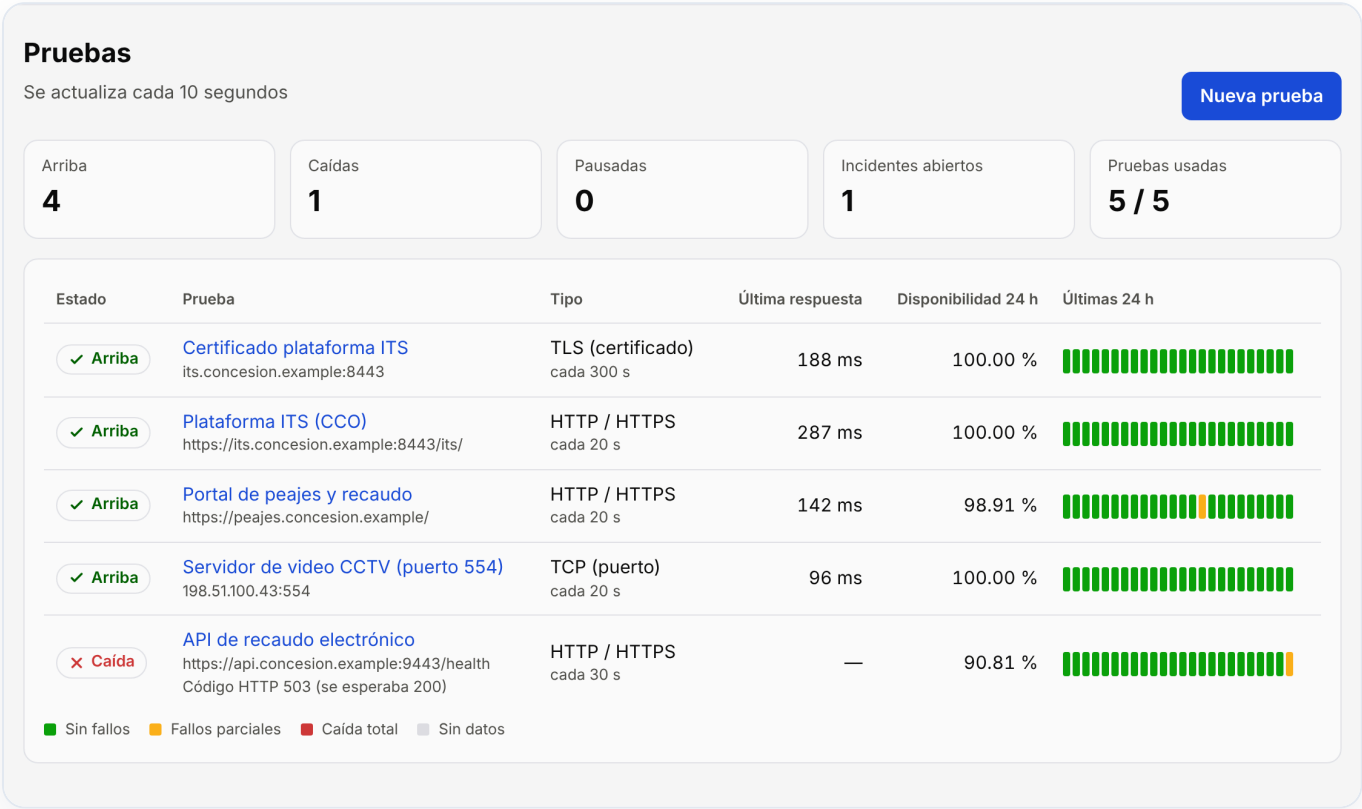
Sus sistemas ITS, vigilados cada 20 segundos

ITSAnalytics comprueba desde Internet que las plataformas ITS de su concesión vial siguen respondiendo —centro de control (CCO), peajes y recaudo, video, atención al usuario— y avisa al instante cuando una cae y cuando se recupera.



HTTP / HTTPS

¿La plataforma ITS responde? Comprueba la aplicación en su puerto estándar o en uno específico (por ejemplo 8443).

