→ OTHERWAY LABS

GUÍA COMPLETA 2026

TU ESTRATEGIA DE AGENTES IA: NEMOCLAW

→ Qué es, cómo funciona y cómo usarlo en tu empresa
→ Instalación paso a paso + casos de uso reales

OpenClaw es el sistema operativo de los agentes de IA.
NemoClaw es la capa de seguridad que lo hace apto para empresas.
Esta guía te explica todo lo que necesitas saber para empezar.

→ CONTEXTO

EL MOMENTO MÁS IMPORTANTE PARA TU EMPRESA EN LA ÚLTIMA DÉCADA

El 16 de marzo de 2026, Jensen Huang, CEO de NVIDIA, subió al escenario del GTC en San José, California, frente a más de 30,000 personas de 190 países. En un punto del discurso, hizo una pregunta directa a los CEOs, directivos y líderes tecnológicos presentes:

> "Para los CEOs, la pregunta es: ¿cuál es su estrategia de OpenClaw? La necesitamos. Todos tuvimos una estrategia de Linux. Todos necesitamos una estrategia de HTML, que inició el internet. Todos necesitamos una estrategia de Kubernetes, que hizo posible el cloud. Hoy, cada empresa en el mundo necesita una estrategia de agentes de IA." — Jensen Huang, GTC 2026

Esta no es otra declaración de hype tecnológico. Huang lo comparó directamente con los momentos fundacionales de la computación: cuando apareció Linux, cuando apareció HTML, cuando apareció Kubernetes. Las empresas que no adoptaron esas tecnologías a tiempo quedaron rezagadas. Esta vez la tecnología se llama OpenClaw, y el sistema que la hace apta para empresas se llama NemoClaw.

OPENCLAW NEMOCLAW NVIDIA AGENTES IA ESTRATEGIA ENTERPRISE

→ FUNDAMENTOS

QUÉ ES OPENCLAW Y POR QUÉ IMPORTA

Antes de entender NemoClaw, necesitas entender OpenClaw. OpenClaw es un sistema operativo de agentes de IA de código abierto. No es un chatbot. No es una herramienta que responde preguntas. Es un sistema que **ejecuta tareas completas de forma autónoma**: accede a archivos, llama a APIs, ejecuta código, divide problemas en subtareas y delega a sub-agentes, todo sin intervención humana constante.

La analogía de Huang es exacta: así como Windows hizo posible la era de las computadoras personales, OpenClaw está haciendo posible la era de los agentes personales. En semanas desde su lanzamiento, OpenClaw se convirtió en el proyecto de código abierto de mayor crecimiento en la historia de la computación, superando lo que Linux logró en 30 años.

→

¿QUÉ PUEDE HACER UN AGENTE DE OPENCLAW?

■ **Acceder a archivos y sistemas** — Lee, escribe y organiza documentos, bases de datos y sistemas de archivos.

→ Reemplaza trabajo manual de gestión documental

- **Llamar a herramientas y APIs externas** — Se conecta a servicios como Slack, GitHub, CRMs, ERPs y más.

→ Automatiza flujos de trabajo multi-sistema sin código

- **Ejecutar código y scripts** — Escribe y ejecuta código para resolver problemas complejos.

→ Tiene capacidad técnica de un desarrollador junior

- **Descomponer tareas complejas** — Divide un objetivo en pasos y los ejecuta en secuencia.

→ Gestiona proyectos de principio a fin

- **Crear sub-agentes** — Lanza otros agentes para trabajar en paralelo.

→ Escala el trabajo como un equipo virtual

> Imagina tener un empleado que nunca duerme, que puede operar 10 sistemas a la vez, que sigue instrucciones al pie de la letra y que aprende nuevas habilidades cada vez que lo necesita. Eso es un agente de OpenClaw bien configurado.

→ EL PROBLEMA

POR QUÉ OPENCLAW SOLO ES UN RIESGO PARA TU EMPRESA

OpenClaw es poderoso. También es peligroso si se despliega sin control en un entorno empresarial. Un agente con acceso a tus sistemas puede —sin que nadie lo programe explícitamente— acceder a datos sensibles de empleados, información financiera, datos de clientes, y enviarlos fuera de la organización. No por malicia, sino porque nadie le dijo que no podía.

