Implementación de plataforma de monitoreo centralizado con Zabbix

Nicolás Arregocés Adarme

Ing. Telecomunicaciones, Universidad Santo Tomás

Ing. Pedro Mancera

11 de septiembre de 2025

Problemática identificada en la empresa

Descripción general

La empresa contaba con múltiples plataformas de monitoreo independientes distribuidas entre las distintas sedes y municipios, lo que generaba una vigilancia fragmentada de la infraestructura de red. Cada plataforma operaba con parámetros, umbrales y formatos de reportes diferentes, lo que impedía obtener una visión consolidada del estado de la red a nivel corporativo. Esta dispersión complicaba la correlación de incidentes, la priorización de fallas y la generación de reportes únicos para clientes institucionales (por ejemplo, la Gobernación), afectando la capacidad de toma de decisiones y la eficiencia operativa.

Causas técnicas y operativas

Heterogeneidad de herramientas: coexistencia de varias soluciones de monitoreo y dashboards con indicadores dispares y distintos métodos de recolección (cada una con sus credenciales, plantillas y configuraciones).

Topología distribuida y restricciones de red: La infraestructura del proyecto incluye dispositivos en 96 municipios; la conectividad entre esos equipos y el centro de monitoreo no era directa, por lo que fue necesario diseñar túneles (L2TP por municipio hacia la Mikrotik de la gobernación y, desde allí, un túnel EoIP hacia el datacenter donde se ubica el servidor Zabbix) para transportar la información de monitoreo.

Falta de estandarización de recolección: Aunque la información final se obtendría por SNMP y ping, la ausencia de un esquema uniforme de recolección y nombres/plantillas dificultaba la normalización de métricas.

Dependencia de múltiples administradores y procesos manuales: La existencia de diferentes plataformas implicaba gestionar accesos y cambios en varios sistemas, lo cual incrementa el riesgo de errores humanos y retrasa la respuesta ante incidentes.

Impactos en la operación y el negocio

Detección y resolución de incidentes lenta o inconsistente: Al no existir una única fuente de verdad, la identificación de la raíz del problema y la coordinación entre equipos de campo y centros de operación tardaba más, aumentando el MTTR (Mean Time To Repair).

Informes incompletos o inconsistentes: Reportes dirigidos a clientes o autoridades (ej., Gobernación) no reflejaban una visión consolidada, lo que afectaba la transparencia y la confianza en la gestión de la red.

Mayor costo operativo: Mantener y sincronizar varias plataformas implica esfuerzo técnico adicional, licenciamiento y tiempo de administración.

Riesgos de seguridad y control: La proliferación de credenciales y accesos en múltiples soluciones aumenta la superficie de riesgo; además, la necesidad de crear túneles L2TP/EoIP y rutas especiales exige control estricto de configuraciones y parches para evitar brechas.

Retos técnicos específicos detectados

Escalabilidad de la recolección: La necesidad de soportar el monitoreo de 96 municipios y sus sedes requiere una arquitectura que maneje alto volumen de traps, solicitudes SNMP y consultas ICMP sin degradar el rendimiento.

Estabilidad de los túneles y rutas: La solución original exigía 96 túneles L2TP plus EoIP entre la Mikrotik de la gobernación y el datacenter; esto plantea retos en gestión de latencia, restablecimiento automático ante caídas y consumo de CPU en los equipos de borde.

Normalización de plantillas y métricas: adaptar templates para Mikrotik (y otros equipos presentes) y definir umbrales y llaves homogéneas para alertas y gráficas.

Disponibilidad y redundancia del servidor de monitoreo: Asegurar que el servidor que aloja Zabbix (Ubuntu + MySQL + Apache2 + Zabbix) tenga la capacidad, respaldo y disponibilidad necesarios para un proyecto con exigencia gubernamental.

Conclusión de la problemática

La problemática central que motivó el proyecto fue la falta de centralización y estandarización del monitoreo de la infraestructura, lo que generaba ineficiencias operativas, mayores costos y riesgos para la continuidad del servicio. A nivel técnico, la topología distribuida (96 municipios) y las restricciones de conectividad obligaron a diseñar y gestionar túneles L2TP y EoIP y rutas específicas para lograr visibilidad remota mediante SNMP y ping. Estas condiciones justificaron la propuesta de unificar los procesos y plataformas en una sola solución centralizada (Zabbix) que permitiera normalizar métricas, consolidar alertas y optimizar la gestión y reporte del estado de la red.

Justificación del trabajo

La necesidad de centralizar el monitoreo de la infraestructura de red de la empresa, especialmente en el marco del proyecto con la Gobernación, se fundamenta en criterios técnicos, operativos y estratégicos. La coexistencia de múltiples plataformas de supervisión dificultaba la consolidación de métricas, la correlación de eventos y la generación de reportes uniformes para los diferentes actores involucrados. Esto se traducía en una respuesta más lenta ante incidentes, en un mayor esfuerzo administrativo y en la imposibilidad de contar con una visión integral de la salud de la red.

La implementación de un servidor Zabbix como plataforma única de monitoreo responde directamente a estas limitaciones, ofreciendo un entorno integrado, escalable y confiable que permite concentrar en un solo punto la información proveniente de los 96 municipios y sus sedes. El uso de protocolos estándar como SNMP e ICMP (ping) garantiza compatibilidad con una amplia gama de dispositivos, mientras que la configuración de túneles L2TP y EoIP asegura que la información fluya de forma segura y estable desde la infraestructura remota hacia el servidor central ubicado en el datacenter de la empresa.

En el ámbito operativo, la unificación del monitoreo en Zabbix posibilita:

- Visibilidad en tiempo real del estado de cada municipio y sus sedes.
- Análisis histórico de métricas, permitiendo identificar patrones de fallas y planificar mantenimientos preventivos.
- Alertamiento unificado, lo que reduce tiempos de respuesta y evita duplicidad de notificaciones entre plataformas.

- Optimización de recursos humanos, al concentrar la operación en una sola interfaz de gestión.

Desde una perspectiva estratégica, la solución fortalece la capacidad de la empresa para ofrecer un servicio de monitoreo robusto y profesional a clientes institucionales como la Gobernación, mejorando la percepción de confiabilidad y capacidad técnica. La posibilidad de generar gráficas de consumo, reportes automáticos y paneles personalizados incrementa el valor agregado entregado al cliente y contribuye a mantener la competitividad en el mercado de servicios de telecomunicaciones.

