que no existen bloqueos de red para el Gateway interno.

- **Implantación inicial y piloto:** Configuración de un Gateway centralizado y despliegue del nodo Molty en un grupo reducido de desarrolladores "beta testers". En esta fase se deben definir las "Políticas de Seguridad de Nodo" para limitar qué comandos puede ejecutar la IA (whitelist).

- **Formación y capacitación:** Sesiones técnicas enfocadas en la sintaxis de los Deep Links y el uso productivo de la integración con PowerToys para activar la IA sin fricción.

- **Seguimiento y feedback:** Revisión periódica de los logs de ejecución para ajustar los prompts del sistema y evitar falsos positivos en la ejecución de scripts.

### Necesidades de formación del equipo

Es imprescindible formar al equipo en ingeniería de prompts aplicada a la automatización de sistemas, así como en la monitorización de costes de tokens si se utilizan modelos propietarios. Al usarlo te das cuenta de que la mayor curva de aprendizaje no está en la instalación, sino en saber estructurar peticiones para que la IA interactúe con el SO de forma predecible.

### Perfiles necesarios

- **Perfiles técnicos necesarios:** Administrador de Sistemas Windows, Desarrollador .NET (para posibles extensiones) y Experto en Seguridad/DevSecOps.

- **Personal externo recomendado:** Consultor en implementación de IA local para la configuración óptima de los modelos de lenguaje que alimentarán al nodo.

### Retorno de la inversión (ROI)

- **Tiempo:** A partir del tercer mes se observa una reducción en el tiempo dedicado a tareas repetitivas de mantenimiento y reporte.

- **Cómo medirlo, KPIs:** Reducción del tiempo de ejecución de scripts manuales (MTTR), número de automatizaciones activas ejecutadas por nodos sin intervención humana y ahorro en licencias de software de automatización propietario (RPA).

### Otros

Mi experiencia en implantaciones me lleva a pensar que el mayor desafío es la gestión de las notificaciones y los permisos de usuario (UAC) en Windows. Es fundamental configurar correctamente el protocolo MXC para que el nodo no sea bloqueado por soluciones antivirus (EDR/AV) agresivas, que podrían interpretar la

captura de pantalla y ejecución de scripts como comportamiento sospechoso. La integración con la bandeja del sistema estilo Windows 11 facilita la adopción, ya que se siente como una herramienta nativa del sistema y no como un "parche" externo.

## TUTORIAL BÁSICO

### Instalación

La instalación de OpenClaw varía según el sistema operativo, pero la vía más estable y recomendada actualmente es el uso del script oficial o la aplicación nativa para Windows.

- **Windows (Recomendado):** Descarga e instala **OpenClaw Companion** (vía Hub o el instalador .exe nativo). Esto provisiona automáticamente una instancia de WSL2 (Windows Subsystem for Linux), que es el entorno más estable para el Gateway.
- **Windows (PowerShell):** Si prefieres la terminal, usa `iwr -useb https://openclaw.ai/install.ps1 | iex`.
- **macOS / Linux:** Utiliza el comando `curl -fsSL https://openclaw.ai/install.sh | bash`.
- **Configuración inicial:** Tras la instalación, ejecuta `openclaw onboard --install-daemon`. Este asistente te guiará para configurar tu proveedor de IA (Anthropic, OpenAI, etc.) y las claves de API.
- **Requisitos de Node:** Asegúrate de tener **Node 24** (recomendado) o al menos la versión 22.19+. Si instalas desde el código fuente, es obligatorio el uso de `pnpm`.

### Uso en el día a día

- **Control Central:** Accede a la interfaz de usuario basada en web con el comando `openclaw dashboard`. Es la forma más rápida de interactuar con el asistente y ver el estado del sistema.
- **Gestión de Canales:** OpenClaw brilla por su capacidad multicanal. Puedes conectar tu asistente a WhatsApp, Telegram o Discord usando `openclaw channels login`. Según mi experiencia, Telegram es el canal más sencillo de configurar inicialmente solo con un bot token.
- **Estado del Gateway:** Si el asistente no responde, lo primero es verificar el motor con `openclaw gateway status`. El Gateway debe estar escuchando por defecto en el puerto 18789.
- **Persistencia en Linux:** Si usas Linux o WSL2, es vital habilitar el "lingering" para que el servicio no se detenga al cerrar la sesión: `sudo loginctl enable-linger $USER`.