→

LOS 4 PROBLEMAS CRÍTICOS DE OPENCLAW EN EMPRESAS

→ RIESGO 01

SIN CONTROL DE ACCESO A ARCHIVOS

El agente puede leer y escribir en cualquier parte del sistema por defecto. Tus contratos, bases de datos, credenciales y archivos sensibles están expuestos.

→ RIESGO 02

SIN RESTRICCIONES DE RED

El agente puede conectarse a cualquier servidor externo. Si recibe una instrucción maliciosa (prompt injection), puede filtrar datos hacia afuera sin que nadie lo note.

→ RIESGO 03

SIN GUARDRAILS DE PRIVACIDAD

Las consultas al modelo de IA salen directamente a servidores en la nube. Tus datos confidenciales pueden quedar en logs de terceros.

→ RIESGO 04

SIN GOBIERNO CORPORATIVO

No hay registro de auditoría, no hay políticas definidas, no hay forma de saber qué hizo el agente, cuándo y por qué. Imposible cumplir regulaciones de privacidad.

> Gartner publicó en diciembre de 2025 que las plataformas de gobernanza para agentes de IA serían la infraestructura crítica que las empresas necesitan antes de poder adoptar esta tecnología. NVIDIA escuchó.

→ LA SOLUCIÓN

NEMOCLAW: OPENCLAW PREPARADO PARA EMPRESAS

NemoClaw es la respuesta de NVIDIA a todos esos problemas. No es un reemplazo de OpenClaw. Es una **capa de seguridad y control que envuelve OpenClaw** y lo hace apto para operar dentro de entornos corporativos con datos sensibles, regulaciones de privacidad y políticas de acceso definidas. NVIDIA lo desarrolló junto a Peter Steinberger, el creador original de OpenClaw.

La lógica es simple: OpenClaw pone el motor. NemoClaw pone el volante, los frenos y el cinturón de seguridad.

→

LOS 5 COMPONENTES CLAVE DE NEMOCLAW

→ OPENSHELL — SANDBOX DE SEGURIDAD

El motor de aislamiento de NemoClaw. Crea un contenedor sandboxed donde el agente opera. Usa tecnología de kernel Linux (Landlock, seccomp, network namespaces) para que el agente no pueda salir de sus límites, incluso si es comprometido.

KERNEL-LEVEL ISOLATION | AUDIT TRAIL COMPLETO | SIN FUGA DE DATOS

→ PRIVACY ROUTER — CONTROL DE MODELOS

Evalúa cada solicitud al modelo de IA y decide si va al modelo local (Nemotron en tu hardware) o al modelo cloud. Las tareas con datos sensibles (credenciales, PII, información confidencial) nunca salen de tu máquina.

LOCAL-FIRST PARA DATOS SENSIBLES | CLOUD PARA TAREAS NO CRÍTICAS | CERO LOGS EN TERCEROS

→ POLICY GUARDRAILS — POLÍTICAS YAML

Un archivo de configuración (openclaw-sandbox.yaml) donde defines exactamente qué puede hacer el agente: qué carpetas puede leer, qué dominios puede contactar, qué herramientas puede usar. Las reglas de red se pueden actualizar en caliente sin reiniciar.

CONFIGURACIÓN EN CÓDIGO (GITOPS) | RED: HOT-RELOAD SIN REINICIO | FILESYSTEM: LOCK AL ARRANQ

→ NEMOTRON MODELS — MODELOS PROPIOS

NVIDIA incluye sus propios modelos de lenguaje open-source (Nemotron 3, Cosmos, Groot) para que no dependas de OpenAI o Anthropic para las tareas críticas. Puedes correr inferencia 100% local si tienes GPU NVIDIA.

