



MANUAL DEL USUARIO • CENTRO DE AYUDA DE SIAC

La Malla SIAC

Tus servidores, gobernados como un solo sistema. Cada servidor es un nodo con identidad propia y un catálogo de herramientas con su riesgo declarado; una sola puerta MCP los pone al alcance de tus agentes, de Airo y de tus herramientas de desarrollo. Lo irreversible lo confirma una persona y todo queda en el ledger.

Dirigido a

Administradores

Plataforma

SIAC v1.0.134+repo

Tiempo

15 minutos

Pantallas capturadas

**26 de septiembre de
2026**

Contenido

1 · Antes de empezar	3
2 · Cómo funciona	4
3 · La pantalla de un vistazo	5
4 · Encender un nodo y elegir qué expone	7
5 · Herramientas y riesgo	2
6 · Confirmar lo irreversible	11
7 · Servidores que se hablan	13
8 · Dominios con tu marca	15
9 · Unir un servidor externo	17
10 · Agentes que aceptan tareas	19
11 · El ledger	21
12 · La puerta MCP	23
13 · Preguntas frecuentes	24

CAPÍTULO 1

Antes de empezar

PARA QUIÉN ES

Administradores de la organización que gobiernan sus servidores de Dev Studio y los que se unen desde fuera.

TIEMPO ESTIMADO

15 minutos

PANTALLAS DE

SIAC v1.0.134+repo · capturadas el 26 de septiembre de 2026

Lo que necesita

- Ser administrador de tu organización (o de la plataforma).
- Al menos un servidor de Dev Studio, o un servidor propio que quieras unir.

Tabla 1. Permisos

Rol	Qué puede hacer aquí
Administrador de la organización	Encender y apagar nodos, elegir qué exponen, aprobar o negar acciones, crear rutas, registrar dominios y unir servidores externos de tu organización.
Operador de la plataforma	Lo mismo en todas las organizaciones, y las rutas que cruzan organizaciones (quedan escritas).

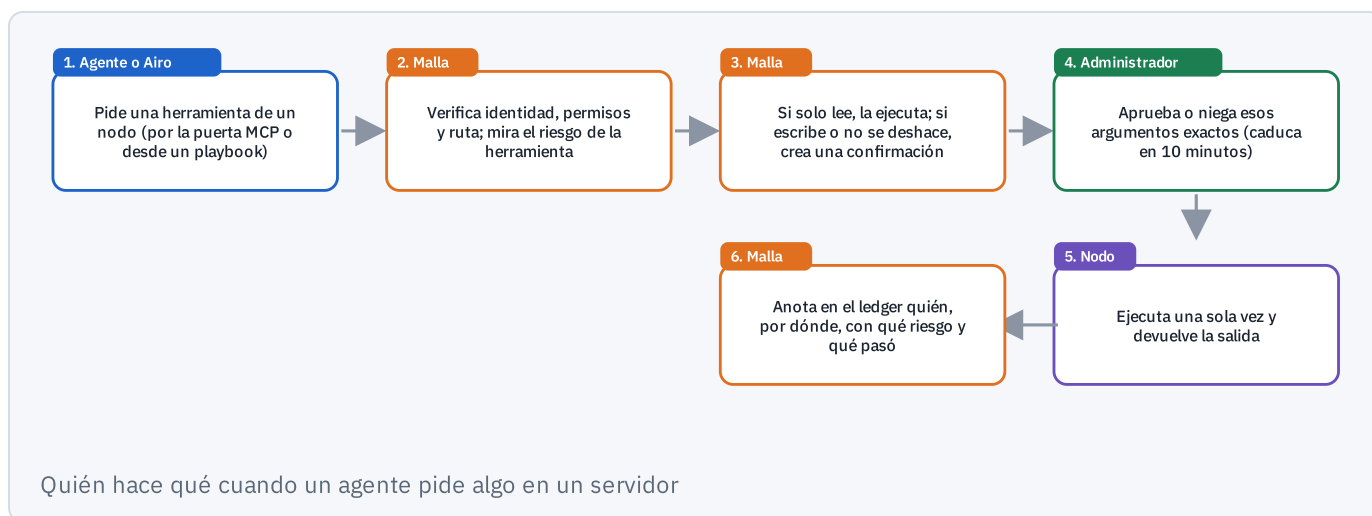
CAPÍTULO 2

Cómo funciona

Un agente propone; la Malla verifica; una persona decide lo irreversible

Hasta ahora cada servidor era una isla: se entraba por su terminal y lo que pasaba adentro solo lo sabía quien estaba sentado. La Malla convierte cada servidor en un **nodo**: recibe una identidad firmada por SIAC (un certificado que se renueva solo cada 24 horas), declara qué herramientas ofrece y con qué riesgo, y solo responde a quien tu organización autorizó.

Los servidores que alojan instancias dedicadas de SIAC de un cliente **no entran en la Malla**: nunca reciben certificado y no aparecen en ninguna lista. Esa separación es a propósito y no se puede apagar.