### Trucos de experto

- **Node Mode en Windows:** Activa el "Node Mode" en la configuración del Windows Hub para que el agente de IA pueda ejecutar comandos nativos como capturas de pantalla (`screen.snapshot`), notificaciones de sistema o incluso ejecutar scripts locales mediante `system.run`.
- **Aislamiento de Configuración:** Lo que más me gusta es su estrategia de "Tailoring". Mantén siempre tus personalizaciones (prompts, memorias y habilidades) en `~/.openclaw/workspace`. Mi recomendación profesional es convertir esa carpeta en un repositorio Git privado para versionar la evolución de la "personalidad" de tu asistente sin riesgo a perderlo en actualizaciones.
- **Aprobación de dispositivos:** Cuando conectes una nueva interfaz (como el Windows Companion), el Gateway solicitará aprobación. Usa `openclaw devices list` y `openclaw devices approve <id>` para autorizar el emparejamiento. Es una capa de seguridad crítica.
- **Modo MCP:** Puedes usar Windows Hub como un servidor MCP local para clientes como Claude Desktop o Cursor, permitiéndoles usar capacidades de Windows sin necesidad de tener el Gateway de OpenClaw corriendo permanentemente.

### Posibles problemas/incidencias

- **Error en Sharp (npm):** Al instalar globalmente en Linux/macOS, a veces la librería sharp falla. Se soluciona forzando la compilación local con: `SHARP_IGNORE_GLOBAL_LIBVIPS=1 npm install -g openclaw@latest`.
- **Comandos bloqueados:** Los comandos sensibles (cámara, micrófono, ejecución de sistema) requieren una lista blanca explícita en `openclaw.json`. Si un comando falla con un error de permisos, revisa la sección `gateway.nodes.allowCommands`.
- **Icono de bandeja desaparecido:** En Windows, si el proceso `OpenClaw.Tray.WinUI.exe` está activo pero no ves el icono, suele estar oculto en el menú desplegable de la barra de tareas o requiere ser anclado manualmente.
- **Incompatibilidad de red en WSL2:** Si necesitas acceder al Gateway de WSL desde otro dispositivo de la red local, recuerda que WSL tiene una IP virtual propia; necesitarás configurar un portproxy mediante `netsh` en Windows.

### Otros

- **Seguridad de credenciales:** OpenClaw almacena los tokens de canales en `~/.openclaw/credentials/`. Ten especial cuidado con la carpeta `whatsapp` si compartes el equipo, ya que los `creds.json` permiten el acceso directo a la sesión.

- **Diagnóstico rápido:** Si algo se comporta de forma errática, el comando `openclaw doctor` es tu mejor aliado; analiza la configuración, versiones y conectividad buscando fallos comunes.

## PREGUNTAS FRECUENTES

---

### ¿Qué es OpenClaw Windows Node (Molty)?

Es una suite de acompañamiento nativa de código abierto diseñada para convertir un PC con Windows en un nodo activo de inteligencia artificial. A diferencia de los chatbots convencionales, esta herramienta permite que la IA interactúe directamente con el sistema operativo, ejecutando comandos de PowerShell, capturando pantalla o gestionando notificaciones nativas.

### ¿Para qué sirve en un entorno profesional?

Sirve para automatizar flujos de trabajo locales y tareas de administración de sistemas mediante agentes de IA. Permite la monitorización de infraestructura, la ejecución de scripts de validación de código y la integración de la IA en la bandeja del sistema de Windows para un acceso rápido a tareas de productividad técnica.