NEMOTRON 3 SUPER 120B | SIN DEPENDENCIA DE TERCEROS | OPERABLE SIN INTERNET

→ NEMOCLAW CLI — INTERFAZ DE CONTROL

Una interfaz de línea de comandos que orquesta todo el stack: crea sandboxes, gestiona políticas, monitorea logs y maneja el ciclo de vida de los agentes desde un solo lugar.

```
NEMOCLAW STATUS
```

```
NEMOCLAW LOGS --FOLLOW
```

```
NEMOCLAW ONBOARD
```

→ ARQUITECTURA

CÓMO FUNCIONA NEMOCLAW POR DENTRO

NemoClaw implementa un modelo de defensa en profundidad con 4 capas de aislamiento que operan a nivel de kernel del sistema operativo. El agente no puede eludir ninguna de ellas, incluso si recibe instrucciones maliciosas a través de prompt injection.

→ CAPA 1 — RED (NETWORK)

Bloquea TODAS las conexiones salientes excepto los hosts que explícitamente autorices. Las reglas son hot-reloadable: puedes cambiarlas sin reiniciar el sandbox. Si el agente intenta contactar un dominio no autorizado, OpenShell lo bloquea y lo registra.

→ CAPA 2 — SISTEMA DE ARCHIVOS

El agente solo puede escribir en /sandbox y /tmp. El resto del sistema es read-only o completamente bloqueado. Esta restricción se define al crear el sandbox y no puede modificarse mientras corre. Tus archivos en /home, /etc, credenciales en .env o .ssh están completamente aislados.

→ CAPA 3 — PROCESOS

Usa Landlock, seccomp y network namespaces del kernel Linux para bloquear escalada de privilegios y syscalls peligrosas. El agente no puede lanzar procesos con más permisos de los que tiene asignados.

→ CAPA 4 — INFERENCIA

Todas las llamadas al modelo de IA pasan por el OpenShell Gateway. El agente nunca tiene acceso directo a las API keys del modelo. Las credenciales viven fuera del sandbox, gestionadas por NemoClaw de forma transparente.

> La diferencia fundamental con OpenClaw sin NemoClaw: las restricciones existen fuera del agente, en el entorno que lo ejecuta. Aunque el agente sea comprometido completamente, el sandbox mantiene los límites. No confías en el agente. Confías en el entorno.

→ INSTALACIÓN

CÓMO INSTALAR NEMOCLAW EN TU EMPRESA

> NemoClaw está en fase Alpha (desde marzo 2026). Es funcional y usable para experimentación y proyectos piloto, pero NVIDIA aún no lo considera production-ready. Perfecto para empezar a entender la tecnología y probar casos de uso internos.

→

REQUISITOS PREVIOS

→ Ubuntu 22.04 LTS o superior (Linux obligatorio — no macOS, no Windows nativo)

→ Node.js v20 o superior + npm 10 o superior

→ Docker instalado y corriendo con NVIDIA Container Toolkit

→ OpenShell instalado (capa de seguridad de NVIDIA)

→ Mínimo 4 vCPU, 8 GB RAM (16 GB recomendado)

→ Mínimo 20 GB de disco libre (40 GB recomendado para caché)

→ NVIDIA API key gratuita — obtenerla en build.nvidia.com

→ PASO 01

INSTALAR CON UN SOLO COMANDO

Ejecuta este comando en tu terminal Linux:

```
curl -fsSL https://www.nvidia.com/nemoclaw.sh | bash
```

Este script instala automáticamente las dependencias faltantes, integra OpenShell, configura el gateway de inferencia y lanza el asistente de configuración interactivo.

→ PASO 02

CONFIGURAR TU PRIMER AGENTE

Una vez instalado, inicia el asistente de configuración:

```
nemoclaw onboard
```

El wizard te preguntará: nombre del agente, tu NVIDIA API key, modelo a usar (por defecto: nemotron-3-super-120b) y políticas de acceso básicas. Acepta los defaults para un setup inicial rápido.

