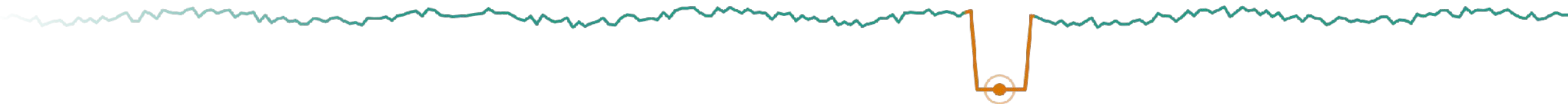




MONITOREO PARA MITIGAR MICROCORTES EN TOPOLOGÍAS ISP BASADAS EN MIKROTIK, MEDIANTE LENGUAJE NATURAL

Telemetría centralizada on-premise y diagnóstico en lenguaje natural con un LLM local



Joaquín T. Riedmaier · Santiago A. Zualet

Facultad de Ingeniería · Universidad Nacional de
Misiones Dir.: Ing. Xander Germán · Ing. De Sosa
Hector

La conectividad del interior la sostienen los ISPs locales



+1.500

ISPs PyME y cooperativas

invierten en infraestructura aún en contextos adversos

CABASE, 2025



12,99 M

accesos fijos a Internet

en todo el país

ENACOM, 4.º trim. 2025



82,6 %

de los hogares con internet fijo

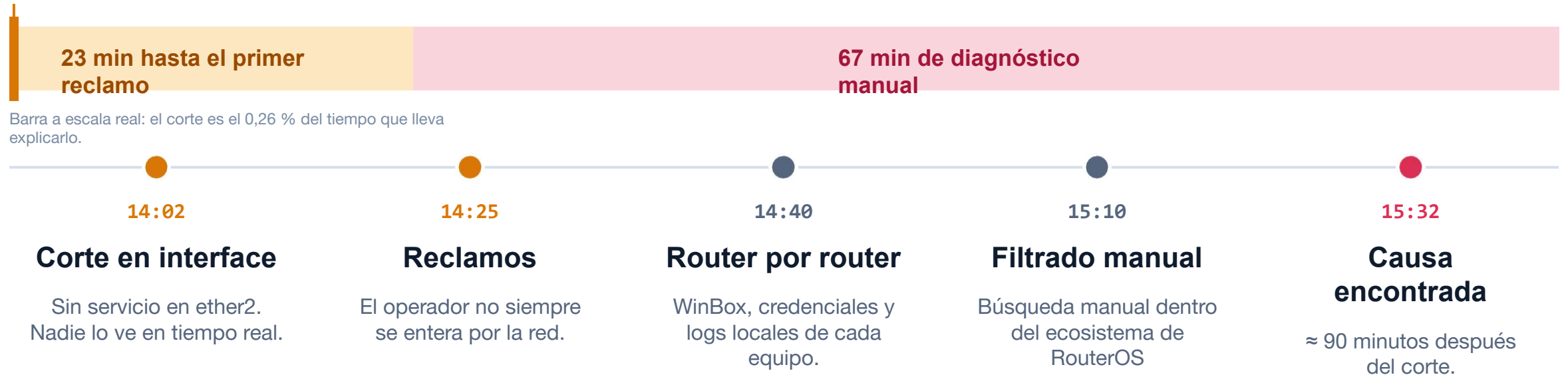
la exigencia de calidad crece con la penetración

CABASE Internet Index 2025

Diagnósticos reactivos lentos y falta de monitoreo preventivo

14 s de corte

≈ 90 min del corte a la causa



Recorrido típico estimado para un evento crítico. Horarios ilustrativos

¿Por qué tarda tanto?



Logs dispersos

Cada router guarda lo suyo y se pierde al reiniciar.