CAPÍTULO 3

La pantalla de un vistazo

Todo el estado de tu malla, arriba

DÓNDE ESTÁ

Malla

QUIÉN LA USA

Administradores de la organización

DIRECCIÓN

/malla

CUÁNDO USARLA

Cada vez que quieras saber **qué servidores tienes, qué espera tu aprobación o qué pasó en ellos.**

Arriba ves el resumen 2: cuántos nodos están encendidos sobre el total, cuántas herramientas declaran, cuántas llamadas hubo en las últimas 24 horas y cuántas acciones esperan a una persona. **Actualizar** 1 vuelve a leer todo; úsalo después de encender un nodo o si alguien aprobó algo desde otra sesión.

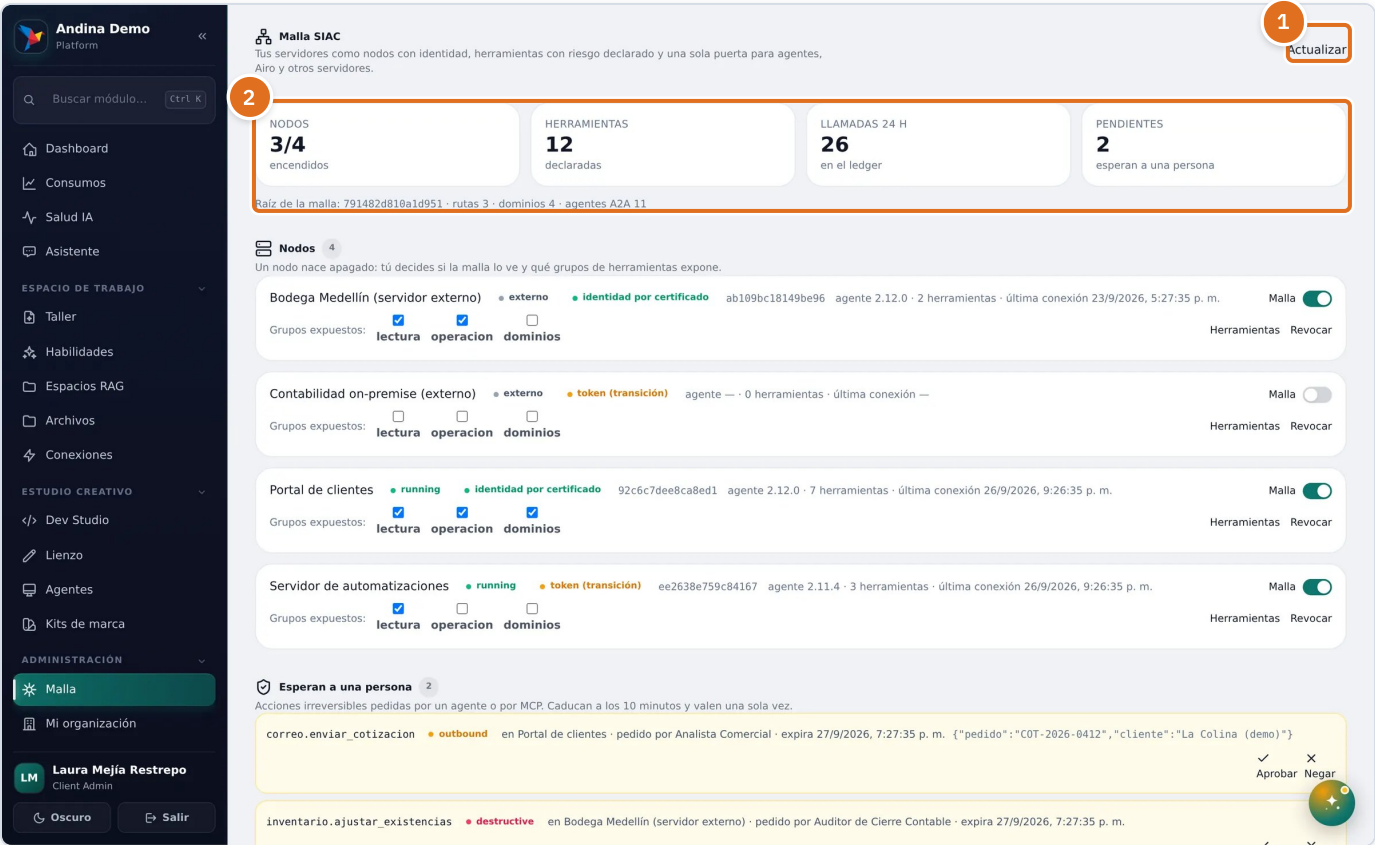


Figura 1. La Malla de una organización con cuatro nodos en estados distintos.

- 1 **Actualizar.** Vuelve a leer nodos, pendientes, rutas, dominios y el ledger; úsalo tras encender un nodo o si alguien aprobó algo desde otro lado.

- 2 **Nodos · Herramientas · Llamadas 24 h · Pendientes.**
Resumen de un vistazo: nodos encendidos sobre el total, herramientas declaradas, llamadas del último día y acciones que esperan a una persona; abajo, la huella de la raíz de la malla.

REGLA DEL SISTEMA

Solo ves los nodos de tu organización. Un superadministrador ve todos.

Tabla 2. Qué hace cada elemento de «La pantalla de un vistazo» · los usan: Administradores de la organización

Elemento	Qué hace
Actualizar	Vuelve a leer nodos, pendientes, rutas, dominios y el ledger; úsalo tras encender un nodo o si alguien aprobó algo desde otro lado.
Nodos · Herramientas · Llamadas 24 h · Pendientes	Resumen de un vistazo: nodos encendidos sobre el total, herramientas declaradas, llamadas del último día y acciones que esperan a una persona; abajo, la huella de la raíz de la malla.

