



CENTRO DE CONFIANZA

# Ficha técnica del conector de red

Qué conexiones abre, qué viaja por ellas, cómo se autentica y cómo se revoca. Para el equipo de redes y de seguridad del Cliente.

| Versión | Fecha                    | Vigencia                        | Acceso            | Contacto                                                     |
|---------|--------------------------|---------------------------------|-------------------|--------------------------------------------------------------|
| 1.0     | 25 de septiembre de 2026 | Desde la disponibilidad general | Documento público | <a href="mailto:security@igniten.io">security@igniten.io</a> |

**Vigencia.** Este documento describe el servicio Igniten tal como se presta desde su disponibilidad general. Entra en vigor en la fecha en que la plataforma esté disponible comercialmente y rige para cada Cliente desde que celebra el contrato. Hasta entonces se publica solo con fines informativos y no genera obligaciones para ninguna de las partes.

## 1. Qué es y para qué sirve

El conector es un contenedor que su equipo instala y opera dentro de su propia red. Permite que Igniten consulte **las bases de datos que su equipo declare**, y nada más.

Correo, almacenamiento de archivos, reuniones, mensajería y los sistemas de gestión en la nube llegan a Igniten por las interfaces de sus respectivos proveedores, sobre internet, y no pasan por el conector. Una organización que decide no instalarlo pierde la consulta a sus bases internas; no pierde el producto.

Esta ficha está escrita para que su equipo pueda aprobar o rechazar el conector sin una reunión con nosotros. Cada afirmación tiene, en la sección 12, una forma de comprobarla desde su lado.

El código del conector está disponible para que su equipo de seguridad lo revise: se entrega a pedido, bajo acuerdo de confidencialidad. La imagen de contenedor es pública, está firmada y lleva adjunto su inventario de componentes. Le pedimos a su equipo que la verifique, no que confíe.

## 2. Requisitos de red

| Requisito                              | Valor                                                                                                                                                                 |
|----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Dirección de las conexiones            | Solo salientes, desde su red hacia Igniten                                                                                                                            |
| Puerto y protocolo                     | 443/TCP, TLS                                                                                                                                                          |
| Reglas de entrada en su cortafuegos    | Ninguna                                                                                                                                                               |
| Servicios suyos publicados en internet | Ninguno                                                                                                                                                               |
| Destinos de salida                     | Dos nombres públicos del dominio de Igniten: uno que se usa una sola vez, en el alta, y otro permanente para el túnel. Ambos figuran en el instructivo de instalación |
| Resolución de nombres                  | La de su red, para los destinos que su equipo declara                                                                                                                 |

Desde el lado de Igniten **no se inicia ninguna conexión hacia su red**. El conector no abre ningún puerto a la escucha: no acepta conexiones entrantes de ningún origen.

Si alguien le pide abrir un puerto de entrada para Igniten, algo está mal configurado.

## 3. El protocolo

### 3.1 El canal

Toda comunicación entre el conector e Igniten viaja por **TLS con autenticación mutua por certificado**. Las versiones obsoletas del protocolo se rechazan en ambos extremos.

- El conector verifica la identidad del extremo de Igniten contra una **autoridad de certificación exclusiva de los conectores**, que recibe en el alta, y contra el nombre esperado. No usa el almacén público de autoridades.
- El extremo de Igniten exige el certificado del conector y lo verifica contra la misma autoridad. Esa autoridad no firma ninguna otra cosa.
- El cifrado TLS se termina en un único componente de Igniten, que es el único que ve el certificado del conector. Los equipos de red intermedios lo dejan pasar sin terminarlo.

### 3.2 Los tipos de conexión

Cada conexión declara su propósito en el primer mensaje, y solo puede ser una de tres:

| Tipo       | Qué lleva el conector                                          | Qué responde Igniten                                            | Después                                            |
|------------|----------------------------------------------------------------|-----------------------------------------------------------------|----------------------------------------------------|
| Túnel      | Nada más que el tipo                                           | Que el túnel queda en espera                                    | El túnel queda ocioso hasta que llega una petición |
| Latido     | Su versión y los <b>nombres lógicos</b> que declara su archivo | Que la instancia está viva, y los pedidos de destino pendientes | Se cierra                                          |
| Renovación | Una solicitud de certificado nueva                             | El certificado renovado                                         | Se cierra                                          |

Una conexión de un conector no reconocido recibe un rechazo y se cierra. Hacia afuera, todos los rechazos de identidad usan el mismo texto, para que no sirvan como oráculo sobre qué organizaciones son clientes de Igniten.

Los nombres lógicos que viajan en el latido son los que su equipo eligió en el archivo de destinos (sección 5). Nunca viajan máquinas ni puertos.