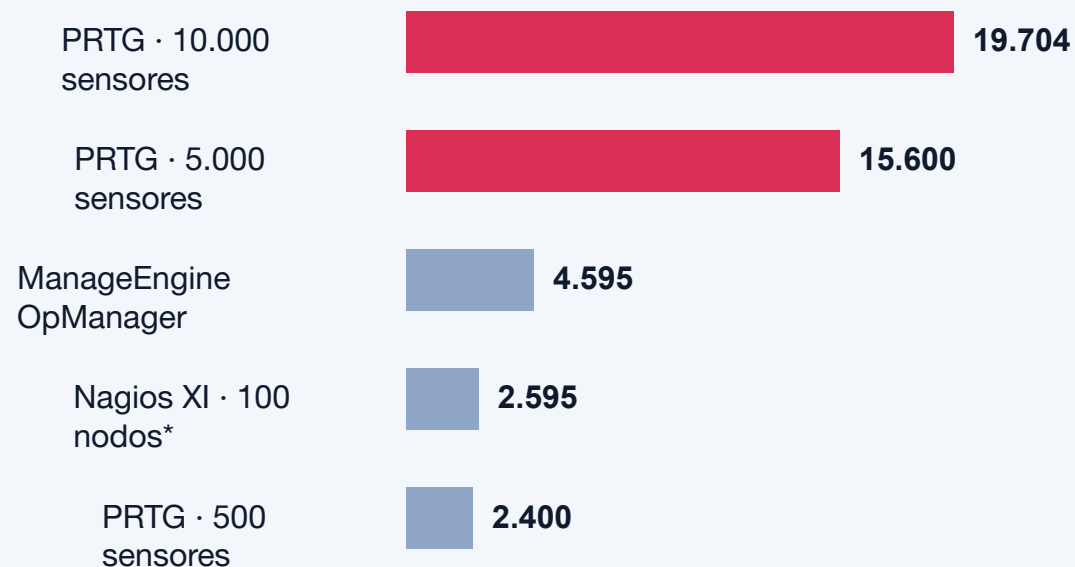
Ruido

Cientos de eventos irrelevantes tapan la causa raíz.

Soluciones que desatienden al grueso del sector

Herramientas empresariales quedan sobredimensionadas, mientras que las alternativas libres trasladan parte del costo al tiempo de ingeniería.

Licencias NMS corporativas · USD / año



Fuentes: listas de precios de Paessler (PRTG), ManageEngine (OpManager Enterprise, 250 dispositivos) y Nagios, consultadas en sep. 2026. *Nagios: licencia perpetua + ~20 % anual de soporte.



NMS corporativos

Licencia por sensor o nodo, sobredimensionados para un ISP PyME e interfaces que exigen certificación.



Open source y nativos

Sin licencia, pero el costo pasa a horas de ingeniería: plantillas SNMP a mano, capacitación oficial Zabbix de USD 2.450 a 6.750. The Dude: inestable al escalar.



Dos esferas, en el medio quedan +1.500 ISPs

sin una herramienta a su escala, ni en costo ni en complejidad.

Dos canales de recolección de datos, una sola fuente de verdad



PUSH · asíncrono

Syslog sobre UDP

- Eventos critical / error / warning
- Caídas y flapping de enlaces
- Desconexiones PPPoE / RADIUS
- Intentos fallidos SSH, WinBox, API



PULL · bajo demanda

API REST de RouterOS v7 (JSON)

- Tráfico, errores y descartes por interfaz / VLAN
- CPU y RAM de cada equipo
- Connection tracking y tabla ARP
- Sesiones activas por NAS