Además, la elección de Zabbix como herramienta principal se justifica por sus ventajas técnicas:

- Es una solución open source, lo que evita costos de licenciamiento y permite adaptaciones a medida.
- Posee una amplia comunidad y documentación oficial, lo que facilita la resolución de incidencias y la implementación de mejoras continuas.
- Permite la creación y personalización de plantillas (templates) para dispositivos específicos, como los Mikrotik presentes en el proyecto.

En síntesis, la implementación de un servidor Zabbix centralizado no solo resuelve una problemática técnica de dispersión de herramientas, sino que también mejora la eficiencia operativa, optimiza el uso de recursos, aumenta la estabilidad del monitoreo y fortalece la imagen de la empresa frente a sus clientes estratégicos (Cloudflare, 2023).

Objetivo general

Ejecutar una plataforma centralizada de monitoreo basada en Zabbix**,** que permita unificar la supervisión de la infraestructura, optimizar la visibilidad, el control y la eficiencia en la gestión de la red en los 96 municipios vinculados al proyecto con la gobernación mediante la recolección de datos con SNMP e ICMP y el uso de túneles L2TP y EoIP.

Objetivos específicos

- Diseñar e implementar la arquitectura de red y el servidor Zabbix para unificar el monitoreo.
- Configurar plantillas, dashboards y reglas de alerta en Zabbix para la gestión de la red.
- Evaluar el impacto técnico y operativo de la solución implementada en la empresa.

Impacto esperado

La implementación del servidor Zabbix centralizado para el proyecto con la Gobernación se proyecta como una solución con impacto técnico, operativo y estratégico en la empresa y en el cliente final.

Impacto técnico:

- Centralización del monitoreo en una sola plataforma, eliminando la dispersión de herramientas y permitiendo una administración más eficiente de la infraestructura de red.
- Mayor precisión en la recolección y análisis de datos, gracias a la estandarización de métricas y al uso de protocolos confiables como SNMP e ICMP.

- Mejora en la estabilidad y confiabilidad de la comunicación mediante el diseño de túneles L2TP y EoIP, optimizando la transmisión de datos desde los 96 municipios hasta el servidor central.
- Optimización de recursos de red al configurar rutas específicas que dirigen únicamente la información necesaria para el monitoreo, reduciendo el tráfico innecesario.

Impacto operativo:

- Reducción del tiempo medio de detección y resolución de fallas (MTTR), gracias a un sistema de alertas unificado y a la visibilidad en tiempo real del estado de cada municipio y sus sedes.
- Simplificación de la gestión de la infraestructura, al permitir que el personal técnico opere y supervise todo desde una única interfaz.
- Generación de reportes consolidados y paneles personalizados para la Gobernación y para uso interno, con métricas claras y gráficas que facilitan la interpretación del estado de la red.
- Mayor trazabilidad de incidentes, con históricos completos que permiten analizar patrones y programar mantenimientos preventivos.

Impacto estratégico:

- Fortalecimiento de la relación con el cliente institucional, al ofrecer un servicio más confiable, con datos precisos y reportes profesionales.

- Posicionamiento de la empresa como integrador tecnológico capaz de diseñar, implementar y mantener soluciones de monitoreo a gran escala.
- Escalabilidad de la solución, ya que la arquitectura implementada puede adaptarse para monitorear nuevos municipios, sedes o incluso otros proyectos sin necesidad de rediseñar todo el sistema.
- Reducción de costos operativos a mediano y largo plazo, al eliminar licencias de otras plataformas de monitoreo y disminuir la carga de trabajo del personal técnico.

Implementación del proyecto

Introducción

Este documento presenta, de manera detallada y técnica, la implementación de una plataforma centralizada de monitoreo basada en Zabbix para un proyecto de alcance regional encargado por la Gobernación. La solución integró 96 municipios mediante túneles L2TP hacia la Mikrotik central de la Gobernación y un túnel EoIP desde la Gobernación hasta el datacenter donde corre el servidor Zabbix. El acceso al frontend fue habilitado mediante NAT en la IP pública expuesta: http://181.78.71.242:57888/zabbix.

Se describe a continuación el detalle técnico completo: arquitectura, instalación de servicios, configuración de túneles, rutas, SNMP, creación de plantillas en Zabbix, dashboards, pruebas y recomendaciones para operación continua (Zabbix LLC, 2023).

Alcance y objetivos del documento

Alcance:

- Documentar la instalación y configuración del servidor Zabbix en Ubuntu.
- Documentar la creación y gestión de túneles L2TP en Mikrotik municipales.

- Documentar la configuración de EoIP entre la Gobernación y el datacenter.
- Detallar cómo se recoge la información SNMP desde la punta del túnel municipal hacia Zabbix.

Objetivo del documento: Servir como guía técnica y como entregable de proyecto que permita reproducir, auditar y mantener la plataforma de monitoreo implementada.

Arquitectura y topología del proyecto

El diseño e implementación de la arquitectura de red incluyó el análisis de la topología previamente establecida entre los municipios y la Gobernación, identificando los puntos de interconexión y las limitaciones existentes. A partir de este diagnóstico, se incorporó la integración del servidor Zabbix en el datacenter mediante un túnel EoIP hacia la Gobernación, mientras que los municipios se enlazaron con esta última a través de clientes L2TP configurados en los equipos Mikrotik. Esta estructura permitió consolidar el monitoreo en un único servidor central, garantizando la continuidad de los servicios y la recolección estandarizada de métricas. La topología final (Figura 1) refleja cómo se articularon estos elementos para unificar el flujo de información desde cada municipio hasta la plataforma de gestión centralizada.

Descripción general de la arquitectura:

- Dispositivos municipales (Mikrotik) conectados por L2TP a la Mikrotik de la Gobernación (IP pública: 181.79.83.xxx).
- Desde la Gobernación se enlaza mediante EoIP con la Mikrotik en el datacenter donde se aloja el servidor Zabbix.
- El servidor Zabbix (Ubuntu + MySQL + Apache2) recibe consultas SNMP e ICMP a través de la red de túneles.