CAPÍTULO 4

Encender un nodo y elegir qué expone

Apagado por defecto; lo enciende el dueño

DÓNDE ESTÁ Malla	DIRECCIÓN /malla
QUIÉN LA USA Administradores de la organización	CUÁNDO USARLA Cuando un servidor nuevo aparece en la Malla, o cuando quieres cambiar lo que ofrece.

Un servidor aparece en la Malla en cuanto su agente se conecta con identidad, pero **nace apagado**: nadie puede invocar nada en él hasta que lo enciendas. Cada tarjeta 1 muestra su estado, su versión y su última conexión; la **identidad** 2 debe decir «identidad por certificado». El interruptor 3 lo enciende o lo apaga, y las casillas 4 eligen qué grupos de herramientas expone: **lectura** (recursos, contenedores, servicios, archivos permitidos), **operación** (reiniciar servicios, escribir en rutas permitidas) y **dominios** (publicar sitios).

Un nodo nace apagado: tú decides si la malla lo ve y qué grupos de herramientas expone.

Nodo	Estado	Identidad	Agente	Herramientas	Última conexión	Malla
Bodega Medellín (servidor externo)	externo	identidad por certificado	ab109bc18149be96	agente 2.12.0 · 2 herramientas	última conexión 23/9/2026, 5:27:35 p. m.	☒
Contabilidad on-premise (externo)	externo	token (transición)	agente —	0 herramientas	última conexión —	☐
Portal de clientes	running	identidad por certificado	92c6c7dee8ca8ed1	agente 2.12.0 · 7 herramientas	última conexión 26/9/2026, 9:26:35 p. m.	☒
Servidor de automatizaciones	running	token (transición)	ee2638e759c84167	agente 2.11.4 · 3 herramientas	última conexión 26/9/2026, 9:26:35 p. m.	☒

Figura 2. La tarjeta de un nodo encendido con sus grupos expuestos.

- 1 Tarjeta del nodo.** Un servidor de la malla con su estado, su identidad, la versión del agente, cuántas herramientas tiene y su última conexión.
- 2 identidad por certificado.** Cómo se identifica el nodo: «identidad por certificado» es lo esperado; «token (transición)» indica un nodo que aún no migró a certificado.
- 3 Malla.** Enciende o apaga la malla en este servidor. Apagado, ningún agente ni la puerta MCP lo ven.
- 4 Grupos expuestos:** Casillas de los grupos de herramientas (recursos, contenedores, servicios, archivos...) que este nodo ofrece a la malla; marca solo lo que necesitas.
- 5 Herramientas.** Abre la lista de herramientas del nodo con su nivel de riesgo, para revisarlas o ejecutar las que no piden datos.
- 6 Revocar.** Revoca el acceso a este nodo.

- 6 Revocar.** Revoca la identidad del nodo: deja de poder hablar con la malla hasta que se vuelva a enrolar. Pide confirmación.

PASO A PASO

- 1** Busca la tarjeta del servidor en **Nodos**.
- 2** Comprueba que diga **identidad por certificado** 2. La huella es la de la llave del propio servidor; la raíz que la firma está en la cabecera de la pantalla.
- 3** Enciende el interruptor **Malla** 3.
- 4** Marca solo los grupos que ese servidor debe ofrecer 4. Empieza por **lectura**; agrega **operación** solo si un agente la necesita.
- 5** Si el servidor cambió de manos o sospechas de él, pulsa **Revocar** 6: se queda sin certificado y vuelve a nacer apagado en su siguiente conexión.

IMPORTANTE

Revocar corta la identidad del servidor de inmediato. Para volver, tendrá que conectarse de nuevo y alguien tendrá que encenderlo.

Tabla 3. Qué hace cada elemento de «Encender un nodo y elegir qué expone» · los usan: Administradores de la organización

Elemento	Qué hace
Tarjeta del nodo	Un servidor de la malla con su estado, su identidad, la versión del agente, cuántas herramientas tiene y su última conexión.
identidad por certificado	Cómo se identifica el nodo: «identidad por certificado» es lo esperado; «token (transición)» indica un nodo que aún no migró a certificado.
Malla	Enciende o apaga la malla en este servidor. Apagado, ningún agente ni la puerta MCP lo ven.
Grupos expuestos:	Casillas de los grupos de herramientas (recursos, contenedores, servicios, archivos...) que este nodo ofrece a la malla; marca solo lo que necesitas.
Herramientas	Abre la lista de herramientas del nodo con su nivel de riesgo, para revisarlas o ejecutar las que no piden datos.
Revocar	Revoca la identidad del nodo: deja de poder hablar con la malla hasta que se vuelva a enrolar. Pide confirmación.

CAPÍTULO 5

Herramientas y riesgo

Cada herramienta dice qué tan grave es equivocarse

DÓNDE ESTÁ Malla	DIRECCIÓN /malla
QUIÉN LA USA Administradores de la organización	CUÁNDO USARLA Antes de exponer un grupo, para saber qué ofrece; o para ejecutar una consulta a mano.

