UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI

FACULTAD DE INDUSTRIAS AGROPECUARIAS Y CIENCIAS AMBIENTALES

CARRERA DE COMPUTACIÓN

Tema: "Tráfico de redes IP y Calidad de servicios"

Trabajo de Integración Curricular previo a la obtención del título de Ingeniera en Ciencias de la Computación

AUTORA: Revelo Montenegro Steffany Dayana

TUTOR: Ing. Del Hierro Mosquera Milton Gabriel MSc.

Tulcán, 2026.

CERTIFICADO DEL TUTOR

Certifico que la estudiante Revelo Montenegro Steffany Dayana con el número de cédula 1005275829 respectivamente ha desarrollado el Trabajo de Integración Curricular: "Tráfico de redes IP y Calidad de servicio"

Este trabajo se sujeta a las normas y metodología dispuesta en la Codificación del Reglamento de Régimen Académico y de Estudiantes de la UPEC, por lo tanto, autorizo la presentación de la sustentación para la calificación respectiva.

Firmado electrónicamente por:
MILTON GABRIEL DEL HIERRO MOSQUERA
Validar únicamente con FirmaEC

_____

Ing. Del Hierro Mosquera Milton Gabriel MSc.

TUTOR

Tulcán, enero de 2026

AUTORÍA DE TRABAJO

El presente Trabajo de Integración Curricular constituye un requisito previo para la obtención del título de Ingeniera en la Carrera de Computación de la Facultad de Industrias Agropecuarias y Ciencias Ambientales

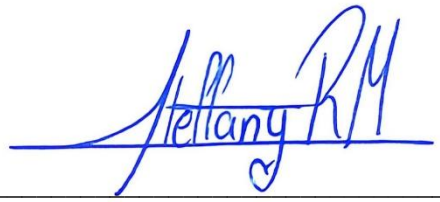
Yo, Revelo Montenegro Steffany Dayana con cédula de identidad número 1005275829 respectivamente declaro que la investigación es absolutamente original, auténtica, personal y los resultados y conclusiones a los que he llegado son de mi absoluta responsabilidad.

Revelo Montenegro Steffany Dayana
AUTORA

Tulcán, enero de 2026

ACTA DE CESIÓN DE DERECHOS DEL TRABAJO DE INTEGRACIÓN CURRICULAR

Yo Revelo Montenegro Steffany Dayana declaro ser autora de los criterios emitidos en el Trabajo de Integración Curricular: "Tráfico de redes IP y calidad de servicio" y eximo expresamente a la Universidad Politécnica Estatal del Carchi y a sus representantes de posibles reclamos o acciones legales.



Revelo Montenegro Steffany Dayana

AUTORA

Tulcán, enero de 2026

AGRADECIMIENTO

Gracias a Dios, por darme la fortaleza para continuar cuando el cansancio pesaba más que las ganas, por acompañarme en cada etapa y por recordarme que todo esfuerzo tiene su recompensa.

Gracias a mis padres, por su amor incondicional, por la paciencia infinita, por cada sacrificio silencioso y por creer en mí incluso cuando las dudas me ganaban. Ustedes fueron el motor que me sostuvo en los momentos más difíciles; este logro no es solo mío, es nuestro.

Gracias a mis hermanos, por su compañía incondicional, por su cariño sincero y por convertirse en mi mayor motivación. Cada esfuerzo, cada desvelo y cada paso en este camino fue pensando en ustedes; nunca olviden que todo lo que hago es por y para ustedes.

A mis abuelitos, gracias por su amor infinito, por sus enseñanzas y por ser raíz y refugio en mi vida. A los que hoy me cuidan desde el cielo, los llevo en cada paso y en cada logro; y a los que aún me acompañan en la tierra, gracias por su presencia, sus consejos y su cariño. Este triunfo también lleva su nombre y su bendición.

A mi tutor, el Magíster Milton del Hierro, mi sincero agradecimiento por su guía constante, su compromiso y, sobre todo, por brindarme una amistad sincera en los momentos más difíciles, cuando el apoyo humano fue tan importante como el académico.

Al MSc. Javier Torres, gracias por su tiempo, su disposición y su valioso apoyo, así como por compartir sus conocimientos de manera generosa, los cuales fortalecieron y enriquecieron este trabajo de investigación.

