

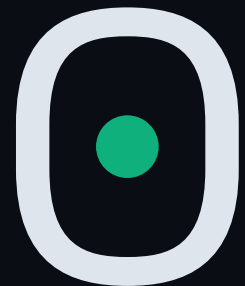
POISON/ZERO

Onboarding

Seis pasos para administradores y desarrolladores, de la clave de instalación al feedback.

- 01 Preparar la consola
- 02 Instalar
- 03 Configurar
- 04 Usar
- 05 Ver la telemetría
- 06 Enviar feedback

Para **poison0** **exec0**



1

Preparar la consola

PLAN

CONSOLA

Enterprise

`https://<tenant>.poison0.com` o tu propio dominio

Solo Dev, Pro

`https://console.poisonzero.com`

1

Invitar a más administradores: **Settings** → **Acceso y seguridad** → **Personas** → introduce el correo → **Invitar**. El enlace vale 7 días.

2

Crear una clave de instalación: **Dispositivos** → **Despliega varios dispositivos con una clave** → **Elegir variante: Cloud** → **Generar clave**. La clave se muestra una sola vez.

3

Pasa la clave a los desarrolladores o a IT. Vale 30 días y para tantos dispositivos como permita tu plan (Enterprise: ilimitado).

2

Instalar

Variante A o B. Ambas configuran `/pz` y la línea de estado en Claude Code.

Comprobar tras instalar: reinicia Claude Code. La línea de estado muestra  **PoisonZero** .

2A. El desarrollador instala por su cuenta

MACOS / LINUX · TERMINAL

```
curl -fsSL https://poisonzero.com/install.sh | sudo PZ_ENROLL_CODE=<clave> PZ_SETUP_AGENTS=claude PZ_SETUP_STATUSLINE=1 sh
```

WINDOWS · POWERSHELL COMO ADMINISTRADOR

```
$env:PZ_ENROLL_CODE='<clave>'; $env:PZ_SETUP_AGENTS='claude'; $env:PZ_SETUP_STATUSLINE='1'; irm https://poisonzero.com/install.ps1 | iex
```

Dispositivos headless (p. ej. por SSH): añade `PZ_HEADLESS=strict`. Los cambios dudosos se revierten al instante en lugar de preguntar en un diálogo. Sin indicarlo, el agente poison0 lo detecta solo.

2B. IT despliega con Jamf, Intune o Ansible

Paso 1: instalar (como root o SYSTEM)

MACOS / LINUX · ROOT

```
PZ_ENROLL_CODE=<clave> sh -c "$(curl -fsSL https://poisonzero.com/install.sh)"
```

WINDOWS · SYSTEM

```
$env:PZ_ENROLL_CODE='<clave>'; irm https://poisonzero.com/install.ps1 | iex
```

Paso 2: configurar Claude Code (como el usuario con sesión iniciada)

MACOS / LINUX · USUARIO

```
poisonzero setup-claude
poisonzero setup-claude --statusline-only
```

WINDOWS · USUARIO

```
& "$env:ProgramFiles\PoisonZero\poisonzero.exe" setup-claude
& "$env:ProgramFiles\PoisonZero\poisonzero.exe" setup-claude --statusline-only
```

JAMF · ROOT, EN LA CUENTA DEL USUARIO CON SESIÓN INICIADA

```
u=$(stat -f%Su /dev/console)
sudo -u "$u" -H env -u SUDO_USER /usr/local/bin/poisonzero setup-claude
sudo -u "$u" -H env -u SUDO_USER /usr/local/bin/poisonzero setup-claude --statusline-only
```

HERRAMIENTA AJUSTE

Intune	Ejecutar el script con las credenciales del usuario con sesión iniciada: Sí ("Run this script using the logged on credentials"). Hace falta la ruta completa porque <code>PATH</code> no incluye la carpeta del programa.
Jamf	Se ejecuta como root; la pestaña Jamf ejecuta el paso 2 en la cuenta del usuario con sesión iniciada.

2C. Nombre del dispositivo al instalar (opcional)

Añade una de estas variables junto a `PZ_ENROLL_CODE`. Se aplica la primera definida, en este orden:

VARIABLE	EFFECTO
<code>PZ_DEVICE_NAME="Platform / Laptop 07"</code>	El nombre se toma tal cual
<code>PZ_DEVICE_NAMES_CSV=<archivo o URL https></code>	CSV con la cabecera <code>hostname,name</code> . El instalador busca su propio hostname y toma el nombre. Solo se envía el nombre, nunca el hostname
<code>PZ_DEVICE_NAME_FROM_HOSTNAME=1</code>	El hostname pasa a ser el nombre del dispositivo. No recomendado

PZ-NAMES.CSV

```
hostname,name
mbp-0231,Platform / Laptop 07
```

Nota: El nombre del dispositivo lo decide el administrador. El nombre no debe contener datos personales, por ejemplo ningún nombre de persona.