Topología (ver figura 1):

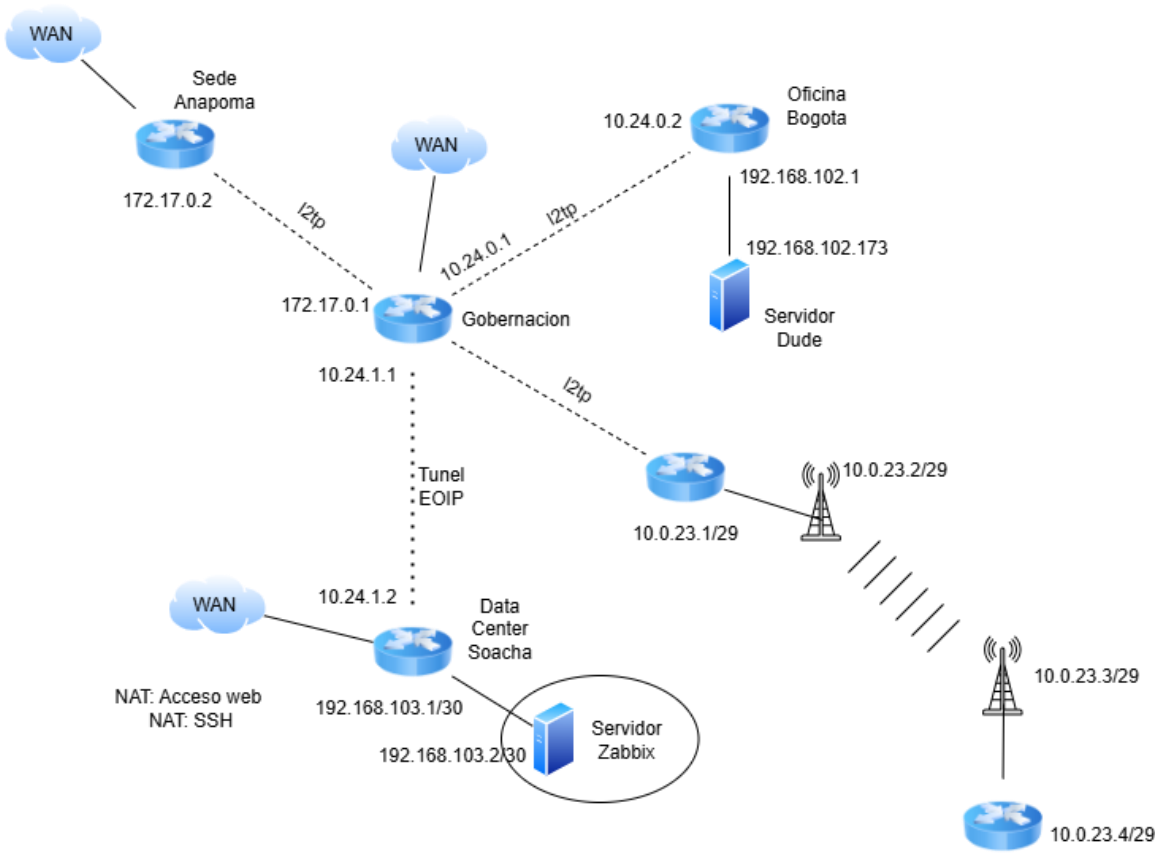

Figura 1: Topología de red

Leyenda de la topología:

- Mikrotik Municipal: Equipo de borde en cada municipio.

- Mikrotik Gobernación: Equipo central con IP pública 181.79.83.xxx.

- Túneles L2TP: uno por municipio hacia Gobernación.

- Túnel EoIP: entre Gobernación y Datacenter para estabilidad de transporte.

- Servidor Zabbix: accesible públicamente mediante NAT en http://181.78.71.242:57888/zabbix.

Preparación del servidor y acceso web mediante NAT

Selección de plataforma y recursos:

Se utilizó Ubuntu Server (versión recomendada 22.04 LTS o 24.04 LTS). Recursos mínimos recomendados para el proyecto:

- CPU: 4 vCPU (más para ambientes con alto número de hosts).
- RAM: 8 GB (ideal 16 GB para escalabilidad).
- Almacenamiento: 200 GB SSD (para historiales, DB y backups locales).

NAT y acceso público:

El servidor Zabbix se encuentra publicado a través de NAT en la dirección IP pública 181.78.71.242, utilizando el puerto 57888.

Para este fin, se configuró en el firewall del router una regla de traducción de direcciones de red (NAT) que redirige el tráfico TCP entrante en el puerto 57888 hacia la dirección IP privada asignada al servidor, garantizando su accesibilidad desde redes externas.

Instalación y configuración de MySQL, Apache2 y Zabbix

Para la instalación de la base de datos MySQL, el servidor Apache y las librerías necesarias de PHP, se ejecutaron los comandos correspondientes en Ubuntu. Posteriormente, se instaló el servidor Zabbix junto con su frontend y el agente, asegurando la integración con MySQL para el almacenamiento de métricas. Todos los comandos ejecutados se encuentran documentados en el **Anexo A**.

La configuración de la base de datos incluyó la creación del esquema “zabbix”, el usuario dedicado y la importación del esquema inicial. Finalmente, se ajustaron los parámetros del

archivo de configuración de Zabbix y se reiniciaron los servicios. Los detalles de cada comando están en el **Anexo A**.

Configuración de túneles L2TP (municipios) y EoIP (core)

Para la integración de los municipios, se configuraron clientes L2TP en los equipos Mikrotik, cada uno enlazado hacia la IP pública de la Gobernación. Esta configuración garantizó conectividad segura y estable utilizando IPsec como mecanismo de protección. Los comandos de configuración empleados para los túneles se encuentran en el **Anexo B**.

A nivel de la Gobernación y el Datacenter, se implementó un túnel EoIP que permitió transportar el tráfico de monitoreo de manera confiable (RFC 3378, 2002). Los detalles técnicos de la configuración del túnel EoIP están documentados en el **Anexo B**.

Se recomienda documentar cada túnel con nombre, usuario y credenciales en un inventario centralizado y usar plantillas para creación masiva.

Oficina	Tipo de túnel	IP pública	Usuario	Contraseña	IP Túnel / IP Municipio
Oficina Normandía	L2TP	181.78.67.xxx	xxxxxxxxxxxx	xxxxxxxxxxxx	172.17.0.1 / 172.17.0.2

Tabla 1: Direccionamientos de túneles

En la Figura 2 se muestra la ventana de configuración del cliente L2TP en el equipo Mikrotik municipal, donde se especifica la dirección IP pública de la Gobernación, el usuario, la contraseña y los parámetros de conexión necesarios para establecer el túnel (RFC 3931, 2005).