Herramientas en la tarjeta abre el catálogo del nodo 1. El agente del servidor lo declara y SIAC lo sella: si cambia, se nota. Cada herramienta trae su **riesgo** 2:

- **safe**: solo lee; se ejecuta directo.
- **sensitive**: lee algo que podría revelar datos; se ejecuta y se anota quién lo pidió.
- **overwrite** y **outbound**: escribe o sale hacia afuera; pide confirmación.
- **destructive**: no se deshace; siempre pide confirmación de una persona.

Ejecutar 3 corre la herramienta y muestra su salida; si su riesgo lo exige, queda esperando una aprobación.

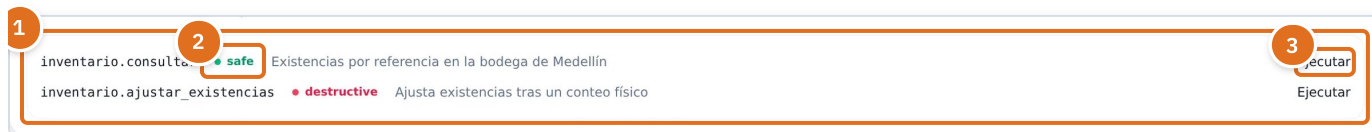


Figura 3. El catálogo de un nodo con el riesgo de cada herramienta.

- Herramientas del nodo.** Lista de herramientas visibles de este nodo, cada una con su riesgo, su descripción y, si no pide datos, el botón para ejecutarla; la salida aparece debajo.
- Riesgo.** Nivel de riesgo declarado de la herramienta. Las de riesgo alto no se ejecutan de inmediato: quedan esperando la confirmación de una persona.
- Ejecutar.** Ejecuta la herramienta en el nodo. Si su riesgo lo exige, queda pendiente en «Esperan a una persona».

REGLA DEL SISTEMA

Las rutas del sistema (llaves, credenciales, la configuración del agente) están protegidas: ninguna herramienta las lee ni las escribe, sea quien sea quien lo pida.

Tabla 4. Qué hace cada elemento de «Herramientas y riesgo» · los usan: Administradores de la organización

Elemento	Qué hace
Herramientas del nodo	Lista de herramientas visibles de este nodo, cada una con su riesgo, su descripción y, si no pide datos, el botón para ejecutarla; la salida aparece debajo.
Riesgo	Nivel de riesgo declarado de la herramienta. Las de riesgo alto no se ejecutan de inmediato: quedan esperando la confirmación de una persona.
Ejecutar	Ejecuta la herramienta en el nodo. Si su riesgo lo exige, queda pendiente en «Esperan a una persona».

CAPÍTULO 6

Confirmar lo irreversible

Un agente propone; una persona decide

DÓNDE ESTÁ Malla	DIRECCIÓN /malla
QUIÉN LA USA Administradores de la organización	CUÁNDO USARLA Cuando el resumen muestra pendientes , o te llega el aviso de una acción por aprobar.

Cuando un agente, Airo o un cliente MCP pide algo **overwrite**, **outbound** o **destructive**, la Malla no lo ejecuta: crea una acción pendiente en **Esperan a una persona** 1. Cada una 2 dice qué herramienta, en qué nodo, quién la pidió, con qué argumentos y cuándo caduca.

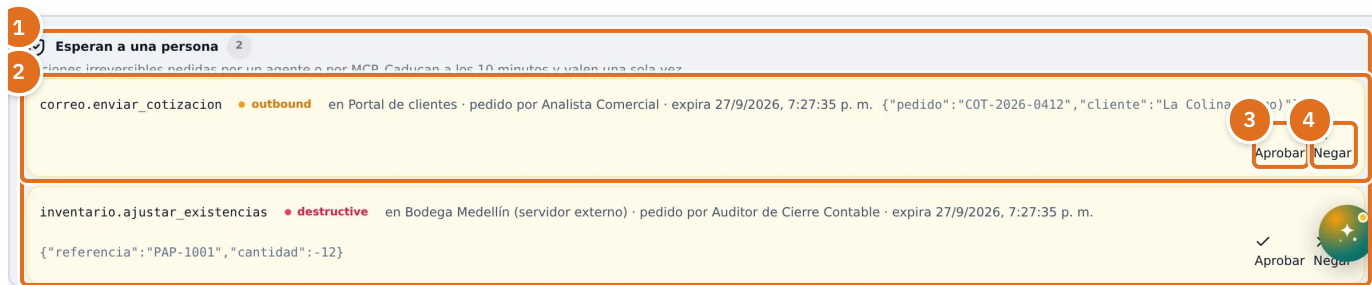


Figura 4. Dos acciones que esperan a una persona.

- 1 Esperan a una persona.** Acciones irreversibles que pidió un agente o la puerta MCP. Caducan a los 10 minutos y valen una sola vez: revísalas y decide.
- 2 Acción pendiente.** Una acción pendiente: qué herramienta, en qué nodo, quién la pidió, con qué argumentos y cuándo expira.
- 3 Aprobar.** Autoriza la acción pendiente; se ejecuta una sola vez y queda registrada en el ledger.
- 4 Negar.** Rechaza la acción pendiente; no se ejecuta y el rechazo queda en el ledger.