### 3.3 La petición

Por un túnel ocioso, Igniten envía **un único dato: el nombre lógico del destino**. Es el único campo que existe; cualquier otro campo hace rechazar la petición, no se ignora.

No hay campo para una máquina ni para un puerto. Un destino que su equipo no declaró no es un destino rechazado: es un destino que no se puede expresar.

El conector busca ese nombre en **su** archivo:

- si no está declarado, rechaza la petición, lo registra y no abre ninguna conexión;
- si está declarado y la base responde, confirma la apertura y desde ese momento el túnel transporta los bytes del protocolo de la base, sin que el conector los mire ni los altere;

- si está declarado y la base no responde, rechaza con un motivo genérico. La máquina y el puerto quedan solo en el registro local de su conector.

Cada túnel sirve **una sola consulta** y se cierra; el conector mantiene algunos túneles ociosos y vuelve a abrir otro enseguida. No hay multiplexado: el dominio de falla es una consulta, y las filas de una consulta no pueden cruzarse con las de otra.

### 3.4 Qué viaja

| Sentido            | Qué viaja                                                                                                             |
|--------------------|-----------------------------------------------------------------------------------------------------------------------|
| Igniten → conector | El nombre lógico del destino; después, el protocolo de la base (la consulta)                                          |
| Conector → Igniten | Las filas y los errores que devuelve su base; el latido, con la versión del conector y los nombres lógicos declarados |
| Entre conectores   | Nada                                                                                                                  |

El asistente de Igniten solo genera consultas de lectura y rechaza cualquier escritura antes de que salga. La garantía que su equipo puede exigir, y que vale aunque Igniten fallara, es que la credencial que crea en su base sea **de solo lectura** (ver sección 11).

## 4. Autenticación: una identidad por instancia

Cada instancia del conector tiene **su propio certificado**, que la identifica a ella y a su organización. Retirar una instancia no afecta a ninguna otra, ni de su organización ni de otra.

### 4.1 Alta

1. Un administrador de su organización genera un **token de alta** en el panel. Es de un solo uso y vence si no se usa. Igniten guarda solo un resumen del token, nunca el token.
2. Al arrancar por primera vez, el conector **genera su propia clave privada** en el volumen que su equipo le asigna, legible solo por el proceso del conector.
3. El conector envía el token, el nombre de la instancia y una **solicitud de firma de certificado** en formato estándar, que contiene solo la clave pública.
4. Igniten firma, con la autoridad de conectores, un certificado que dice **a qué organización pertenece y cuál es la instancia**, habilitado solo para autenticarse como cliente. De la solicitud se toma la clave pública y nada más.
5. El conector recibe el certificado y la autoridad de certificación.

**La clave privada nunca sale de su red.** Igniten no la genera, no la ve y no la guarda.

### 4.2 Doble comprobación en cada conexión

1. El certificado tiene que verificar contra la autoridad de conectores.

2. Igniten consulta además su **registro de conectores vigentes**: esa organización, esa instancia, esa huella de certificado, y que la instancia no esté retirada.

El certificado dice quién era el conector el día que se emitió; el registro dice quién es hoy. Un certificado válido de un conector retirado pasa la primera comprobación y no la segunda. Si el registro no se puede consultar, el conector no se identifica: **falla cerrado**.

## 5. Ciclo de vida de la credencial

| Etapa      | Qué pasa                                                                                                                                                                                                   |
|------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Emisión    | En el alta, a partir de la clave que genera el propio conector (sección 4.1)                                                                                                                               |
| Vigencia   | Los certificados son de vida corta                                                                                                                                                                         |
| Renovación | Antes del vencimiento, el conector genera <b>una clave nueva</b> y pide la renovación por el propio túnel, autenticado con el certificado vigente. El token de alta ya no sirve para nada después del alta |
| Reemplazo  | Al renovarse, el certificado anterior deja de ser aceptado                                                                                                                                                 |
| Revocación | Retirar la instancia la saca del registro de conectores vigentes; su certificado deja de ser aceptado aunque no haya vencido (sección 8)                                                                   |

La renovación es automática y no requiere intervención de su equipo.

## 6. La lista de destinos: un archivo suyo

La lista de lo que Igniten puede alcanzar dentro de su red es **un archivo que vive en su infraestructura**, junto al conector, montado en modo de solo lectura. Solo su equipo lo edita. Igniten no tiene forma de agregarle nada: ni desde el panel, ni desde el protocolo, ni desde su plano de control.

La lista se **aplica del lado del conector**. Aunque el plano de control de Igniten estuviera comprometido, no existe un camino por el que Igniten pueda ampliar su alcance dentro de su red. No es una promesa de conducta: es una imposibilidad técnica.