TCP (puerto)

¿El servidor está alcanzable? Verifica que la IP pública y el puerto del servicio —video, VPN, base de datos— aceptan conexiones.

Certificado TLS

¿El certificado sigue vigente? Avisa con días de anticipación, antes de que el portal aparezca como «no seguro».

Qué se vigila en una concesión

- **Plataforma de gestión ITS** y aplicaciones del CCO.
- **Peajes y recaudo**: portales y recaudo electrónico.
- **Video y CCTV**: servidores y pasarelas publicados.
- **Atención al usuario**: sitio web, PQR, estado de la vía.
- **Accesos remotos**: VPN hacia la red de campo.
- **Integraciones** con interventoría y entidades.

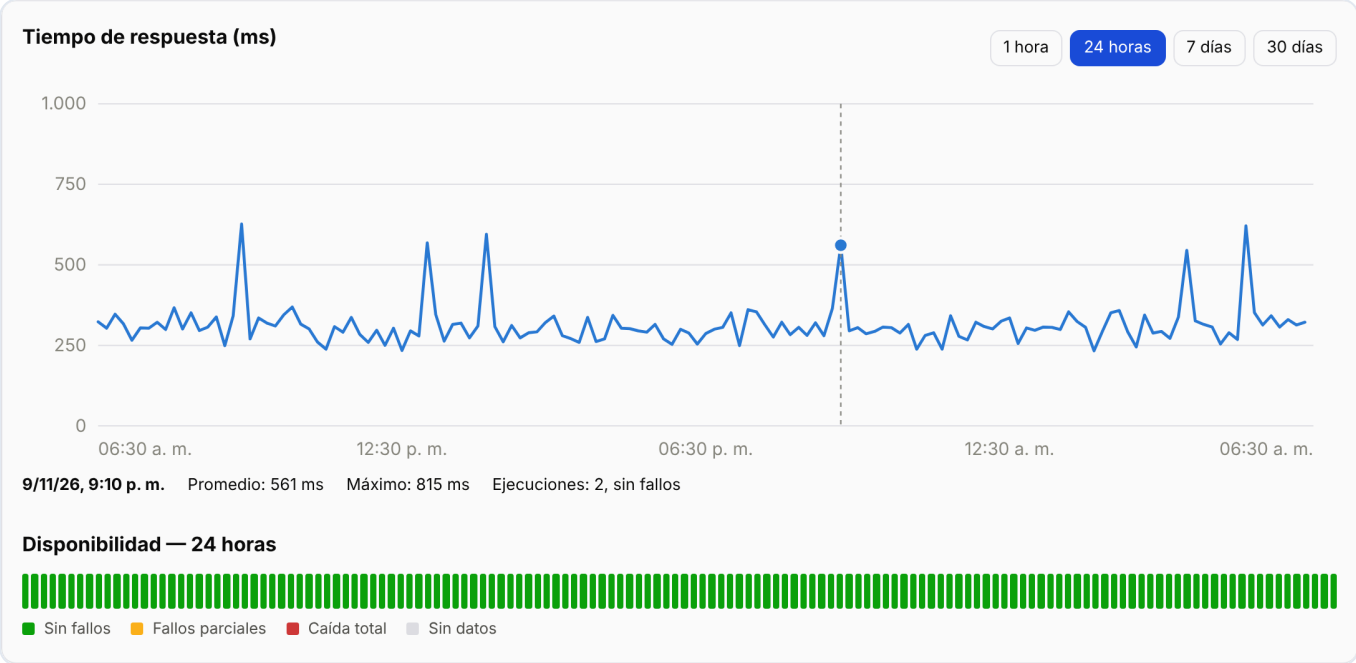
Alcance. Se vigilan servicios publicados en Internet (IP o dominio público). Los equipos de campo en redes privadas —paneles, postes SOS, básculas, cámaras— se vigilan a través de la plataforma o el servicio que los publica. El histórico de disponibilidad e incidentes sirve de soporte para los informes de operación.