A mis docentes, por su enseñanza, su exigencia y por aportar de manera significativa a mi formación académica y profesional.

A la Universidad Politécnica Estatal del Carchi, por abrirme sus puertas, brindarme formación académica y convertirse en el espacio donde crecí no solo como estudiante, sino también como persona.

A mis tíos y tías, agradezco esa mano que me otorgaron para sostenerme, agradezco su apoyo, sus palabras de aliento y el acompañamiento brindado a lo largo de este

proceso, los cuales fueron importantes para continuar y alcanzar este logro, estaré eternamente agradecida.

A mis primos agradezco los recuerdos compartidos y el valor de tenerlos en mi vida, ya que cada momento juntos se convirtió en una experiencia única que acompañó este proceso.

A mi familia Revelo Aragón, a mi Evy, por acompañarme, apoyarme y celebrar conmigo cada paso alcanzado, me enseñaron que para ser familia une el amor y no la sangre.

A mi team, a mis amigas Andre, Lore, Bere, Nico y María, gracias por una amistad que nació en la escuela y que el tiempo supo hacer más fuerte. Gracias por las risas descontroladas en cada locura, por convertir los momentos simples en recuerdos eternos, por convertir mis problemas en los suyos. Ustedes fueron esa curita al corazón que siempre sanó. Tenerlas en mi vida ha sido uno de los regalos más grandes de este camino.

A mis amigos de la universidad, Sami, Eri, Ander, Alex y Jhoel, gracias por esa amistad que nació sin esfuerzo y se fue construyendo con confidencias, risas y también lágrimas. Por esas conversaciones largas donde una botella se convirtió en excusa para abrir el corazón, por escuchar sin juzgar y por esos abrazos sinceros que siempre llegaron justo a tiempo. Gracias por acompañarme en esta etapa tan importante y por regalarme recuerdos que no se quedan en la universidad, sino que vivirán conmigo para siempre.

Revelo Montenegro Steffany Dayana

DEDICATORIA

A Dios, porque incluso cuando sentí que ya no podía seguir, Él nunca me soltó. Fue mi refugio en los días más oscuros, mi fuerza cuando las ganas se apagaban y mi paz cuando el cansancio parecía vencerme.

A mi mamá, Julia Montenegro, mi hogar, mi refugio y mi mayor ejemplo de amor. Gracias por creer en mí cuando yo misma dudé, por ser mi compañera de risas y mi compinche, por sostenerme en silencio, por secar mis lágrimas y por recordarme, una y otra vez, que sí podía lograrlo, me llena de orgullo ser su hija.

A mi papá, Fabián Revelo, por estar siempre, por su apoyo firme y constante, y por enseñarme que ningún sueño es imposible cuando se camina con esfuerzo, constancia y fe, pero sobre todo por darme esa humildad y ese carisma que nos caracteriza, es un honor ser su hija.

A mis hermanos, mi amado Cris y mi amada Panchita, por ser mi alegría en los días difíciles, por su cariño sincero, su amor infinito y esas locuras que siempre lograron sacarme una sonrisa, pero sobre todo por ser parte de mi motivación diaria, nunca duden que cada logro es por y para ustedes.

A mi perrito Maxi, mi compañero fiel, testigo silencioso de tantas noches largas, quien sin palabras supo darme calma, compañía y un amor tan puro que me devolvió fuerzas cuando más lo necesitaba.

A mis abuelitos, a los que hoy me cuidan desde el cielo, Papá Liz y Mamita Juli, los llevo en cada latido y en cada logro, sé que nunca me soltaron; y a los que aún me acompañan en la tierra, Hernán y Mariani, gracias por su amor, su presencia y por ser raíz en mi vida.

Y, finalmente, a mí, a esa versión de hace cuatro años que lloró, que tuvo miedo y atravesó dolores tan profundos que cualquiera se habría rendido. Pero ella se levantó una y otra vez, aun creyendo que no llegaría hasta aquí. Hoy la abrazo con orgullo y le digo que sí pudo, que fue valiente, que resistió y que cada lágrima valió la pena, ya puedo celebrar con ella.