PASO A PASO

- 1 Lee los **argumentos exactos** de la acción 2 y quién la pidió.
- 2 Si es lo que esperabas, pulsa **Aprobar** 3: se ejecuta una sola vez y queda en el ledger.
- 3 Si algo no cuadra, pulsa **Negar** 4 y escribe por qué.

IMPORTANTE

Aprobar no significa «confío en el agente»: significa «vi estos argumentos y quiero que pasen». Caduca a los 10 minutos y sirve para un solo uso.

SI SIAC NO LO DEJA AVANZAR

«La confirmación caducó»

Por qué aparece. Pasaron más de 10 minutos desde que el agente la pidió.

Qué hacer. Pide al agente que vuelva a intentarlo: se crea una confirmación nueva.

Tabla 5. Qué hace cada elemento de «Confirmar lo irreversible» · los usan: Administradores de la organización

Elemento	Qué hace
Esperan a una persona	Acciones irreversibles que pidió un agente o la puerta MCP. Caducan a los 10 minutos y valen una sola vez: revísalas y decide.
Acción pendiente	Una acción pendiente: qué herramienta, en qué nodo, quién la pidió, con qué argumentos y cuándo expira.
Aprobar	Autoriza la acción pendiente; se ejecuta una sola vez y queda registrada en el ledger.
Negar	Rechaza la acción pendiente; no se ejecuta y el rechazo queda en el ledger.

CAPÍTULO 7

Servidores que se hablan

Una ruta dice qué puede pedirle un nodo a otro

DÓNDE ESTÁ Malla	DIRECCIÓN /malla
QUIÉN LA USA Administradores de la organización	CUÁNDO USARLA Cuando un servidor necesita invocar herramientas de otro (por ejemplo, un servidor de integración que consulta a otro de datos).

Por defecto ningún servidor ve a otro. Una ruta 1 autoriza a un nodo de origen a invocar, en un nodo de destino, una lista concreta de herramientas. En el ledger queda que llamó **un nodo**, no una persona.

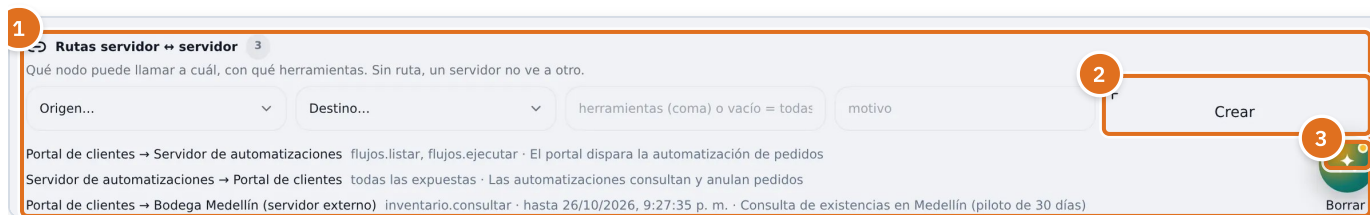


Figura 5. Las rutas entre servidores de la organización.

- 1 Rutas servidor ↔ servidor.** Qué nodo puede llamar a cuál y con qué herramientas. Sin ruta, un servidor no ve a otro. Elige origen, destino, herramientas y motivo.
- 2 Crear.** Crea la ruta entre el nodo de origen y el de destino con las herramientas indicadas (vacío = todas las expuestas).
- 3 Borrar.** Borra la ruta: el origen deja de poder llamar al destino.

PASO A PASO

- 1 Elige el nodo de **origen** y el de **destino**, y las herramientas que puede invocar (vacío = todas las expuestas).
- 2 Pulsa **Crear** 2.
- 3 Para cortar el acceso, pulsa **Borrar** 3 en la ruta.

REGLA DEL SISTEMA

Las rutas viven dentro de tu organización. Solo la plataforma puede cruzar organizaciones, y queda escrito.

Tabla 6. Qué hace cada elemento de «Servidores que se hablan» · los usan: Administradores de la organización

Elemento	Qué hace
Rutas servidor ↔ servidor	Qué nodo puede llamar a cuál y con qué herramientas. Sin ruta, un servidor no ve a otro. Elige origen, destino, herramientas y motivo.
Crear	Crea la ruta entre el nodo de origen y el de destino con las herramientas indicadas (vacío = todas las expuestas).
Borrar	Borra la ruta: el origen deja de poder llamar al destino.

CAPÍTULO 8

Dominios con tu marca

Más de una puerta de entrada, con tu nombre

DÓNDE ESTÁ Malla	DIRECCIÓN /malla
QUIÉN LA USA Administradores de la organización	CUÁNDO USARLA Cuando quieres que SIAC —o un sitio que corre en tu servidor— responda en un dominio propio.

En **Dominios** 1 registras un dominio —tuyo o un subdominio de SIAC— y eliges su destino: la aplicación SIAC con tu marca o un servidor de la Malla. Cada dominio muestra su **estado** 3: pendiente, verificado o activo.