→ PASO 03

CONECTAR Y USAR EL AGENTE

```
# Conectar al sandbox del agente
nemoclaw my-assistant connect

# Revisar estado
nemoclaw my-assistant status

# Ver logs en tiempo real
nemoclaw my-assistant logs --follow
```

→ PASO 04

DEFINIR POLÍTICAS DE SEGURIDAD

Edita el archivo openclaw-sandbox.yaml para definir exactamente qué puede hacer tu agente. Ejemplo de política para un agente de desarrollo:

```
# openclaw-sandbox.yaml — política de ejemplo
version: "2026-03"
agent_id: "dev-assistant"
capabilities:
  file_system:
    allow:
      - "/home/user/projects/**"   # Solo acceso al proyecto
      - "/tmp/agent-workspace"     # Workspace temporal
    deny:
      - "**/.*"                    # Bloquea archivos ocultos (.env, .ssh)
      - "/etc/**"                  # Sin acceso a configuración del sistema
  network:
    mode: "allowlist"
    allow_domains:
      - "api.github.com"           # GitHub API
      - "pypi.org"                 # Instalar paquetes Python
```

→ PASO 05 — OPCIONAL: DEPLOY EN CLOUD GPU

SI NO TIENES SERVIDOR LINUX LOCAL

NVIDIA ofrece una opción gratuita de 90 días en su plataforma Brev (build.nvidia.com). Crea un entorno NemoClaw pre-configurado en la nube con GPU A100. Ideal para hacer pruebas sin infraestructura propia.

→ APLICACIONES PRÁCTICAS

CÓMO USAR NEMOCLAW EN TU EMPRESA

NemoClaw no es solo una herramienta técnica. Es una plataforma para automatizar procesos de negocio reales con agentes de IA que operan dentro de límites corporativos definidos. Aquí van los casos de uso más relevantes para empresas latinoamericanas:

→ AGENTE DE ANÁLISIS INTERNO

Conecta el agente a tus bases de datos internas, sistemas ERP o Google Sheets. Dale acceso solo a las carpetas y APIs que necesita. El agente puede responder preguntas de negocio, generar reportes y detectar anomalías sin que nadie tenga que escribir SQL.

→ Reemplaza: horas de análisis manual

✓ Ahorro estimado: 15-30 hrs/semana

✓ Riesgo: bajo (acceso solo a datos definidos)

→ AGENTE DE SOPORTE INTERNO

Agente que responde preguntas de empleados sobre políticas de empresa, procesos de RRHH, o troubleshooting técnico. Accede solo a la base de conocimiento interna. Toda la conversación queda en tu servidor, sin pasar por servidores externos.

→ Reemplaza: FAQs manuales y tickets de soporte

✓ Ahorro estimado: 40% de tickets nivel 1

✓ Riesgo: muy bajo (solo lectura de docs internos)

→ AGENTE DE DESARROLLO DE SOFTWARE

Agente con acceso controlado al repositorio de código y APIs de GitHub. Puede revisar PRs, sugerir fixes, escribir tests y documentación. Las políticas YAML definen exactamente qué puede modificar y qué no.

→ Reemplaza: code review parcial y documentación

✓ Ahorro estimado: 10-20 hrs/semana por dev

→ Riesgo: medio (configurar políticas con cuidado)

→ AGENTE DE PROSPECCIÓN Y VENTAS

Agente que investiga leads, enriquece datos de CRM y redacta outreach personalizado. Solo accede a tus herramientas de ventas definidas (HubSpot, Apollo, etc). Opera de forma continua mientras tu equipo duerme.

→ Reemplaza: investigación manual de leads

✓ Ahorro estimado: 20-40 hrs/semana del equipo

✓ Riesgo: bajo (datos públicos + CRM propio)

→ AGENTE DE MONITOREO Y ALERTAS

Agente always-on que monitorea métricas de negocio, sistemas en producción o actividad de redes sociales. Envía alertas a Slack cuando detecta anomalías. Corre 24/7 en tu servidor sin costo de personal.