Revelo Montenegro Steffany Dayana

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ÍNDICE DE ANEXOS

RESUMEN

La presente investigación tiene como objetivo analizar el comportamiento del tráfico de red en la Universidad Politécnica Estatal del Carchi (UPEC) mediante el uso de una herramienta especializada de monitoreo, con el propósito de identificar problemas en la infraestructura de red y proponer soluciones orientadas a mejorar la calidad del servicio para estudiantes, docentes y personal administrativo. Para ello, el estudio se desarrolló bajo un enfoque metodológico mixto, integrando técnicas cuantitativas y cualitativas. Inicialmente, se seleccionó la herramienta de monitoreo Zabbix, evaluando su capacidad para analizar el tráfico, su impacto en la congestión y su aporte al rendimiento de la red institucional. Posteriormente, a través del monitoreo en tiempo real de interfaces críticas, se identificaron los tipos de conexiones que generan mayor saturación, así como patrones de uso del tráfico concentrados en horarios y rutas específicas. El análisis cuantitativo permitió medir el impacto del exceso de tráfico en la calidad del servicio, considerando indicadores como el uso de ancho de banda, la latencia, la pérdida de paquetes y la disponibilidad de los servicios digitales. Estos resultados se complementaron con el análisis cualitativo, que incluyó encuestas a estudiantes, docentes y personal administrativo, además de una entrevista al personal del área de Tecnologías de la Información y Comunicación, con el fin de conocer la percepción de los usuarios sobre el desempeño de la red. Los resultados evidencian que el incremento del tráfico digital, especialmente en periodos de alta actividad académica y administrativa, afecta la estabilidad y velocidad de los servicios institucionales. Finalmente, se proponen recomendaciones orientadas a optimizar la gestión del tráfico, como la priorización de servicios, el refuerzo de interfaces críticas, la segmentación lógica de la red y la configuración de alertas inteligentes, con el objetivo de garantizar una conectividad más estable y eficiente para la comunidad universitaria.

Palabras Claves: Trafico de redes, calidad de servicio, monitoreo en tiempo real, gestión del tráfico, segmentación de red.

ABSTRACT

The present research aims to analyse the behaviour of network traffic at the State Polytechnic University of Carchi (UPEC) through the use of a specialized monitoring tool, in order to identify issues within the network infrastructure and propose solutions aimed at improving service quality for students, faculty members, and administrative staff. To this end, the study was conducted under a mixed-methods approach, integrating both quantitative and qualitative techniques. In the initial stage, the monitoring tool Zabbix was selected, and its capacity to analyse network traffic, its impact on congestion, and its contribution to the performance of the institutional infrastructure were evaluated. Subsequently, through real-time monitoring of critical interfaces, the types of connections generating the highest levels of saturation were identified, as well as traffic usage patterns concentrated at specific times and along particular routes. The quantitative analysis made it possible to measure the impact of excessive traffic on service quality by considering indicators such as bandwidth utilization, latency, packet loss, and the availability of digital services. These results were complemented by a qualitative analysis that included surveys administered to students, faculty members, and administrative staff, as well as an interview with personnel from the Information and Communication Technologies department, in order to assess users' perceptions of network performance. The findings reveal that the increase in digital traffic, particularly during periods of high academic and administrative activity, negatively affects the stability and speed of institutional services. Finally, recommendations are proposed to optimize network traffic management, including service prioritization, reinforcement of critical interfaces, logical network segmentation, and the configuration of intelligent alerts, with the aim of ensuring more stable and efficient connectivity for the university community.

Keywords: Network traffic, quality of service, real-time monitoring, traffic management, network segmentation.

INTRODUCCIÓN

En la actualidad, el monitoreo de red en tiempo real se ha convertido en un componente esencial para garantizar el correcto funcionamiento de los servicios tecnológicos dentro de una institución. Cuando el tiempo de respuesta y la disponibilidad del servicio es fundamental poder reconocer y responder rápidamente a fallas o amenazas marca la diferencia entre un sistema estable y uno vulnerable. Según IBM (2023), las soluciones modernas de monitoreo ofrecen una amplia visibilidad del tráfico y permiten responder ante posibles ciberataques con mayor eficiencia gracias a la automatización en la detección y el análisis de amenazas.