### ¿Es open source y puedo descargarlo de GitHub?

Sí, el proyecto es totalmente de código abierto bajo la licencia MIT. El código fuente y los binarios están disponibles de forma pública en los repositorios de la organización OpenClaw en GitHub, lo que permite su auditoría técnica y modificación según las necesidades del usuario.

### ¿Cuánto cuesta utilizar esta tecnología?

El software es gratuito y no tiene limitaciones de uso. No obstante, el usuario debe asumir los gastos operativos derivados del consumo de tokens de las API de los modelos de lenguaje (como OpenAI o Anthropic) que decida conectar al nodo para procesar las peticiones de IA.

### ¿Cómo afronta la privacidad y la soberanía de los datos?

OpenClaw prioriza la ejecución local y el autocontrol. Al ser una solución autohospedada, la lógica de ejecución y los datos permanecen bajo el control del profesional o la empresa, evitando la dependencia total de infraestructuras SaaS de terceros y ofreciendo un entorno de trabajo privado.

### ¿Es una tecnología segura para uso corporativo?

La herramienta utiliza el protocolo de seguridad MXC para garantizar una ejecución de comandos contenida y segura dentro de Windows. Sin embargo, debido a su capacidad para ejecutar scripts del sistema, requiere que el administrador configure manualmente políticas de ejecución y archivos JSON de seguridad.

### ¿Qué nivel técnico se requiere para su implementación?

El nivel técnico requerido es alto para la instalación y medio para el uso diario. El profesional debe estar familiarizado con el uso de terminales (PowerShell), la gestión de servicios de Windows, la configuración de WebSockets y la instalación de SDKs específicos como .NET 10.

### ¿Cumple con la normativa española de protección de datos?

Al ser una herramienta de código abierto y ejecución local (self-hosted), facilita el cumplimiento del RGPD y otras normativas españolas, ya que el control del tratamiento de los datos recae sobre el usuario o la organización que lo despliega, permitiendo auditorías de código completas.

### ¿Se integra con otras herramientas de Windows?

Sí, ofrece una integración nativa con PowerToys mediante una extensión para la Command Palette (Win+Alt+Space). También utiliza WinUI 3 para su interfaz de usuario en la bandeja del sistema, es compatible con el esquema de enlaces profundos 'openclaw://' y soporta arquitecturas modernas como ARM64.

## CONTRATOS Y CONDICIONES

### Opinión inicial

Tras verificar los repositorios oficiales y la arquitectura técnica de OpenClaw Windows Node (Molty), mi opinión profesional es que nos encontramos ante una herramienta de **impacto legal alto** para una empresa española. Aunque el software sea de código abierto (Open Source), su capacidad para ejecutar comandos de PowerShell, capturar pantalla y acceder a la cámara del sistema operativo implica un riesgo crítico de seguridad y privacidad si no se supervisa. Desde el punto de vista de cumplimiento, el uso de la licencia MIT facilita la adopción empresarial sin costes de royalties, pero traslada toda la responsabilidad del cumplimiento del RGPD y la seguridad a la empresa que lo despliega, ya que no existe un contrato de servicios (SLA) ni una entidad jurídica que responda por fallos en el software.

### Principales recomendaciones

- Realizar una Evaluación de Impacto en la Protección de Datos (EIPD) antes de desplegarlo, dado que la herramienta puede monitorizar la actividad del empleado mediante capturas de pantalla y acceso a cámara.
- Configurar estrictamente los archivos JSON de políticas de seguridad para limitar qué comandos de PowerShell puede ejecutar el nodo, evitando el acceso a directorios con información sensible.
- Desactivar las funciones de captura de pantalla y cámara si no son estrictamente necesarias para la función laboral, siguiendo el principio de minimización de datos del RGPD.
- Asegurar que la conexión entre el nodo de Windows y el Gateway de OpenClaw se realice mediante protocolos cifrados (TLS) y dentro de una red privada o VPN corporativa.
- Designar un responsable técnico que audite los logs de ejecución de comandos que genera la herramienta localmente.