Vectores de análisis sobre esos datos



Telemetría RADIUS

estados y cortes de
abonados



Métricas L2 / L3

enlaces caídos,
paquetes perdidos



Auditoría contrack

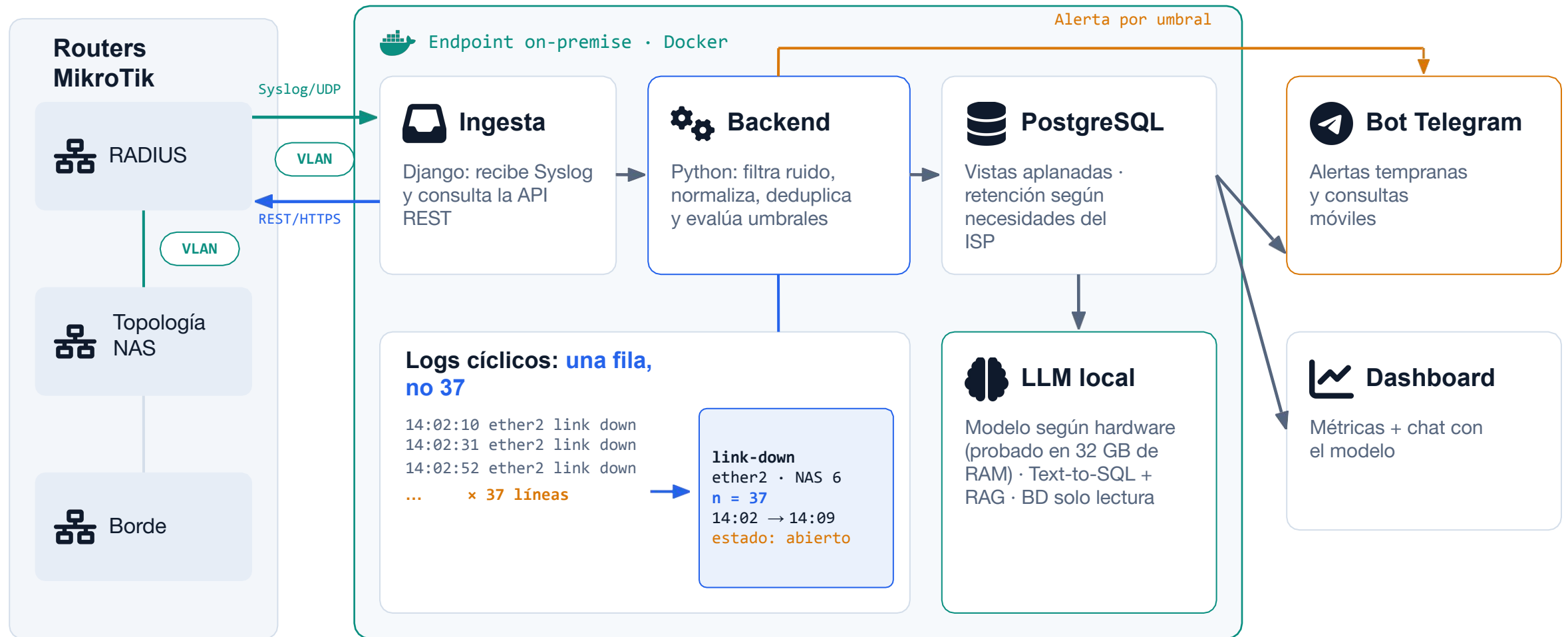
saturación y patrones
DDoS



Correlación topológica

causa raíz en fallas en
cascada

Todo corre en un nodo local, dentro del ISP



Preguntar en lenguaje natural, responder con datos



“¿Qué routers registraron caídas en las últimas 4 horas?”

SQL generado (solo lectura)

```
SELECT dispositivo, interfaz, count(*) AS caidas
FROM v_eventos_criticos
WHERE tipo = 'link-down' AND ts > now() - interval '4 hours'
GROUP BY 1, 2 ORDER BY caidas DESC;
```



“NAS 6 registró 7 caídas en ether2 entre 14:02 y 14:09: patrón de flapping. Afectó 23 sesiones PPPoE.”

Ejemplo
ilustrativo



Vistas aplanadas

El esquema se simplifica para el modelo: menos JOINS, menos alucinaciones.



Solo SELECT

Usuario de base de datos de solo lectura: el modelo no puede modificar nada.



Respuestas ancladas

RAG + system prompt: la respuesta se basa en filas reales. Meta: $\geq 95\%$.

Una incidencia se explica mejor cuando varias mediciones cuentan la misma historia

No es un resultado medido: es el tipo de correlación que el sistema busca soportar.

CORRELACIÓN

“¿Qué cambió entre 12:00 y 12:10 y qué señales aparecieron juntas?”