### 6.1 Formato

El archivo usa el formato estándar `TOML`. Cada destino es una sección cuyo nombre es el nombre lógico:

| Campo                | Obligatorio | Qué es                                                                     |
|----------------------|-------------|----------------------------------------------------------------------------|
| Nombre de la sección | Sí          | El nombre lógico que Igniten pide. Minúsculas, dígitos, guion y guion bajo |
| Máquina              | Sí          | Nombre o dirección de la base, resuelto en su red                          |
| Puerto               | Sí          | Puerto de la base                                                          |
| Para qué             | Sí          | Descripción libre, para su propio control                                  |

Reglas del archivo:

- **Claves cerradas.** Una clave desconocida, o una faltante, invalida el archivo entero.
- **Se lee al arrancar,** y la huella del archivo queda en el registro local.
- **Falla cerrado.** Si el archivo falta o está mal escrito, no hay ningún destino alcanzable, y el motivo queda en el registro. Nunca al revés.
- **Declare pares máquina–puerto, no rangos.**

## 6.2 Pedidos de destino

Si Igniten necesita un destino nuevo, lo **pide**. El pedido aparece en el registro local del conector y en su panel, y **no surte efecto** hasta que alguien de su equipo lo agrega al archivo y reinicia el conector. No existe forma de aprobarlo desde el panel de Igniten, a propósito.

## 6.3 Igniten no aprende su topología

Del lado de Igniten se direcciona un nombre lógico; la resolución ocurre en su red. Igniten no almacena rangos, nombres de máquina ni rutas de su red.

# 7. Aislamiento en la infraestructura de Igniten

Cada conector tiene **su propio espacio de red** del lado de Igniten. Cada túnel es un canal cifrado propio, ligado a la identidad de una instancia, y no existe una red compartida entre conectores.

- Un conector no puede alcanzar los destinos ni los túneles de otro conector, ni de su organización ni de otra.
- Las peticiones que Igniten envía por un túnel corresponden exclusivamente a la organización dueña de ese conector. Esta separación forma parte de la batería de pruebas de aislamiento entre organizaciones que Igniten corre de forma permanente.

# 8. Procedimiento de revocación

| Quién     | Cómo                                       | Efecto                                                                                                                            |
|-----------|--------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|
| Su equipo | Detener el contenedor                      | Inmediato. La conexión es suya                                                                                                    |
| Su equipo | Quitar un destino del archivo y reiniciar  | Ese destino deja de ser alcanzable                                                                                                |
| Su equipo | <b>Retirar</b> la instancia desde el panel | Se cortan de inmediato todos los túneles de esa instancia, <b>incluso con una consulta en curso</b> , y todo reintento se rechaza |
| Igniten   | Retirar la instancia                       | El mismo efecto; su organización queda notificada en el panel                                                                     |

Para retirar una instancia comprometida sin afectar a las demás:

1. Retire la instancia desde el panel. Sus túneles se cortan y su certificado deja de aceptarse.
2. Detenga el contenedor y elimine el volumen que guarda su identidad.
3. Si va a reemplazarla, genere un token de alta nuevo y dé de alta una instancia con otro nombre.

Las demás instancias de su organización siguen operando sin cambios.

## 9. Comportamiento ante caída

| Situación                                              | Qué pasa                                                                                                                                        |
|--------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| El conector no llega a Igniten                         | Reintenta solo, con espera creciente entre intentos. El panel lo muestra como caído cuando deja de recibir latidos                              |
| Llega una consulta y no hay conector conectado         | Quien pregunta recibe de inmediato un aviso claro de que el conector no está conectado y cómo se resuelve. No hay espera hasta agotar el tiempo |
| Igniten reinicia el componente que termina los túneles | Los túneles se cortan y el conector vuelve a conectarse solo                                                                                    |
| El registro de conectores vigentes no responde         | Ningún conector se identifica: falla cerrado                                                                                                    |
| Su base no responde                                    | Queda como inalcanzable en el registro local, con máquina y puerto; hacia Igniten sale solo un motivo genérico                                  |
| El archivo de destinos falta o es inválido             | Cero destinos alcanzables, con el motivo en el registro                                                                                         |

En ningún caso una falla amplía lo que el conector puede alcanzar.