Gráficas: qué pasó, cuándo y por cuánto tiempo

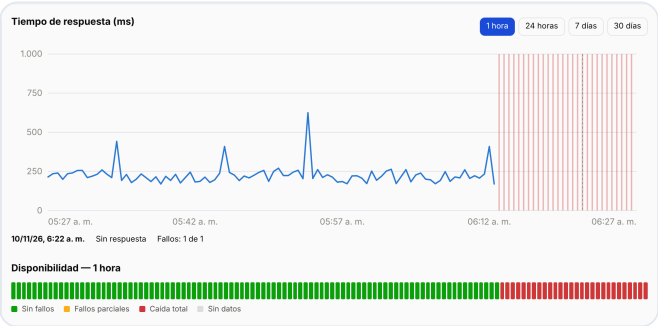
Cada sistema vigilado tiene su página de detalle con indicadores, tiempo de respuesta y disponibilidad en periodos de 1 hora, 24 horas, 7 días y 30 días. Al pasar el cursor se ve el detalle de cada momento.

Disponibilidad 24 h	Disponibilidad 7 días	Disponibilidad 30 días	Respuesta promedio 24 h	Certificado TLS
90.81 %	**97.48 %**	**99.38 %**	**235 ms**	**52 días**

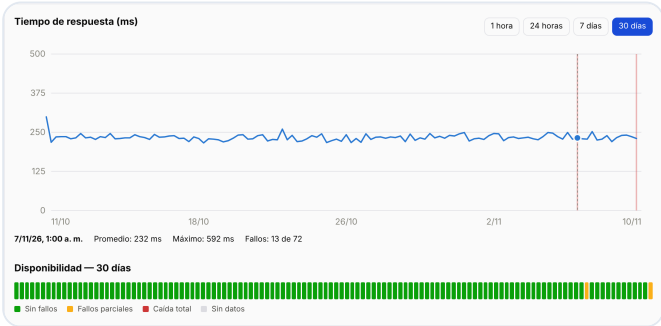
Indicadores. Disponibilidad a 24 horas, 7 días y 30 días, tiempo de respuesta promedio y días restantes del certificado.



Operación normal, 24 horas. La línea muestra el tiempo de respuesta; los picos revelan momentos de lentitud de la plataforma aunque no haya caído.



Caída en curso, 1 hora. Las franjas rojas marcan cada comprobación fallida; la tira inferior pasa de verde a rojo.



Tendencia, 30 días. Los incidentes pasados quedan a la vista: amarillo para fallos parciales, rojo para caída total.

Incidentes

Inicio	Fin	Duración	Causa
10/11/26, 6:13:11 a. m.	✕ Caída	14 min 4 s	Código HTTP 503 (se esperaba 200)
7/11/26, 4:27:11 a. m.	7/11/26, 5:27:11 a. m.	1 h 0 min	Código HTTP 503 (se esperaba 200)

Historial de incidentes. Inicio, fin, duración y causa de cada caída.

Alertas: el aviso llega al caer y al recuperarse

Cada concesión define a qué correos y a qué webhooks se avisa: el CCO, el equipo de tecnología o el proveedor del sistema. La caída se notifica una sola vez, cuando se confirma, y de nuevo cuando el servicio vuelve.

CAÍDA **[ITSAnalytics] CAÍDA: API de recaudo electrónico — Concesión Vial Demo**
Para: cco@concesion.example

```
La prueba "API de recaudo electrónico" está caída.
Destino: https://api.concesion.example:9443/health
Causa: Código HTTP 503 (se esperaba 200)
Inicio: 10/11/26, 6:13:11 a. m.
Detalle: https://…/o/concesion-demo/checks/…
```

RECUPERADA **[ITSAnalytics] RECUPERADA: Portal de peajes y recaudo — Concesión Vial Demo**
Para: cco@concesion.example

```
La prueba "Portal de peajes y recaudo" se
recuperó.
Destino: https://peajes.concesion.example/
Causa: Tiempo de espera agotado
Inicio: 9/11/26, 9:07:11 p. m.
Fin: 9/11/26, 9:27:11 p. m.
Duración: 20 min 0 s
Detalle: https://…/o/concesion-demo/checks/…
```