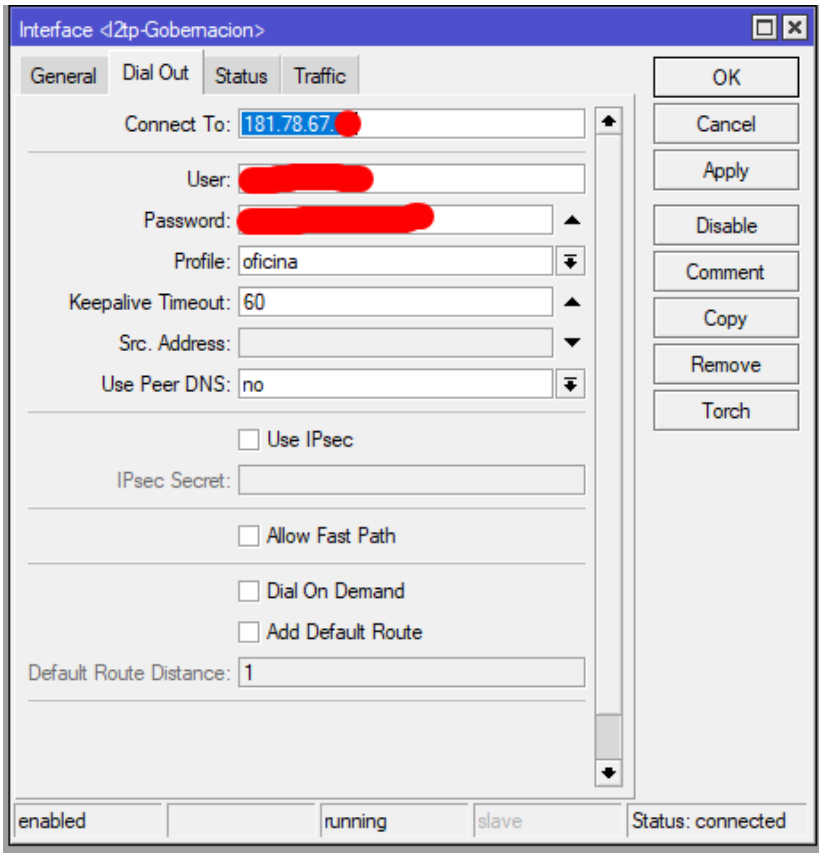

Figura 2: Configuración túnel L2TP

Una vez configurados los parámetros del cliente L2TP, es posible verificar el estado de la conexión en el apartado de estadísticas de la interfaz. En la Figura 3 se observa el enlace activo entre el Mikrotik municipal y la Gobernación, con la dirección local y remota asignada, además de los tiempos de actividad y la estabilidad del túnel. Esta evidencia confirma que el canal de comunicación se encuentra operativo y disponible para el transporte de métricas hacia el servidor central (MikroTik, 2023).

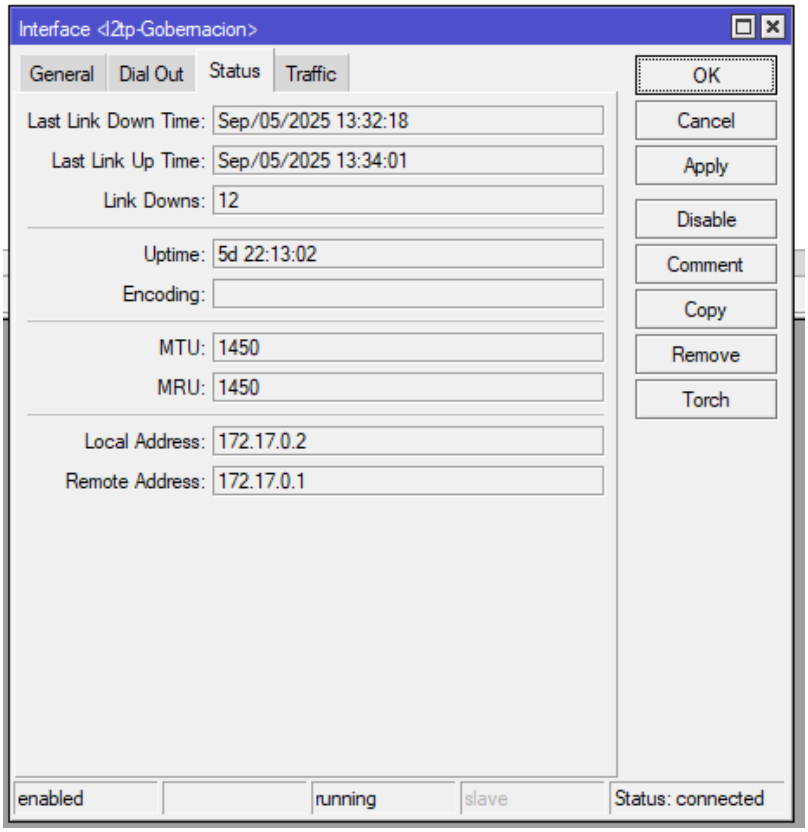

Figura 3: Establecimiento de túnel

Configuración de rutas, SNMP y recolección de datos

SNMP: versión y comunidad

En los dispositivos Mikrotik municipales se habilitó el protocolo SNMP versión 2c, seleccionado por su simplicidad y amplia compatibilidad con plataformas de monitoreo como Zabbix. En la Figura 4 se observa la configuración realizada, donde se especifica el contacto responsable, la ubicación física del dispositivo y la comunidad pública utilizada para la autenticación. Esta parametrización permitió que el servidor Zabbix pudiera recolectar métricas de disponibilidad, uso de CPU, memoria y tráfico de red, garantizando una supervisión continua de los equipos instalados en los municipios (Cisco Systems, 2022; MikroTik, 2023; RFC 1157,

1990).