Longitud	de 1 a 60 caracteres, sin caracteres de control
Nombre no válido	se ignora y el dispositivo se registra igualmente
Cuándo se aplica el nombre	solo al registrar un dispositivo por primera vez. En un dispositivo ya registrado, cambia el nombre en la consola: Dispositivos → Renombrar dispositivo .
Disponible desde	la versión 1.16.45

3 Configurar

- 1 Nombrar los dispositivos sin nombre: **Dispositivos** → en el dispositivo **Renombrar dispositivo** → escribe el **Nombre visible del dispositivo**, por ejemplo «Platform / Laptop 07».
- 2 Separar equipos (opcional): crea una clave de instalación por equipo, cada una con su propio **Perfil (opcional)**. Gestionar perfiles: **Settings** → **Protección y dispositivos** → **Perfiles**.

3 **Comprobar las llamadas de herramientas con `exec0` (opcional)**

`exec0` comprueba cada llamada a herramientas de tus agentes de IA antes de que se ejecute. El dispositivo necesita una GPU adecuada para Melira Ultra. La página del dispositivo muestra si puede ejecutar `exec0`.

Configuración: **Settings** → **Protección y dispositivos** → **Perfiles** → **Editar** en el perfil → **exec0 con Melira AI** → **Modo**

MODO	EFEECTO
Desactivado (predeterminado)	Sin comprobación
Observar	Comprueba cada llamada. Las reglas fijas siguen bloqueando y las llamadas peligrosas solo se cuentan. 14 días por defecto, después <code>exec0</code> sigue observando y no cambia a Protección por sí mismo.
Protección	Bloquea las llamadas peligrosas antes de que se ejecuten

Casos dudosos: en ambos modos decide la persona en el dispositivo.

Comprobación imposible: en Protección la llamada se bloquea (predeterminado).

Dispositivos privados: se configura en el dispositivo; en Windows sin `sudo` en un terminal abierto como administrador.

COMANDO	EFEECTO
<code>sudo poison0 exec0 observe</code>	Observar
<code>sudo poison0 exec0 enforce</code>	Protección
<code>sudo poison0 exec0 off</code>	Desactivado
<code>poison0 exec0 fail open</code>	Dejar pasar una llamada cuando <code>exec0</code> no puede comprobarla

Más: [Cómo revisa `exec0` las llamadas de herramientas](#)

4

Usar

DÓNDE	ENTRADA	RESULTADO
Claude Code	/pz	Estadística de protección de este mes
Claude Code	Línea de estado	● protección activa; ● el servicio funciona pero informa de un problema; ● el servicio no funciona
Línea de comandos	poisonzero stats	Estadística de protección
Línea de comandos	sudo poisonzero status	Todas las decisiones, cuarentena abierta
Línea de comandos	sudo poisonzero quarantine list	Cambios retenidos; show , restore , discard <id>
Línea de comandos	poisonzero doctor	Autodiagnóstico
Línea de comandos	sudo poisonzero egress	Lo que ha salido del equipo (en Linux también sin sudo)
Línea de comandos	poisonzero exec0 status	Modo de exec0 en este dispositivo, hook en Claude Code, últimas 24 horas

Windows: sin sudo , en PowerShell como administrador y con la ruta completa & "\$env:ProgramFiles\PoisonZero\poisonzero.exe" .

ACTUALIZACIÓN POR	/PZ EN CLAUDE CODE
install.sh , install.ps1	Los archivos /pz existentes del usuario que instala se renuevan automáticamente
Homebrew, Scoop, .deb / .rpm , actualización automática	Cada usuario ejecuta una vez poisonzero setup-claude

5

Ver la telemetría

CONSOLA	CONTENIDO
Dispositivos	Estado e incidentes por dispositivo
Analítica	Cambios bloqueados por tipo y día; filtro por dispositivo, agente, sistema operativo, 7/30/90 días
Auditoría	Cada incidente con el texto del ataque redactado

Nunca se transmiten: textos completos de los archivos (solo cambios redactados), archivos fuera de las rutas protegidas, información de procesos y del sistema.

6 Enviar feedback

DÓNDE	ENTRADA
Claude Code	<code>/pz feedback <texto></code>
Línea de comandos	<code>poisonzero feedback "<texto>"</code> (sin <code>sudo</code>)
PUNTO	REGLA
Longitud	Como máximo 2000 caracteres
Redacción	En local antes del envío: secretos, direcciones de correo, IBAN, números de tarjeta, direcciones IP, teléfonos, asignaciones de claves y tokens, y el nombre de usuario en rutas personales (<code>/Users/<nombre></code> , <code>/home/<nombre></code> , <code>C:\Users\<nombre></code>). El comando muestra el texto tras la redacción
Envío	Con el siguiente check-in. El dispositivo solo envía el texto, la versión y la plataforma; al recibirlo, PoisonZero guarda con él el nombre actual del dispositivo
Destinatario	Solo el equipo de PoisonZero ve el texto, no tus propios administradores
Respuesta	Si el equipo responde, el titular de la cuenta recibe la fecha y el dispositivo del feedback, no su texto
Modo privado	Bloqueado; usa en su lugar el formulario de contacto de poisonzero.com

Sigue leyendo

Todas las variables y rutas del instalador: [instalar el agente poison0](#). Qué muestra la consola por incidente: [incidentes y auditoría](#). Cómo llegan las actualizaciones: [actualizaciones y ciclo de vida](#).