### Ley de Inteligencia Artificial (AI Act)

Al ser una herramienta que permite la "vigilancia" o monitorización del comportamiento de los trabajadores (mediante capturas de pantalla o seguimiento de actividad para la IA), su uso en el entorno laboral en España podría clasificarse como de **Alto Riesgo** según el Reglamento de IA de la UE. Esto obligaría a la empresa a garantizar la transparencia hacia los empleados, asegurando que estos conocen cuándo y cómo está actuando la IA en sus terminales locales.

### Privacidad y protección de datos

- **Responsabilidades:** La empresa española que instala el nodo actúa como Responsable del Tratamiento. Al ejecutarse localmente, OpenClaw no "recibe" los datos en sus servidores, pero la responsabilidad de la seguridad de los datos procesados por la IA recae totalmente en la empresa usuaria.
- **Ubicación de los datos:** Los datos se procesan localmente en el nodo Windows. Sin embargo, si se configuran APIs externas (como OpenAI o Anthropic) para procesar las peticiones, los datos saldrán del terminal.
- **Transferencia internacional:** Si la empresa configura el nodo para usar modelos de lenguaje de proveedores en EE.UU. (fuera del marco Data Privacy Framework si no están certificados), se estarían realizando transferencias internacionales de datos que requieren cláusulas contractuales tipo.
- **Derechos ARCO:** La empresa debe garantizar que el empleado puede solicitar el acceso o eliminación de los logs de actividad generados por el nodo en su PC local.

### Propiedad intelectual

- **Propiedad de datos:** Según la licencia MIT y la naturaleza self-hosted, la empresa mantiene la total propiedad de los datos de entrada y del contexto del sistema capturado.
- **Propiedad del resultado:** Al ser un software de código abierto, los scripts o resultados generados por el asistente en el PC pertenecen a la empresa usuario, no existiendo reclamaciones de propiedad intelectual por parte de los desarrolladores del software (OpenClaw).

### Usos y prohibiciones

- **Usos admitidos:** Automatización de flujos de trabajo técnicos, gestión de notificaciones de sistema, soporte en depuración de código y tareas administrativas autorizadas por el IT de la empresa.
- **Usos prohibidos:** No debe utilizarse para la monitorización encubierta de empleados (spyware), ni para el tratamiento de datos de categorías especiales (salud, religión, biometría) sin un consentimiento explícito y una base legal reforzada.

### Seguridad y certificaciones

- **Seguridad:** El protocolo MXC (Matrix-based) ofrece una capa de seguridad para la ejecución de comandos, pero la seguridad final depende de la configuración del entorno Windows (.NET 10) y de las políticas de ejecución de scripts de la empresa.
- **Certificaciones:** Tras revisar la documentación, la herramienta no cuenta con certificaciones tipo ISO 27001 o SOC2 de serie, al ser un proyecto comunitario. La empresa debe integrarlo en su propio marco de certificación.

Otros

Es fundamental destacar que la suite Molty utiliza WebView2 para el chat integrado, lo que significa que hereda las políticas de seguridad del navegador Microsoft Edge instalado en el sistema. Cualquier vulnerabilidad en el motor del navegador podría afectar directamente a la seguridad del nodo de IA.

Fuentes consultadas:

- [Sitio web oficial openclaw.ai](#)
- [Github - Repositorio Principal OpenClaw](#)
- [Github - Licencia MIT OpenClaw Windows Node](#)
- [Condiciones de uso y seguridad técnica](#)

#### Para más información y herramientas:

Explora look4.tools para descubrir las mejores soluciones tecnológicas del mercado.

[Inicio](#) [Todas las herramientas](#) [Categorías](#)

Este documento ofrece recomendaciones generadas mediante análisis humano y sistemas de IA automatizados. La información tiene carácter meramente informativo y no constituye asesoramiento legal, profesional ni garantía de resultados. Las marcas, logotipos y nombres comerciales pertenecen a sus respectivos propietarios y se utilizan únicamente con fines identificativos.