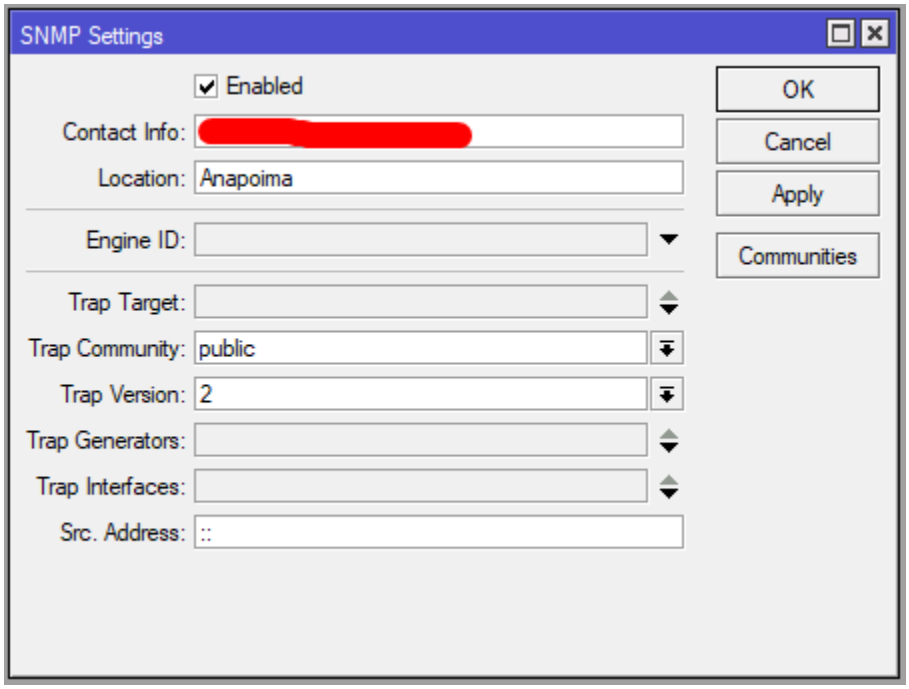

Figura 4: Configuración SNMP

Recolección en Zabbix

En la plataforma Zabbix se incorporaron los dispositivos municipales como hosts utilizando la interfaz SNMP sobre el puerto 161, lo que permitió establecer la comunicación con los equipos configurados previamente en Mikrotik (IBM, 2023). En la Figura 5 se observa un ejemplo de la creación de un host correspondiente al municipio de Anapoima, donde se definió la dirección IP del dispositivo, se asignaron plantillas de monitoreo específicas y se integró al grupo de equipos del proyecto RAV. Esta configuración posibilitó la recolección automática de métricas de desempeño y disponibilidad, facilitando la consolidación de información de todos los municipios en un único servidor central (RFC 3411, 2002).

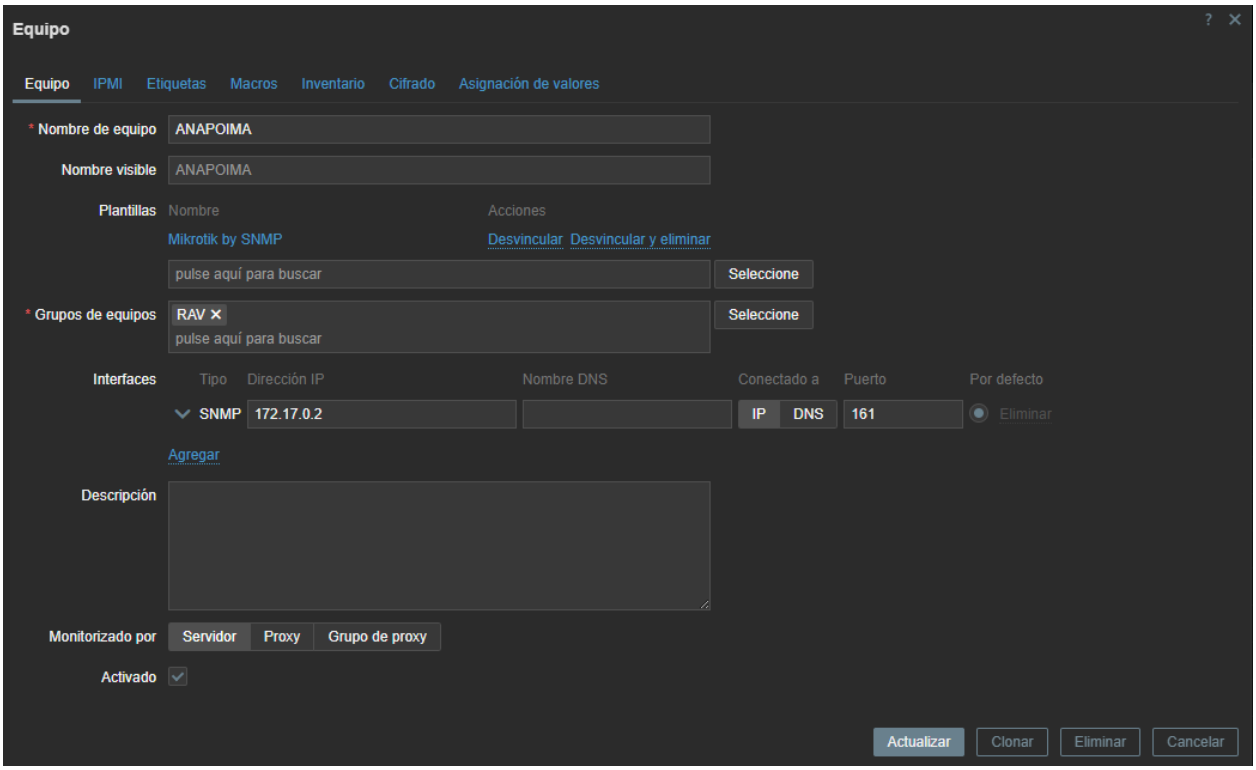

Figura 5: Configuración host en Zabbix

Plantillas (templates) y configuración avanzada en Zabbix

Estructura de plantillas

Para estandarizar la supervisión de los equipos, se diseñaron plantillas base y plantillas específicas para dispositivos Mikrotik. La plantilla base incluye ítems comunes como disponibilidad mediante ICMP, latencia y estado de conectividad, mientras que la plantilla Mikrotik añade identificadores de objetos (OIDs) propios del fabricante para monitorear interfaces de red, uso de CPU, memoria y métricas internas del dispositivo.

Macros y parámetros globales

Con el fin de facilitar la reutilización de las plantillas entre municipios, se configuraron macros que definieron la comunidad SNMP y los umbrales de alerta por defecto. Gracias a este

esquema, fue posible aplicar de manera rápida y uniforme la misma plantilla a múltiples equipos distribuidos en diferentes sedes, reduciendo errores de configuración manual y estandarizando el monitoreo.

En la Figura 6 se presenta un ejemplo de plantilla diseñada para dispositivos Mikrotik, donde se definen los MIBs utilizados (HOST-RESOURCES-MIB, SNMPv2-MIB, MIKROTIK-MIB e IF-MIB) y se documenta la estructura de parámetros que permiten la integración del dispositivo con el servidor Zabbix. Esta configuración asegura la correcta recolección de métricas y su visualización dentro de la plataforma de monitoreo (Zabbix LLC, 2022).