→ Reemplaza: dashboards manuales y alertas reactivas

✓ Ahorro estimado: reducción de tiempo de respuesta 80%

✓ Riesgo: muy bajo (solo lectura de métricas)

→ LA GRAN OPORTUNIDAD

POR QUÉ ESTO CAMBIA TODO PARA TU NEGOCIO

Hay dos tipos de empresas frente a esta tecnología: las que la adopten ahora mientras es compleja, y las que la adopten después cuando sea tarde. La ventana de ventaja competitiva real está en los próximos 12-18 meses.

→

LO QUE VIENE

→ SaaS convertidos en agentes

Huang predijo que "cada empresa de SaaS se convertirá en una empresa de Agent-as-a-Service". Los SaaS que no integren agentes autónomos serán reemplazados. Las empresas que implementen agentes internos antes dejarán de pagar por esos SaaS.

→ Empleados virtuales a costo marginal

Un agente NemoClaw correctamente configurado puede hacer el trabajo de 1-3 empleados en funciones de análisis, soporte, y administración. El costo marginal por hora de trabajo es prácticamente cero.

→ Primera mover advantage

Las empresas que hoy experimenten con NemoClaw estarán 12-18 meses adelante cuando esto se vuelva masivo. Igual que las empresas que adoptaron el cloud en 2010 vs. las que lo hicieron en 2015.

> ¿Qué empresa no debería estar explorando esto hoy? Cualquiera que tenga procesos repetitivos, datos internos que analizar, equipos que pierden horas en tareas manuales, o que quiera escalar sin escalar el headcount.

→ PRÓXIMOS PASOS

CÓMO EMPEZAR CON NEMOCLAW HOY

→ SEMANA 1 — Explorar y entender

Crea una cuenta gratuita en build.nvidia.com y prueba el entorno de NemoClaw en la nube. No necesitas infraestructura propia. Familiarízate con los comandos básicos y las políticas YAML.

→ SEMANA 2-3 — Primer caso de uso piloto

Elige el proceso más repetitivo de tu empresa. Configura un agente con acceso mínimo y mide cuántas horas ahorra. Documenta el proceso para escalar.

→ SEMANA 4-8 — Escalar e integrar

Conecta el agente a tus sistemas internos reales: CRM, ERP, bases de datos. Define políticas de acceso estrictas. Involucra al equipo de IT para validar seguridad.

→ MES 3+ — Múltiples agentes en producción

Despliega agentes por área: uno para ventas, uno para soporte, uno para análisis. Cada uno con políticas independientes. Evalúa reemplazar suscripciones de SaaS que los agentes hacen obsoletas.

→

RECURSOS OFICIALES

→ **Página oficial NemoClaw** nvidia.com/nemoclaw

→ **Documentación del desarrollador** docs.nvidia.com/nemoclaw/latest/

→ **Repositorio GitHub oficial** github.com/NVIDIA/NemoClaw

→ **Entorno cloud gratuito (Brev)** build.nvidia.com

→ **NVIDIA API key gratuita** build.nvidia.com → API Keys

→ SOBRE EL AUTOR



Jorge Riquelme

→ Fundador · Otherway Labs

Ayudo a pymes a recuperar tiempo y dinero a través de automatizaciones con IA con un ROI claro y garantizado. He trabajado con decenas de negocios, identificando los procesos que más les hacen perder tiempo y convirtiéndolos en flujos automáticos que corren solos.

otherwaylabs.cl → LinkedIn: Jorge Riquelme

→ SESIÓN GRATUITA

¿QUIERES IMPLEMENTAR NEMOCLAW EN TU EMPRESA?

Te regalamos una sesión de diagnóstico gratuita. Vamos a revisar juntos qué procesos de tu empresa se pueden automatizar con agentes de IA, cuáles son los primeros candidatos para NemoClaw y cómo hacerlo sin poner en riesgo tu seguridad.

- ✓ Mapa de los procesos con mayor impacto para automatizar en tu empresa.
- ✓ Evaluación de qué nivel de seguridad necesitas para tu caso específico.
- ✓ Hoja de ruta con primeros pasos concretos para empezar esta semana.

Agenda tu sesión en: otherwaylabs.cl →