L2 / L3

errores en
ether2

Connection tracking

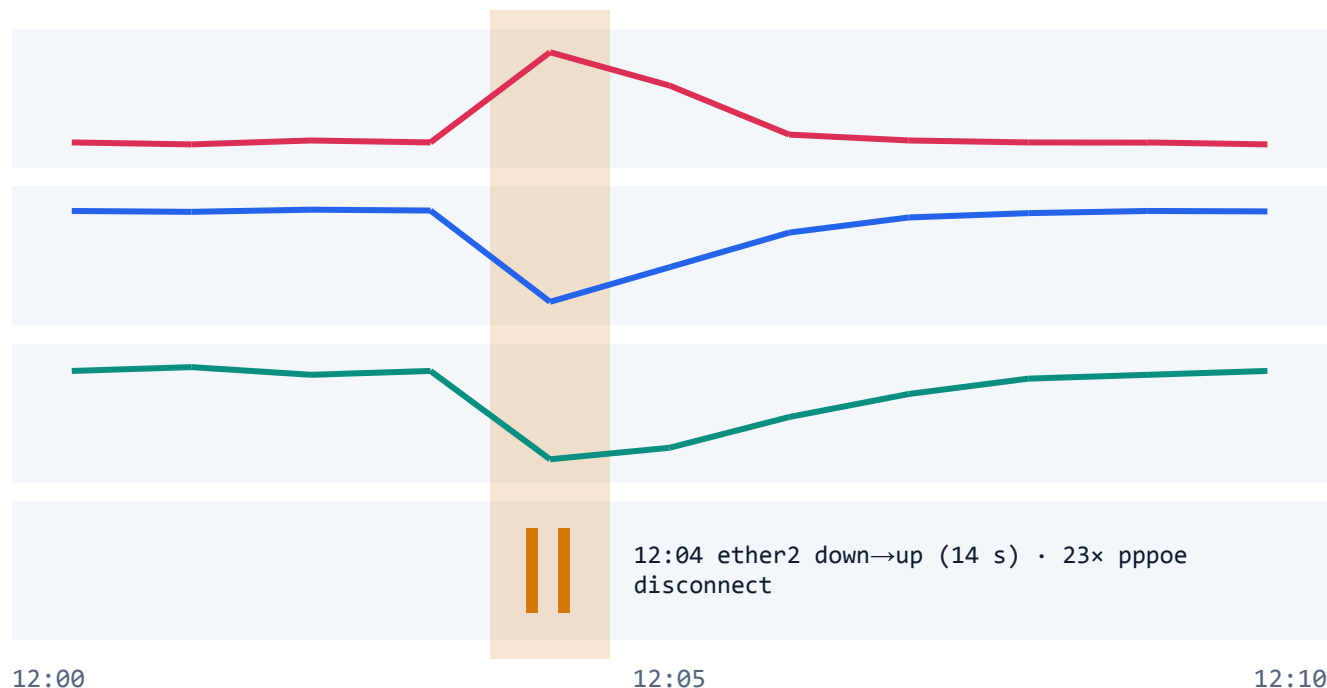
conexiones activas

RADIUS

sesiones
PPPoE

Logs

eventos
Syslog



Lectura correlada

Las cuatro señales cambian en el mismo minuto: 12:04.