Correo. Texto de los avisos de caída y de recuperación, con el destino, la causa, las horas y el enlace al detalle.

```
POST https://mesa.concesion.example/hooks/its
{
  "event": "down",
  "organization": { "name": "Concesión Vial Demo", "slug": "concesion-demo" },
  "check": { "id": "…", "name": "API de recaudo electrónico", "type": "http",
             "target": "https://api.concesion.example:9443/health" },
  "incident": { "id": "…", "cause": "Código HTTP 503 (se esperaba 200)",
                "startedAt": "2026-11-10T11:13:11.000Z", "endedAt": null },
  "text": "La prueba \"API de recaudo electrónico\" está caída. …",
  "timestamp": "2026-11-10T11:13:11.412Z"
}
```

Webhook. El mismo aviso en formato JSON, para integrarlo con la mesa de ayuda, el chat del CCO o el sistema de guardias. El evento es down al caer y up al recuperarse.

Canales (2)

Tipo	Destino		
Correo	cco@concesion.example	Enviar prueba	Eliminar
Webhook	https://mesa.concesion.example/hooks/its	Enviar prueba	Eliminar

Canales. Correos y webhooks de la organización; cada uno se puede probar con un mensaje de prueba.

Últimos envíos

Hora	Evento	Destino	Resultado
10/11/26, 6:13:11 a. m.	Caída	https://mesa.concesion.example/hooks/its	Enviado
10/11/26, 6:13:11 a. m.	Caída	cco@concesion.example	Enviado

Registro de envíos. Queda constancia de cada aviso: hora, evento, destino y si se entregó.

PLAN MENSUAL · COLOMBIA

$1.000.000 COP / mes

No causa IVA: servicio de computación en la nube (art. 476, num. 21, Estatuto Tributario).

- **5 pruebas** de IP o dominios públicos
- Pruebas HTTP/HTTPS, TCP o certificado TLS, a su elección
- Intervalo configurable desde 10 s (20 s por defecto)
- Alertas por correo y webhook
- Panel, históricos e incidentes
- Usuarios con roles y segundo factor

Especificaciones

Tipos de prueba	HTTP y HTTPS (GET o HEAD), conexión TCP a un puerto, certificado TLS.
Destinos	Direcciones IP o dominios públicos, en puertos por defecto o específicos. No se monitorizan direcciones de redes privadas.
Frecuencia	Configurable por prueba entre 10 segundos y 1 hora; 20 segundos por defecto.
Validaciones HTTP	Códigos de respuesta esperados, texto esperado en la respuesta, certificado válido, tiempo de espera de 1 a 30 segundos.
Detección de caídas	Reintento a los 5 segundos; la caída se declara tras fallos consecutivos (2 por defecto, configurable de 1 a 10).
Alertas	Correo electrónico y webhook (HTTPS), al caer y al recuperarse, con causa y duración.
Métricas	Disponibilidad 24 h / 7 d / 30 d, tiempo de respuesta, días restantes del certificado. Resultados detallados conservados 30 días.
Usuarios y roles	Administrador, operador y lector por organización.
Seguridad de acceso	Segundo factor con aplicación de autenticación (TOTP) y códigos de recuperación; la organización puede exigirlo a todos sus usuarios. Bloqueo tras intentos fallidos.
Acceso	Servicio en la nube, desde el navegador en computador o móvil. Sin instalar agentes ni equipos.
Origen de las pruebas	Centro de datos en Estados Unidos (costa este).

Cómo empieza

1. Alta

Creamos la organización de su concesión y su administrador.

2. Pruebas

Pegue la URL de cada plataforma ITS, o indique IP y puerto.

3. Alertas

Añada los correos del CCO o el webhook de avisos.

Precio en pesos colombianos, facturación mensual. Pruebas adicionales a las 5 incluidas: según cotización. La prueba TCP comprueba un puerto abierto; no es un ping ICMP. Las capturas muestran datos de demostración.