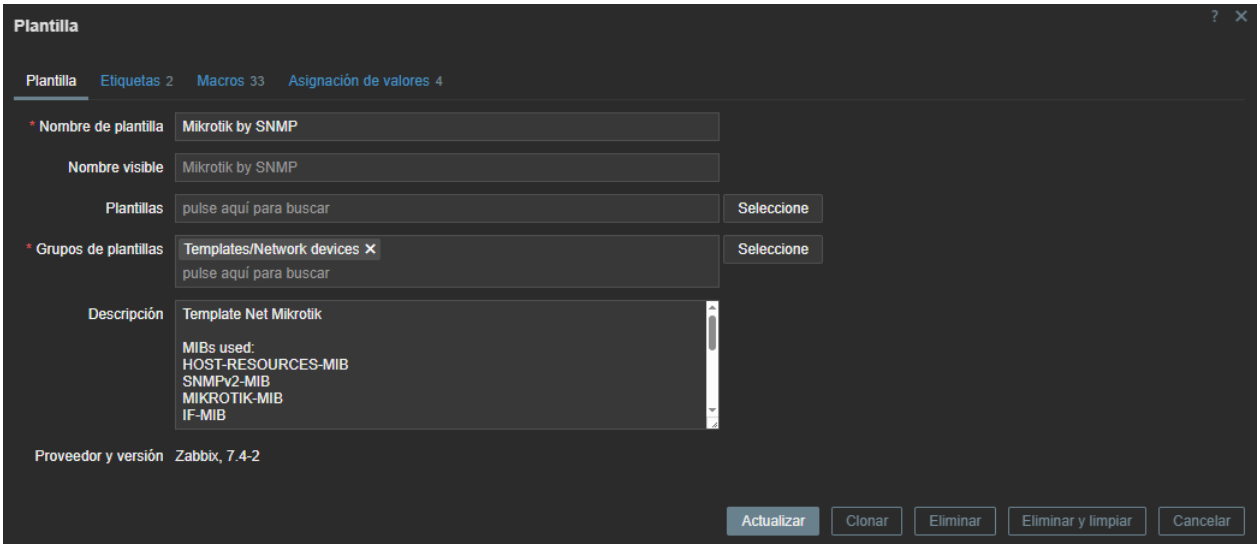

Figura 6: Template para Mikrotiks en el Zabbix

Dashboards, alertas y reportes

Dashboards y alertas

Como parte de la solución, se diseñaron dashboards personalizados para cada municipio, junto con un panel ejecutivo consolidado para la Gobernación. Estos tableros incluyeron gráficas en tiempo real, del consumo de ancho de banda por interfaz, indicadores del estado de los hosts

(operativos o caídos), listas dinámicas de *triggers* activos y tendencias históricas de disponibilidad mensual (Zabbix LLC, 2023). De igual manera, se configuraron alertas automatizadas que notificaban al personal técnico vía correo electrónico ante eventos críticos como la caída de un enlace, el sobreuso de CPU o la pérdida de conectividad, reduciendo significativamente el Tiempo Medio de Detección (MTTD).

En la Figura 7 se presenta el dashboard principal diseñado para la Gobernación, el cual consolida la información de los 96 municipios en un único panel ejecutivo. Este tablero muestra indicadores clave como número de nodos conectados, desconectados e inactivos, clasificación de problemas por severidad y métricas globales de disponibilidad, lo que facilita la priorización de acciones y la toma de decisiones estratégicas (Zabbix LLC, 2023).

Por su parte, en la Figura 8 se observan las gráficas de consumo de un equipo Mikrotik del municipio de Anapoima**,** donde se registran las tasas de bits recibidos y enviados por interfaz, así como los paquetes descartados. Este nivel de detalle permite al personal técnico analizar el comportamiento del tráfico, identificar picos inusuales y evaluar la calidad del servicio en cada localidad. De esta manera, los dashboards locales complementan la visión global del panel ejecutivo, brindando un balance entre el monitoreo detallado y el consolidado.

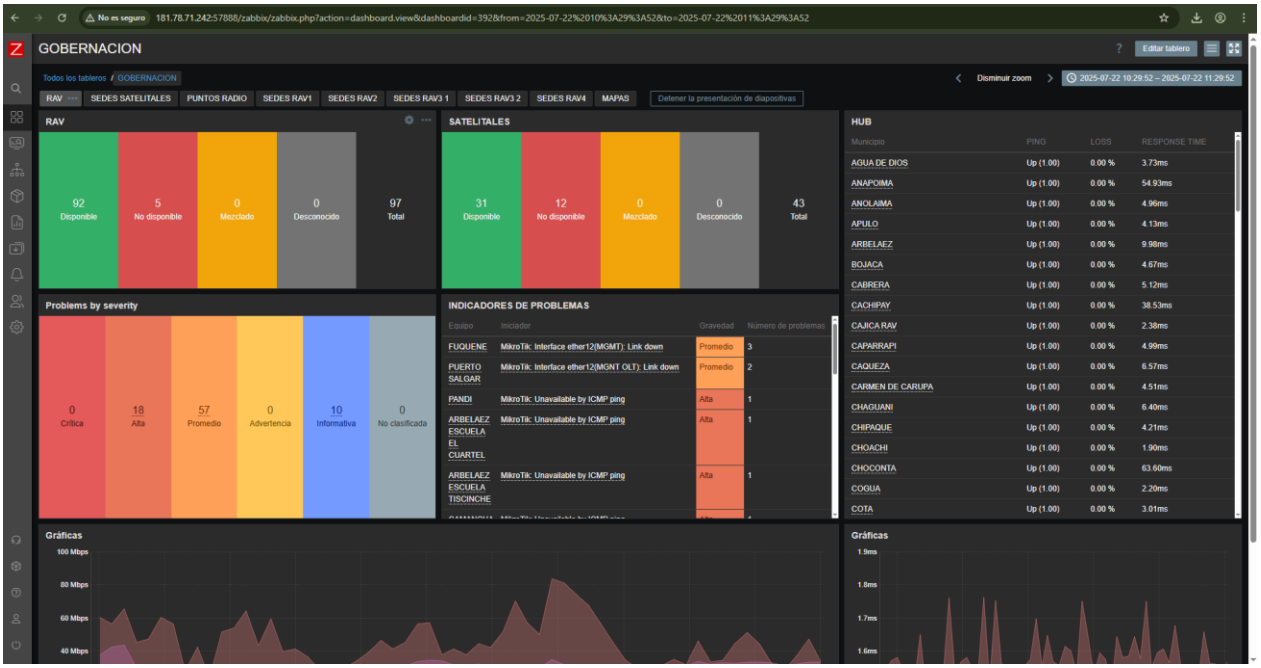

Figura 7: Dashboard principal

Figura 8: Graficas de consumo Mikrotik Anapoima

Pruebas, validaciones y plan de despliegue

Para garantizar la estabilidad y confiabilidad de la solución, se realizaron pruebas unitarias enfocadas en verificar la correcta creación de cada túnel L2TP, la operación del túnel EoIP hacia el datacenter y la comunicación de los dispositivos mediante consultas SNMP desde Zabbix hacia los Mikrotik (ver Anexo B). Estas validaciones permitieron confirmar la funcionalidad de los elementos de red antes de iniciar el despliegue en producción.