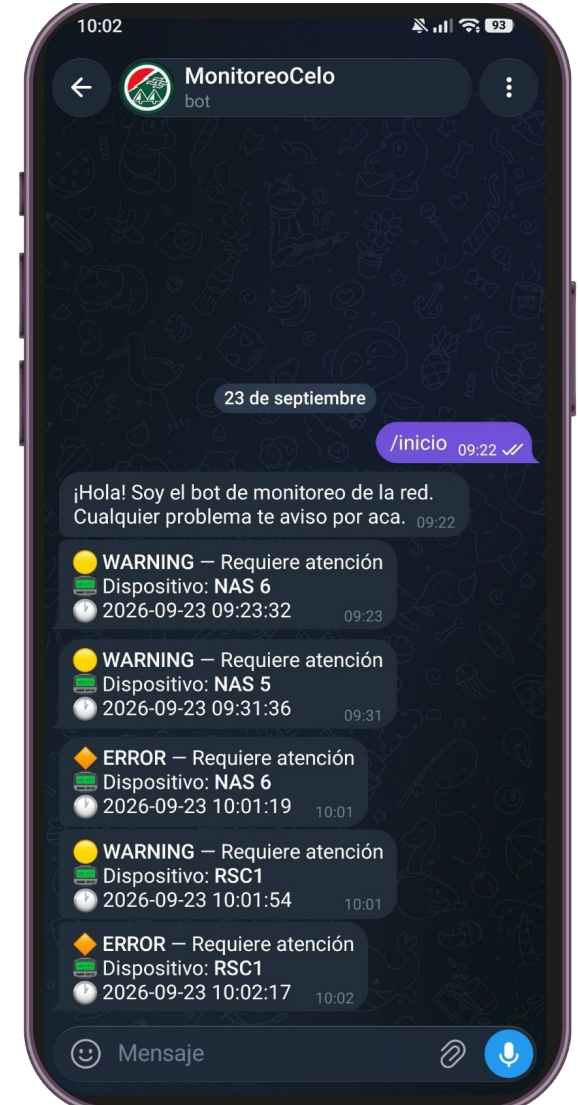
Hipótesis: falla física en ether2 de NAS 6 → caen sesiones PPPoE → caen conexiones.

Sugerencia: revisar enlace y energía del nodo.

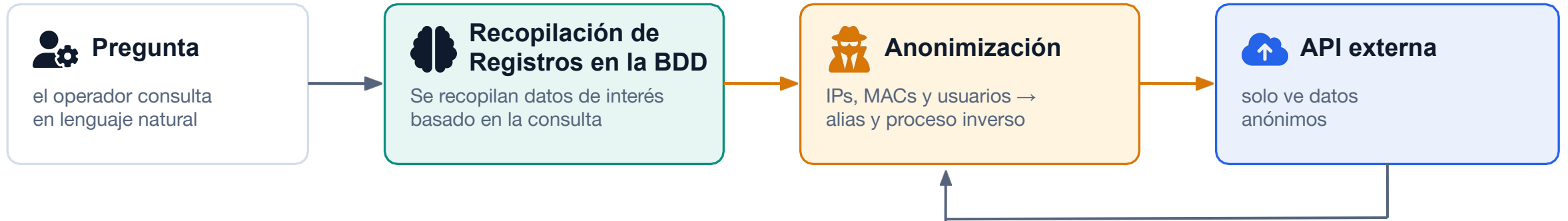
Datos simulados con fines ilustrativos.

La alerta llega antes que la queja

Primero un aviso compacto; después, el detalle donde hace falta.



Local por diseño; modelos externos como extensión, no como dependencia.



+ Qué suma

- Ante la falta de hardware local dedicado, suma la alternativa de utilizar APIs externas que permiten análisis y búsquedas de correlaciones en tiempo real (GPT, Claude, etc.)

🔒 Precauciones

- Anonimización antes de salir de la red
- Registro de cada consulta externa

🏠 Qué no cambia

- Mismo esquema, mismas vistas, misma interfaz

Qué cambia para un ISP PyME



–Tiempo

tiempo de diagnóstico + prevenciones

de ~90 min a ~18 min por evento crítico.
Optimiza el rendimiento de las
horas-hombre del personal técnico del
ISP.



100 %

local

ningún log ni dato de abonados sale
del ISP (Ley 25.326)



Accesibilidad

Accesible para todo ISP

auditorías complejas sin escribir consultas de
SQL, económica. Repercute directamente en
una mejora del servicio y del ecosistema de
redes de la región

Segmentación por VLANs dentro de la topología, datos cifrados y exposición nula de datos sensibles a la
nube



¿Preguntas?

Que la red hable el idioma del operador.

Joaquín T. Riedmaier · Santiago A. Zualet

Facultad de Ingeniería · UNaM · Oberá,
Misiones

joaquintadeoriedmaier33@gmail.com

agustinzualet23@gmail.com