Las redes IP constituyen hoy la base sobre la cual operan la mayoría de las aplicaciones y servicios digitales. Actividades indispensables como videoconferencias, clases virtuales y otros procedimientos administrativos. Sin embargo, a medida que aumentan los usuarios, los dispositivos conectados y los servicios digitales, la gestión eficiente del tráfico de Internet se vuelve más compleja. Esto requiere habilidades técnicas de mayor nivel para asegurar que Internet controle el continuo y la calidad de los servicios ofrecidos.

Al igual que en otras instituciones educativas, la Universidad Politécnica del Estatal de Carchi (UPEC), también ha transformado digitalmente actividades académicas y administrativas. Sin embargo, el aumento de la demanda tecnológica ha revelado algunos problemas de conectividad y saturación de la red que impactan el desarrollo normal de las actividades académicas y administrativas. Una breve desconexión de la red, por ejemplo, puede detener las clases virtuales, interrumpir la investigación y detener procedimientos esenciales. Esto demuestra claramente que el rendimiento de la red y la conectividad es más que un aspecto técnico; es una condición para el desempeño eficiente y seguro de la universidad.

Frente a esta situación, es evidente que el análisis del tráfico de red y el control del perímetro institucional no son alternativas, sino más bien una necesidad que se transforma en una estrategia a seguir para optimizar el sistema de recursos tecnológicos. Gracias al uso de herramientas como Zabbix los administradores de red monitorean la actividad y el flujo de datos, a través de reconocer aquellos momentos de mayor congestión para prevenir el fallo y mejorar la experiencia del usuario. Estas prácticas gestionan, de manera óptima, el ancho de banda y favorecen la Quality

of Service (QoS) para que, cada uno de los usuarios, tenga conexión estable y confiable.

El presente trabajo de investigación tiene fundamentalmente la evaluación del tráfico de red de la UPEC, así como, analizar el impacto en la calidad de servicio, y realizar propuestas de mejora que permitan optimizar la infraestructura tecnológica institucional. Para ello, se seguirá una metodología que tenga un enfoque de tipo mixto, en la que se integren técnicas de análisis cualitativo y cuantitativo. Así se identificarán no solo los problemas conocidos, sino que se plantearán acciones concretas con el objetivo de tener una red más rápida, estable y segura, para el disfrute de toda la comunidad universitaria.

I. EL PROBLEMA

1.1. PLANTEAMIENTO DEL PROBLEMA

En el ámbito global, las redes IP han tomado un rol central en la operación de instituciones académicas y organizaciones que dependen de servicios digitales. A medida que aumentan las videoconferencias, plataformas virtuales y sistemas alojados en la nube, las redes requieren mecanismos de observación continua para garantizar un rendimiento estable. La literatura reciente subraya que la gestión adecuada de la Calidad de Servicio (QoS) depende de monitorear, en tiempo real, los indicadores clave de desempeño. Cristobo et al. (2024), señala que "asegurar una adecuada Quality of Service requiere medir de manera continua el retardo, el jitter, la pérdida de paquetes y el consumo de ancho de banda" (p. 3).

Asimismo, el monitoreo se ha convertido en una pieza esencial para anticiparse a caídas o saturación de la red. Fotopoulou et al. (2021) afirma que "network performance monitoring is essential to identify congestion, detect anomalies, and ensure acceptable levels of Quality of Service in modern IP networks" (p. 4). Esto resalta que la estabilidad de los servicios digitales depende directamente de la capacidad de analizar el tráfico IP de manera constante y precisa.

En Ecuador, distintos estudios coinciden en que la infraestructura tecnológica y la calidad de los servicios digitales se han vuelto determinantes para el funcionamiento adecuado de las instituciones educativas. Hernández (2024) destaca que "el desempeño de la infraestructura tecnológica sigue siendo un factor decisivo para la continuidad y la calidad de los procesos educativos en Ecuador" (p. 52).

Además, evaluaciones recientes han identificado brechas internas entre universidades, especialmente en la administración y el rendimiento de sus plataformas digitales. Morán (2024) sostiene que "existen diferencias significativas en la calidad y rendimiento de los servicios web universitarios, lo que refleja desafíos en la gestión tecnológica institucional" (p. 115). Estas observaciones dejan en evidencia que, dentro del país, las instituciones enfrentan el reto de mejorar la estabilidad,

disponibilidad y gestión del tráfico en sus redes para garantizar la continuidad académica.