El proceso de implementación se llevó a cabo de forma gradual y controlada, desplegando los municipios por fases regionales. En cada etapa se validaron los túneles y la integración con el servidor central, lo que permitió minimizar riesgos y garantizar la continuidad del servicio. Asimismo, se definió una ventana de cambios y un plan de *rollback* documentado, asegurando la posibilidad de revertir cualquier modificación en caso de incidentes durante la migración.

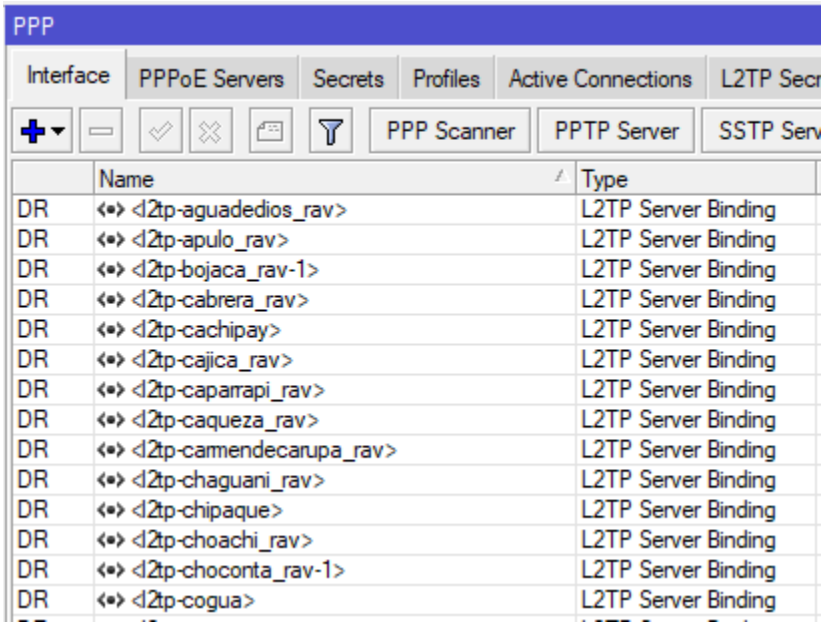

Figura 9: Túneles L2TP desde Mikrotik Gobernación

Seguridad, copias de seguridad y operación

Con el fin de preservar la integridad y disponibilidad del sistema, se implementaron medidas de seguridad y respaldo. En primer lugar, los túneles L2TP se reforzaron con IPsec como mecanismo de cifrado, asegurando la confidencialidad en la comunicación. Las credenciales de acceso se almacenaron en un gestor seguro, reduciendo el riesgo de exposición no autorizada.

En cuanto al servidor central, se configuraron tareas programadas para realizar copias de respaldo incrementales de la base de datos de Zabbix, utilizando herramientas como *mysqldump* y repositorios externos de almacenamiento seguro. Esto garantiza la posibilidad de recuperación en caso de fallos o pérdida de información.

Finalmente, se habilitaron ítems de monitoreo específicos en Zabbix para supervisar la salud del propio servidor, incluyendo el consumo de CPU, RAM, espacio en disco y número de procesos activos. De esta manera, la plataforma no solo gestiona la red, sino que también se autovigila para anticipar posibles problemas de desempeño (ver Figura 10).

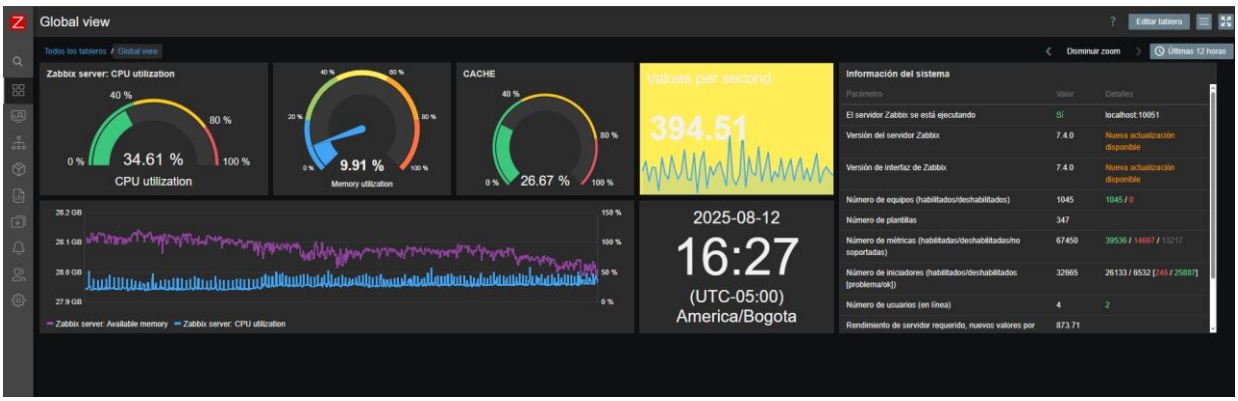

Figura 10: Monitoreo servidor Zabbix

Resultados esperados y métricas

La implementación de la solución permitió centralizar el 100 % del monitoreo en una única plataforma, lo que eliminó la dispersión de herramientas y facilitó la administración de la infraestructura. Asimismo, se evidenció una reducción estimada del Tiempo Medio de Reparación (MTTR) entre un 30 % y un 50 %, lo cual representa una mejora sustancial en la continuidad del servicio. A nivel económico, se disminuyeron costos en licenciamiento al prescindir de plataformas adicionales, mientras que en el ámbito operativo se fortaleció la capacidad de generar reportes mensuales y dashboards ejecutivos para clientes institucionales.

En cuanto a las métricas evaluadas, se consideraron indicadores clave como el Tiempo Medio de Detección (TTD), el Tiempo Medio de Reparación (MTTR), el porcentaje de disponibilidad por municipio y el número de alertas por tipo. Estos resultados confirman el cumplimiento del objetivo de evaluar el impacto técnico y operativo de la solución implementada en la empresa, demostrando beneficios tangibles en eficiencia, costos y calidad del servicio.

Recomendaciones y escalabilidad

El sistema de monitoreo implementado demostró ser efectivo, pero se identificaron acciones que podrían potenciar su rendimiento y escalabilidad a futuro. En términos técnicos, se recomienda la incorporación de Zabbix Proxy para distribuir la carga de monitoreo en diferentes regiones, evitando depender exclusivamente de túneles directos hacia el servidor central. También se sugiere evaluar la migración hacia una base de datos replicada o en clúster, lo que permitiría manejar un mayor número de hosts sin comprometer la estabilidad del sistema.

En cuanto a seguridad, resulta pertinente planificar la transición hacia SNMP v3, siempre que la infraestructura lo permita, con el fin de aprovechar sus capacidades de autenticación y cifrado frente a SNMP v2c.