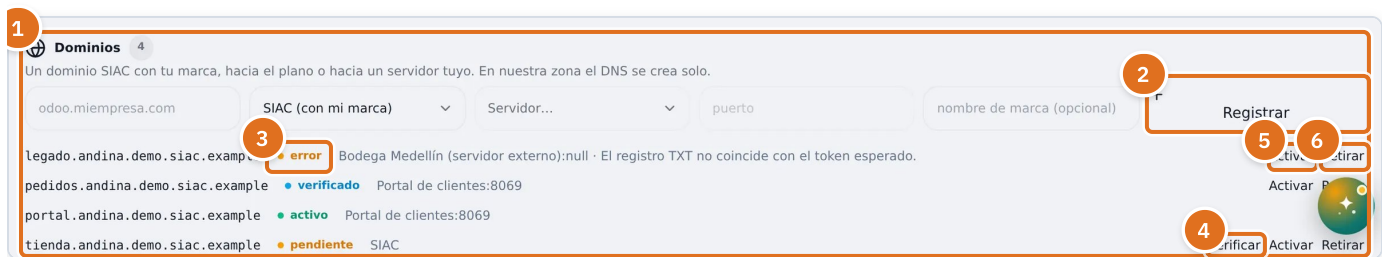


Figura 6. Dominios en sus tres estados.

- 1 Dominios.** Dominios SIAC con tu marca, hacia SIAC o hacia un servidor tuyo. Escribe el dominio, elige el destino y regístralo.
- 2 Registrar.** Registra el dominio escrito con su destino y marca. Queda pendiente hasta verificarlo y activarlo.
- 3 Estado del dominio.** Estado del dominio: pendiente (falta verificar), verificado (listo para activar) o activo (ya sirve tráfico).
- 4 Verificar.** Comprueba que el DNS del dominio apunta a SIAC; en la zona de SIAC el DNS se crea solo.
- 5 Activar.** Pone el dominio a servir tráfico hacia su destino.
- 6 Retirar.** Retira el dominio y deja de servirlo. Pide confirmación.

PASO A PASO

- 1 Escribe el dominio, elige el destino y pulsa **Registrar** 2. Si es de la zona de SIAC, el DNS se crea solo; si es tuyo, la pantalla te dice el registro A que debes crear.
- 2 Pulsa **Verificar** 4: SIAC pregunta a los servidores de nombres autoritativos, no a una caché.
- 3 Pulsa **Activar** 5: se publica la ruta y se emite el certificado HTTPS (suele tardar menos de un minuto).
- 4 Para quitarlo, **Retirar** 6 borra la ruta y, si el DNS era de SIAC, también el registro.

SI SIAC NO LO DEJA AVANZAR**«El dominio todavía no apunta a SIAC»****Por qué aparece.** El registro A no existe o aún no se propagó en todos los servidores de nombres.**Qué hacer.** Crea o corrige el registro A que muestra la pantalla, espera unos minutos y vuelve a pulsar Verificar.

Tabla 7. Qué hace cada elemento de «Dominios con tu marca» · los usan: Administradores de la organización

Elemento	Qué hace
Dominios	Dominios SIAC con tu marca, hacia SIAC o hacia un servidor tuyo. Escribe el dominio, elige el destino y regístralo.
Registrar	Registra el dominio escrito con su destino y marca. Queda pendiente hasta verificarlo y activarlo.
Estado del dominio	Estado del dominio: pendiente (falta verificar), verificado (listo para activar) o activo (ya sirve tráfico).
Verificar	Comprueba que el DNS del dominio apunta a SIAC; en la zona de SIAC el DNS se crea solo.
Activar	Pone el dominio a servir tráfico hacia su destino.
Retirar	Retira el dominio y deja de servirlo. Pide confirmación.

CAPÍTULO 9

Unir un servidor externo

Traer a la Malla un servidor que no creó SIAC

DÓNDE ESTÁ Malla	DIRECCIÓN <code>/malla</code>
QUIÉN LA USA Administradores de la organización	CUÁNDO USARLA Cuando quieres gobernar desde SIAC un servidor tuyo que no nació en Dev Studio.

En **Unir un servidor externo** 1 le das un nombre y pides un código de un solo uso. El instalador solo abre conexiones **hacia afuera**: no expone puertos. En cuanto se conecta, el servidor aparece como nodo **apagado**, esperando a que lo enciendas.



Figura 7. El alta de un servidor externo.

- 1 Unir un servidor externo.** Alta de un servidor que no aprovisionó SIAC: le das un nombre, pides un código y pegas el comando que aparece en ese servidor.
- 2 Pedir código.** Emite un código de un solo uso (15 minutos) y el comando que se ejecuta en el servidor externo para unirlo a la malla con su certificado.

PASO A PASO

- 1** Escribe un nombre para el servidor y pulsa **Pedir código** 2.

- 2

Copia la línea que aparece y pégala en la terminal de ese servidor. El código vale 15 minutos.
- 3

Cuando el servidor aparezca en **Nodos**, enciéndelo y elige qué expone.

REGLA DEL SISTEMA

El código se guarda cifrado y se quema al usarse. Si caducó, pide otro: el anterior deja de servir.

Tabla 8. Qué hace cada elemento de «Unir un servidor externo» · los usan: Administradores de la organización

Elemento	Qué hace
Unir un servidor externo	Alta de un servidor que no aprovisionó SIAC: le das un nombre, pides un código y pegas el comando que aparece en ese servidor.
Pedir código	Emite un código de un solo uso (15 minutos) y el comando que se ejecuta en el servidor externo para unirlo a la malla con su certificado.