Este contexto nacional muestra claramente que, sin herramientas de monitoreo especializadas, las universidades ecuatorianas no pueden identificar oportunamente problemas de saturación, pérdida de paquetes o lentitud en sus sistemas, lo que afecta tanto a estudiantes como a docentes y personal administrativo.

Dentro de la Universidad Politécnica Estatal del Carchi (UPEC), la red institucional se ha convertido en el eje que sostiene el aula virtual, el sistema académico, las plataformas de comunicación, los servicios administrativos y los recursos digitales de apoyo a la docencia. El uso constante de estas herramientas ha incrementado el tráfico IP, exigiendo una supervisión más detallada de la infraestructura. Sin embargo, actualmente la UPEC no cuenta con un sistema integral de monitoreo, que permita observar el comportamiento del tráfico en tiempo real, analizar tendencias o identificar puntos críticos de saturación.

La evidencia científica muestra que esta falta de monitoreo puede generar problemas silenciosos que se vuelven visibles solo cuando el servicio ya está afectado. Pranata et al. (2023) explican que "las redes de los campus suelen sufrir degradación del rendimiento durante las horas pico, principalmente por saturación de ancho de banda y flujos de tráfico no gestionados" (p. 6). Del mismo modo, Altmemi (2022) advierte que "sin monitoreo continuo, la congestión, la pérdida de paquetes y la degradación del servicio permanecen sin detectarse hasta que afectan directamente a los usuarios" (p. 605).

Para la UPEC, esta situación implica riesgos concretos: intermitencias en el aula virtual, lentitud en el sistema académico, fallos en videoconferencias, caídas en los servicios web y dificultades para mantener la calidad educativa. Todo esto evidencia un problema central: la universidad depende cada día más de su infraestructura tecnológica, pero carece de herramientas que permitan medir, analizar y mejorar el comportamiento real del tráfico IP.

1.2. FORMULACIÓN DEL PROBLEMA

¿Cómo afecta el crecimiento del tráfico digital en la calidad de los servicios y qué soluciones de monitoreo en tiempo real podrían optimizar el rendimiento de la red en la Universidad Politécnica Estatal del Carchi?

1.3. JUSTIFICACIÓN

En la actualidad, contar con un acceso a Internet seguro, rápido y confiable constituye uno de los pilares fundamentales para el funcionamiento eficiente de cualquier institución de educación superior. Las universidades modernas dependen cada vez más de infraestructuras tecnológicas basadas en redes IP, que permiten el funcionamiento de aplicaciones académicas y administrativas como plataformas de aprendizaje virtual, correos institucionales, videoconferencias, sistemas de gestión educativa y servicios en la nube. En este contexto la calidad del servicio se convierte en un elemento primordial para garantizar que las actividades funciones sin interrupciones ni demoras ni pérdida de información.

En la Universidad Politécnica Estatal del Carchi, UPEC, se han detectado errores asociados a la gestión del tráfico de red en diferentes periodos académicos. Los errores más habituales son la lentitud para ingresar en plataformas como Moodle, las interrupciones en video llamadas, la perdida temporal de acceso a diferentes recursos institucionales, el que afecta la productividad, la continuidad académica y la calidad del aprendizaje en ambientes digitales.

Por eso, es importante revisar con cuidado cómo se comporta el tráfico de la red usando herramientas especializadas como Zabbix, que permiten monitorear el ancho de banda, la latencia, las pérdidas de paquetes y otros parámetros clave. La investigación está fundamentada en un conjunto de procesos sistemáticos críticos y empíricos que se aplican al estudio de fenómeno o problema (Hernández-Sampieri, Fernández Collado & Baptista-Lucio, 2022). En pocas palabras, usar Zabbix permite detectar a tiempo cuando la red se satura o falla, lo que ayuda a aprovechar mejor los recursos tecnológicos que tenemos. Este trabajo tiene sentido porque responde a lo que realmente necesita la comunidad universitaria, que depende de internet para sus clases, trabajos y trámites administrativos. Además, es totalmente viable porque se usa herramientas de monitoreo gratuitas y de código abierto, y cuenta con el apoyo del TIC de la UPEC, lo que da acceso a datos reales del tráfico de la red.