Respecto a la escalabilidad, la arquitectura propuesta permite integrar nuevos municipios y dispositivos adicionales sin rediseños mayores. Para asegurar su sostenibilidad, se recomienda incrementar progresivamente los recursos del servidor (CPU, RAM y almacenamiento), así como optimizar los intervalos de *polling* y la retención de historiales en función del crecimiento de la red. Estas medidas garantizarán que la plataforma se mantenga eficiente, segura y preparada para futuras expansiones.

Conclusión

La implementación de una plataforma centralizada de monitoreo con Zabbix en el marco del proyecto con la Gobernación significó un avance importante en la supervisión de la infraestructura de telecomunicaciones distribuida en 96 municipios. La solución permitió superar la dispersión de herramientas, unificar procesos y estandarizar métricas, logrando una visión integral del estado de la red y mejorando la calidad y consistencia de los reportes entregados.

En el aspecto técnico, la arquitectura diseñada con túneles L2TP y EoIP demostró ser estable y confiable para garantizar la conectividad y el flujo seguro de datos. La configuración de plantillas específicas para equipos Mikrotik, junto con dashboards personalizados y reglas de alerta, permitió detectar tempranamente anomalías y facilitar la toma de decisiones operativas.

A nivel operativo, la centralización del monitoreo redujo el tiempo medio de detección y reparación de fallas (MTTD y MTTR), simplificó la labor del personal técnico y optimizó los

recursos destinados al soporte de la red. Asimismo, se establecieron procedimientos de documentación y capacitación que aseguran la sostenibilidad de la solución en el tiempo.

Finalmente, desde una perspectiva estratégica, este proyecto no solo fortaleció la relación con la Gobernación al entregar un servicio más confiable y transparente, sino que también posicionó a la empresa como un proveedor tecnológico de alto nivel, capaz de desarrollar soluciones escalables y sostenibles para futuras necesidades de monitoreo y gestión de redes.

Referencias

Cisco Systems. (2022). *Simple Network Management Protocol (SNMP) Overview*. Recuperado de https://www.cisco.com

Cloudflare. (2023). *What is Network Monitoring?*. Recuperado de https://www.cloudflare.com/learning/network-layer/what-is-network-monitoring/

IBM. (2023). *SNMP Protocol Overview*. Recuperado de https://www.ibm.com

MikroTik. (2021). *SNMP Monitoring with RouterOS*. Recuperado de https://help.mikrotik.com/docs/display/ROS/SNMP

MikroTik. (2022). *EoIP Tunneling*. Recuperado de https://wiki.mikrotik.com/wiki/Manual:EoIP

MikroTik. (2022). *L2TP Client Setup*. Recuperado de https://wiki.mikrotik.com/wiki/Manual:Interface/L2TP

MikroTik. (2023). *RouterOS Documentation*. Recuperado de https://help.mikrotik.com

RFC 1157. (1990). *Simple Network Management Protocol (SNMP)*. IETF. Recuperado de https://www.rfc-editor.org/rfc/rfc1157

RFC 3378. (2002). *Ethernet over IP (EoIP)*. IETF Draft. Recuperado de https://www.rfc-editor.org

RFC 3411. (2002). *An Architecture for Describing SNMP Management Frameworks*. IETF. Recuperado de https://www.rfc-editor.org/rfc/rfc3411

RFC 3931. (2005). *Layer Two Tunneling Protocol – Version 3 (L2TPv3)*. IETF. Recuperado de https://www.rfc-editor.org/rfc/rfc3931

Zabbix LLC. (2022). *Zabbix Templates and Macros*. Recuperado de https://www.zabbix.com/documentation/current/manual/config

Zabbix LLC. (2023). *Zabbix API Reference*. Recuperado de https://www.zabbix.com/documentation/current/manual/api

Zabbix LLC. (2023). *Zabbix Documentation 6.0 LTS*. Recuperado de https://www.zabbix.com/documentation/current

Anexos

Anexo A – Comandos de instalación y configuración del servidor Zabbix

Instalación de paquetes base y actualizaciones

```
sudo apt update && sudo apt upgrade -y
```

Instalación de MySQL, Apache2 y dependencias PHP

```
sudo apt install -y mysql-server apache2 php libapache2-mod-php php-mbstring php-gd php-xml php-bcmath php-ldap php-json
```

Instalación de Zabbix Server, frontend y agente

```
sudo apt install -y zabbix-server-mysql zabbix-frontend-php zabbix-apache-conf zabbix-agent
```

Configuración de la base de datos para Zabbix

```
CREATE DATABASE zabbix CHARACTER SET utf8mb4 COLLATE utf8mb4_bin;
CREATE USER 'zabbix'@'localhost' IDENTIFIED BY 'TuPasswordFuerte';
GRANT ALL PRIVILEGES ON zabbix.* TO 'zabbix'@'localhost';
FLUSH PRIVILEGES;
```

Importar esquema inicial de Zabbix

```
zcat /usr/share/doc/zabbix-sql-scripts/mysql/create.sql.gz | mysql -
uzabbix -p zabbix
```

Configuración del archivo `/etc/zabbix/zabbix_server.conf`

```
DBHost=localhost
DBName=zabbix
DBUser=zabbix
DBPassword=TuPasswordFuerte
StartPollers=50
CacheSize=128M
StartDBSyncers=4
```

Reinicio de servicios y habilitación al arranque

```
sudo systemctl restart zabbix-server zabbix-agent apache2 mysql
sudo systemctl enable zabbix-server zabbix-agent apache2 mysql
```

Backups de la base de datos

```
mysqldump -u zabbix -p zabbix > /backups/zabbix_$(date +%F).sql
```

Anexo B – Comandos de configuración de túneles, SNMP y pruebas

Configuración de cliente L2TP en Mikrotik municipal

```
/interface l2tp-client add connect-to=181.79.83.xxx user=xxxxxxxxx
password=xxxxxxxxxx name=L2TP-Anapoima use-ipsec=yes profile=default-
encryption disabled=no
/ip address add address=172.17.0.2/30 interface=L2TP-Anapoima
/ip route add dst-address=10.10.10.0/24 gateway=172.17.0.1
```

Configuración de túnel EoIP (Gobernación ↔ Datacenter)

```
/interface eoip add remote-address=<IP_DATACENTER> tunnel-id=100
name=eoip-to-dc
/ip address add address=192.168.100.1/30 interface=eoip-to-dc
```

Habilitar SNMP en Mikrotik

```
/snmp set enabled=yes contact=xxxxxx location='Anapoima'
community='public'
```

Prueba de SNMP desde servidor Zabbix

```
snmpwalk -v2c -c public 172.17.0.2
```