## 10. El registro del conector

El conector escribe un evento por línea, en formato estructurado, en la salida estándar del contenedor. Es **local y primario**: no depende de que Igniten esté disponible.

| Evento                  | Cuándo                                                                                |
|-------------------------|---------------------------------------------------------------------------------------|
| Arranque                | Al cargar el archivo de destinos, con los nombres declarados y la huella del archivo  |
| Lista vacía o ilegible  | Cuando el archivo no declara destinos o no se puede interpretar                       |
| Paso                    | Cuando se abre un destino declarado (con máquina y puerto, solo en el registro local) |
| Rechazo                 | Cuando Igniten pide un destino no declarado                                           |
| Inalcanzable            | Cuando un destino declarado no responde (con máquina y puerto, solo local)            |
| Alta                    | Resultado del canje del token                                                         |
| En línea / sin conexión | Cambios de estado del túnel, con el motivo                                            |

| Evento     | Cuándo                                          |
|------------|-------------------------------------------------|
| Renovación | Resultado de cada renovación del certificado    |
| Solicitud  | Un pedido de destino nuevo por parte de Igniten |

Hacia Igniten salen solo nombres lógicos y motivos; **nunca máquinas ni puertos**. Los rechazos también quedan visibles en el panel de su organización.

## 11. La imagen y cómo ejecutarla

### 11.1 Cadena de suministro

- La imagen se publica en un registro público de contenedores y se referencia **por su huella**, nunca por una etiqueta móvil. El instructivo de instalación trae la huella exacta.
- Está **firmada** con una clave de Igniten. La clave pública de verificación se entrega en el panel de su organización, junto al instructivo de instalación y la huella exacta de la imagen, y la firma se verifica con herramientas estándar de firma de contenedores.
- Lleva adjunto su **inventario de componentes** en formato estándar `SPDX`, también firmado.
- Su equipo puede **fixar una versión** en lugar de aceptar actualizaciones automáticas.
- La imagen se construye sobre una base mínima fijada por huella, con el menor número posible de dependencias de terceros, instaladas con verificación de integridad.

### 11.2 Permisos que necesita

| Aspecto                                                                         | Requisito                                                               |
|---------------------------------------------------------------------------------|-------------------------------------------------------------------------|
| Usuario                                                                         | Sin privilegios, no administrador                                       |
| Modo privilegiado, capacidades de red, dispositivos de túnel, red del anfitrión | No los necesita                                                         |
| Capacidades del sistema                                                         | Ninguna: puede correr con todas las capacidades retiradas               |
| Sistema de archivos                                                             | Puede ser de solo lectura                                               |
| Montajes                                                                        | El archivo de destinos, en solo lectura, y un volumen para su identidad |
| Salida                                                                          | 443/TCP hacia los dos nombres del instructivo                           |

Recomendamos correrlo sin acceso al resto de su red más allá de los destinos declarados.

### 11.3 Del lado de su base

- Cree un rol dedicado a Igniten, distinto de cualquier rol de persona o de aplicación.

- Concédale **solo lectura**, y solo sobre los esquemas, tablas o vistas que hagan falta.
- Considere vistas sin las columnas sensibles que no aportan al análisis.
- Acote en el motor el tiempo máximo de sentencia y el número de conexiones de ese rol.

## 11.4 Si prefiere no instalar nada de Igniten

Hay alternativas documentadas, sin depender de ningún intermediario contratado: red privada virtual estándar contra la puerta de enlace de Igniten, o conexión directa cifrada con lista de direcciones autorizadas si su base ya está en la nube. Igniten le entrega el procedimiento de cada una, junto con sus direcciones de salida fijas.

## 12. Cómo comprobarlo su equipo

| Afirmación                                   | Cómo se comprueba                                                                                                                   |
|----------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------|
| Igniten nunca inicia conexiones hacia su red | Cero reglas de entrada en su cortafuegos, y el conector funciona igual                                                              |
| Solo sale por 443 hacia dos nombres          | Los registros de salida de su cortafuegos                                                                                           |
| Un destino declarado se alcanza              | Declárelo, reinicie y consulte desde el producto                                                                                    |
| <b>Un destino no declarado se rechaza</b>    | Pida una consulta a una base que no esté en el archivo: tiene que fallar y aparecer como rechazo en el registro local y en su panel |
| No necesita privilegios                      | Córralo sin capacidades y con sistema de archivos de solo lectura: funciona                                                         |
| La clave privada no sale de su red           | La clave está en el volumen del conector; el alta solo envía una solicitud con la clave pública                                     |
| Retirar corta de verdad                      | Retire la instancia en el panel con una consulta en curso: se corta y el reintento se rechaza                                       |
| La imagen es la de Igniten                   | Verifique la firma y el inventario de componentes con la clave pública que le entrega el panel                                      |
| El código hace lo que dice esta ficha        | Pida el código para revisión, bajo acuerdo de confidencialidad                                                                      |

**Compruebe el rechazo en las dos direcciones.** Un sistema que rechaza todo, incluido lo autorizado, se ve igual que uno que aplica bien la lista.