Al final, este estudio aporta valor en dos frentes, por un lado, en lo técnico, ayudará a mejorar las habilidades para gestionar eficientemente el tráfico de la red y aplicar mejoras continuas. Desde el ámbito institucional, sus resultados servirán como base para la toma de decisiones sobre infraestructura tecnológica, fomentando un servicio

digital más estable, sostenible y alineado con los objetivos de calidad educativa de la universidad.

1.4. OBJETIVOS Y PREGUNTAS DE INVESTIGACIÓN

1.4.1. Objetivo General

Analizar el comportamiento del tráfico de red en la Universidad Politécnica Estatal del Carchi mediante una herramienta especializada, la identificación de problemas y el planteamiento de soluciones para la mejora de calidad de servicio para estudiantes, docentes y personal.

1.4.2. Objetivos Específicos

- Seleccionar una herramienta de monitoreo de la red enfocándose en su impacto en la congestión y el rendimiento de la red, obteniendo los resultados correspondientes.
- Identificar qué tipos de conexiones saturan la red de la universidad y detección de patrones de uso que permitan proponer estrategias para la optimización de la red.
- Medir cómo el exceso de tráfico provoca problemas en la calidad de servicio en la UPEC.

1.4.3. Preguntas de Investigación

¿Qué herramienta de monitoreo se adapta mejor a la realidad de la UPEC y cómo ayuda, en la práctica, a entender y controlar la congestión y el rendimiento de la red?

¿Qué tipos de conexiones son las que más saturan la red universitaria y qué patrones de uso diario se pueden descubrir para plantear mejoras reales en su funcionamiento?

¿Cómo influye el exceso de tráfico en la calidad del servicio que reciben estudiantes, docentes y personal administrativo dentro de la UPEC?

II. FUNDAMENTACIÓN TEÓRICA

2.1. ANTECEDENTES DE LA INVESTIGACIÓN

Varios estudios han investigado los problemas de tráfico y seguridad en las redes universitarias, pero hasta hace poco no se habían planteado soluciones prácticas para mejorar su funcionamiento o hacerlas más eficientes.

El trabajo de Ríos y Fermín (2009) quiso entender cómo funciona realmente el tráfico en una red universitaria. Para lograrlo, usaron Colasoft Capsa y estuvieron monitoreando la red durante toda una semana, viendo cómo se movían los datos entre los sistemas académicos y administrativos. Con este análisis, encontraron los momentos donde la red se cargaba más, los picos que se formaban cuando la gente descargaba archivos pesados, y las variaciones que afectaban el rendimiento. Aunque la infraestructura funcionaba bien en general, estos cambios puntuales dejaron claro que es fundamental estar monitoreando el tráfico todo el tiempo.

Su investigación muestra que vigilar la red de forma constante ayuda a evitar fallas antes de que pasen, planificar mejoras con anticipación y asegurar un servicio confiable, especialmente cuando hay muchas aplicaciones funcionando al mismo tiempo y compitiendo por los mismos recursos.

En los últimos años, varios estudios han demostrado que las redes actuales, sobre todo las que incluyen dispositivos IoT, todavía no tienen sistemas lo suficientemente sólidos para detectar y controlar el tráfico extraño o fuera de lo normal. Esta falta de herramientas especializadas no solo afecta el rendimiento de la infraestructura tecnológica, sino que también hace más difícil identificar a tiempo cualquier irregularidad o posible fallo.

Sobre este tema, Vigoya Morales (2023) señala que la falta de sistemas específicos para detectar anomalías en el tráfico IoT ha despertado un interés creciente entre los investigadores, quienes buscan desarrollar soluciones que permitan identificar comportamientos raros de forma eficiente (p. 4). Este planteamiento refuerza la necesidad de implementar herramientas de monitoreo más potentes en las redes institucionales. Un ejemplo claro es Zabbix, que ayuda a gestionar mejor el tráfico,

detectar problemas antes de que se agraven y asegurar un buen nivel de calidad en el servicio.