CAPÍTULO 10

Agentes que aceptan tareas

Cada agente publicado, con su tarjeta A2A

DÓNDE ESTÁ	DIRECCIÓN
Malla	/malla
QUIÉN LA USA	CUÁNDO USARLA
Administradores de la organización	Cuando otro sistema u otro agente debe delegarle trabajo a uno de tus agentes.

Los agentes publicados del Centro de Agentes que puedes usar aparecen aquí 1 con su tarjeta A2A: nombre, habilidades y la dirección a la que otro sistema envía una tarea. El agente trabaja con su modelo y su presupuesto, y la tarea queda en el ledger. Por la puerta MCP cada uno se ve además como la herramienta agente__<slug>.

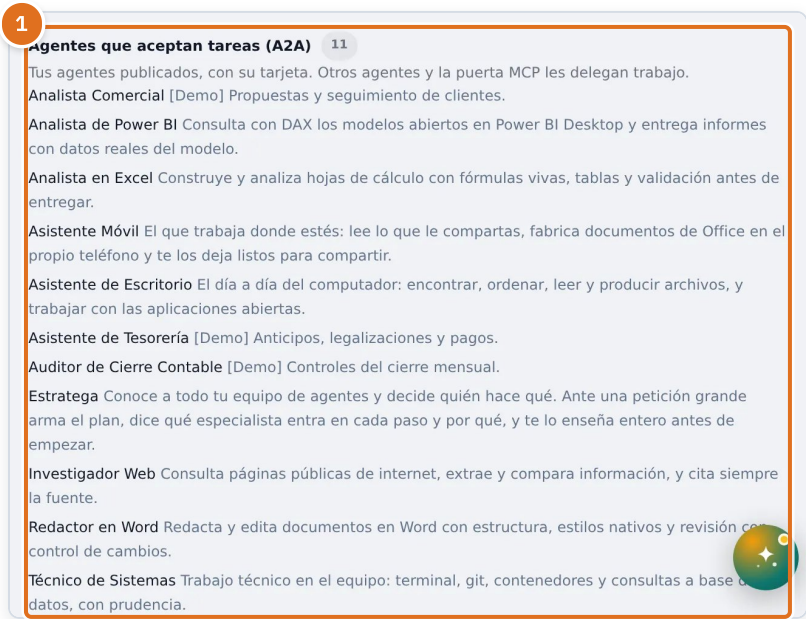


Figura 8. Los agentes que aceptan tareas de otros sistemas.

- 1 Agentes que aceptan tareas (A2A).** Tus agentes publicados con su tarjeta A2A: otros agentes y la puerta MCP pueden delegarles trabajo. Se publican desde el Centro de agentes.

Tabla 9. Qué hace cada elemento de «Agentes que aceptan tareas» · los usan: Administradores de la organización

Elemento	Qué hace
Agentes que aceptan tareas (A2A)	Tus agentes publicados con su tarjeta A2A: otros agentes y la puerta MCP pueden delegarles trabajo. Se publican desde el Centro de agentes.

CAPÍTULO 11

El ledger

Quién pidió qué, por dónde y qué pasó

DÓNDE ESTÁ

Malla

QUIÉN LA USA

Administradores de la organización

DIRECCIÓN

/malla

CUÁNDO USARLA

Para auditar: qué se ejecutó en tus servidores, quién lo pidió y con qué resultado.

Cada invocación —desde la pantalla, desde un agente, por MCP o desde otro nodo— deja una fila 1: cuándo, nodo, herramienta, riesgo, vía, quién (persona, agente o nodo) y resultado 2. No se borra con la retención normal: es la memoria de tu malla.

1

2

CUÁNDO	NODO	HERRAMIENTA	RIESGO	VÍA	QUIÉN	RESULTADO	MS
26/9/2026, 9:15:35 p. m.	Portal de clientes	pedidos.consultar	safe	api	Analista Comercial	ok	180
26/9/2026, 8:21:35 p. m.	Portal de clientes	clientes.buscar	sensitive	mcp	Analista Comercial	ok	240
26/9/2026, 7:27:35 p. m.	Servidor de automatizaciones	flujos.listar	safe	nodo	nodo:Portal de clientes	ok	95
26/9/2026, 6:33:35 p. m.	Servidor de automatizaciones	flujos.ejecutar	outbound	nodo	nodo:Portal de clientes	ok	2100
26/9/2026, 5:39:35 p. m.	Portal de clientes	correo.enviar_cotizacion	outbound	mcp	Analista Comercial	pendiente	—
26/9/2026, 4:45:35 p. m.	Bodega Medellín (servidor externo)	inventario.consultar	safe	airo	persona	error	20000
26/9/2026, 3:51:35 p. m.	Bodega Medellín (servidor externo)	inventario.ajustar_existencias	destructive	api	Auditor de Cierre Contable	pendiente	—
26/9/2026, 2:57:35 p. m.	Portal de clientes	precios.actualizar_lista	overwrite	api	persona	ok	640
26/9/2026, 2:03:35 p. m.	Portal de clientes	pedidos.anular	destructive	api	persona	ok	410
26/9/2026, 1:09:35 p. m.	Servidor de automatizaciones	flujos.ejecutar	outbound	mcp	Asistente de Tesorería	negada	—
26/9/2026, 12:15:35 p. m.	Portal de clientes	correo.enviar	outbound	nodo	nodo:Portal de clientes	ok	850
26/9/2026, 11:21:35 a. m.	Portal de clientes	respaldo.subir	outbound	nodo	nodo:Portal de clientes	ok	60
26/9/2026, 10:27:35 a. m.	Portal de clientes	sistema.reiniciar_servicio	destructive	api	persona	negada	—
26/9/2026, 9:33:35 a. m.	Portal de clientes	a2a.analista-comercial	outbound	api	Analista Comercial	ok	5400
26/9/2026, 8:39:35 a. m.	Portal de clientes	pedidos.consultar	safe	api	Analista Comercial	ok	180
26/9/2026, 7:45:35 a. m.	Portal de clientes	clientes.buscar	sensitive	mcp	Analista Comercial	ok	240
26/9/2026, 6:51:35 a. m.	Servidor de automatizaciones	flujos.listar	safe	nodo	nodo:Portal de clientes	ok	95
26/9/2026, 5:57:35 a. m.	Servidor de automatizaciones	flujos.ejecutar	outbound	nodo	nodo:Portal de clientes	ok	2100
26/9/2026, 5:03:35 a. m.	Portal de clientes	correo.enviar_cotizacion	outbound	mcp	Analista Comercial	pendiente	—
26/9/2026, 4:09:35 a. m.	Bodega Medellín (servidor externo)	inventario.consultar	safe	airo	persona	error	20000
26/9/2026, 3:15:35 a. m.	Bodega Medellín (servidor externo)	inventario.ajustar_existencias	destructive	api	Auditor de Cierre Contable	pendiente	—
26/9/2026, 2:21:35 a. m.	Portal de clientes	precios.actualizar_lista	overwrite	api	persona	ok	640
26/9/2026, 1:27:35 a. m.	Portal de clientes	pedidos.anular	destructive	api	persona	ok	410
26/9/2026, 12:33:35 a. m.	Servidor de automatizaciones	flujos.ejecutar	outbound	mcp	Asistente de Tesorería	negada	—
25/9/2026, 11:39:35 p. m.	Portal de clientes	correo.enviar	outbound	nodo	nodo:Portal de clientes	ok	8
25/9/2026, 10:45:35 p. m.	Portal de clientes	respaldo.subir	outbound	nodo	nodo:Portal de clientes	ok	60

Figura 9. Las últimas llamadas de la malla.

- 1

Ledger. Registro de cada herramienta invocada: quién, por qué vía, con qué riesgo y qué pasó.
- 2

Cuándo · Nodo · Herramienta · Riesgo · Vía · Quién · Resultado. Tabla de las últimas 50 llamadas; la columna Resultado dice si terminó bien, quedó pendiente o falló.

Tabla 10. Qué hace cada elemento de «El ledger» · los usan: Administradores de la organización

Elemento	Qué hace
Ledger	Registro de cada herramienta invocada: quién, por qué vía, con qué riesgo y qué pasó.
Cuándo · Nodo · Herramienta · Riesgo · Vía · Quién · Resultado	Tabla de las últimas 50 llamadas; la columna Resultado dice si terminó bien, quedó pendiente o falló.

CAPÍTULO 12

La puerta MCP

Una sola dirección para Claude Code, Open Code, Airo y tus agentes

DÓNDE ESTÁ	DIRECCIÓN
Malla	/malla
QUIÉN LA USA	CUÁNDO USARLA
Administradores de la organización	Cuando conectas una herramienta de desarrollo o un agente externo a tus servidores.

La Malla habla MCP (Streamable HTTP) en `https://ia.siac.com.co/api/v1/malla/mcp`. Se entra con una clave de API de [Ajustes](#) o con tu sesión, y cada persona ve exactamente lo que vería en la pantalla: sus nodos, las herramientas que exponen y los agentes que puede usar.

Ejemplo para Claude Code:

```
claude mcp add --transport http siac \
https://ia.siac.com.co/api/v1/malla/mcp \
--header "Authorization: Bearer sk-TU-CLAVE"
```

Dentro de un servidor de Dev Studio no hace falta clave: el agente deja un portador propio del nodo que solo ve su propia malla y las rutas que le concedieron.

REGLA DEL SISTEMA

Lo que toca facturación, credenciales o el plano de instancias no pasa por la puerta MCP.

CAPÍTULO 13

Preguntas frecuentes

¿Esto cambia mis agentes o playbooks en producción?

No. La Malla es una capa aparte: nada de lo que ya corre pasa por ella salvo que tú lo conectes.

¿Por qué no veo el servidor donde corre mi instancia SIAC?

Porque aloja instancias dedicadas y está excluido por diseño.

¿Puede un agente destruir algo por su cuenta?

No: cualquier herramienta destructiva exige que una persona apruebe esos argumentos exactos, y la aprobación caduca en 10 minutos.

¿Qué ve otro servidor del mío?

Solo lo que una ruta le concede, mientras la ruta exista.

¿Necesito abrir puertos?

No. Los nodos salen hacia SIAC; nadie entra a ellos.