La seguridad en las redes informáticas se ha vuelto un tema fundamental, especialmente porque cada vez hay más amenazas y necesitamos herramientas que puedan detectar actividades sospechosas en el tráfico de datos. Sobre esto, Guinea Cabrera (2023) explica que los sistemas de detección de intrusos (IDS) son una herramienta poderosa para defenderse de intentos de invasión a redes privadas, ya que monitorean el tráfico que circula por la red y alertan cuando detectan algo fuera de lo común (pp. 60–66).

Esto deja claro lo importante que es vigilar constantemente cómo se comporta la red para anticipar a los riesgos y proteger la infraestructura tecnológica. Para esta investigación, este punto es clave porque confirma que el monitoreo continuo ya sea con IDS, sistemas de análisis o plataformas como Zabbix es indispensable para mantener la estabilidad y la calidad del servicio en redes institucionales como la de la UPEC.

Yaseen et al. (2021) hicieron un análisis detallado sobre cómo funcionan los sistemas de monitoreo en grandes centros de datos, buscando formas más eficientes de recopilar información sin disparar los costos operativos. Durante su investigación, notaron que aunque estos lugares monitorean constantemente cosas como la latencia, el uso de los enlaces, la temperatura de los equipos y los errores en la red, muchas de estas mediciones se hacen con demasiada frecuencia. Esto termina consumiendo recursos de manera innecesaria: espacio de almacenamiento, capacidad de procesamiento y ancho de banda.

Para resolver este problema, los autores aplicaron conceptos del procesamiento de señales, en particular el teorema de Nyquist Shannon, para determinar la frecuencia mínima con la que se puede medir sin perder información importante. Con esto demostraron que es posible reducir bastante los costos sin afectar la calidad del análisis. Como ellos mismos indican, monitorear continuamente una amplia variedad de métricas de rendimiento y fallas se ha convertido en una parte crucial para operar redes de centros de datos a gran escala (Yaseen et al., 2021, p. 1), destacando la importancia de tener soluciones de monitoreo continuas pero eficientes.

Este estudio es valioso para mi investigación porque refuerza la necesidad de implementar herramientas accesibles, de bajo costo y capaces de ofrecer

supervisión constante, como lo hace Zabbix en redes institucionales como la de la UPEC.

Guo, Li, Liu y Yang (2023) desarrollaron un modelo de gestión de tráfico para redes de backbone en entornos IoT utilizando redes neuronales gráficas (GNN). Su estudio demostró que, cuando el tráfico crece de forma descontrolada, la red empieza a sufrir problemas de rendimiento como congestión, latencia elevada y pérdida de paquetes, especialmente en infraestructuras donde muchos dispositivos comparten los mismos recursos. Los autores muestran que el análisis inteligente del tráfico permite detectar patrones de saturación antes de que afecten el servicio, lo cual resulta fundamental para instituciones que dependen de la conectividad continua.

Aunque el trabajo está orientado a redes IoT, sus conclusiones son aplicables a entornos educativos como la UPEC, donde cientos de dispositivos se conectan simultáneamente y generan cargas variables a lo largo del día. Este antecedente confirma la importancia de monitorear el tráfico en tiempo real, analizar comportamientos anómalos y aplicar mecanismos de gestión preventiva para evitar la congestión, lo que respalda directamente el uso de herramientas de monitoreo como Zabbix en infraestructuras académicas.

2.2. MARCO TEÓRICO

2.2.1 Redes IP

Las redes IP (Internet Protocol) son básicamente la columna vertebral de cómo comunicamos digitalmente hoy en día. Son el medio que permite que nuestros dispositivos intercambien información, ya sea a través de Internet o de redes privadas. Este protocolo establece las reglas de juego: cómo se dividen los datos en pequeños paquetes, cómo encuentran su camino y cómo se vuelven a armar cuando llegan a su destino. "Effective traffic monitoring is essential for maintaining stable and reliable network performance in modern IoT backbone infrastructures."(Guo et al., 2023, p. 2).

Si pensamos en una institución como la Universidad Politécnica Estatal del Carchi (UPEC), las redes IP son las que mantienen funcionando todo lo importante: las aulas virtuales, el correo institucional, los sistemas de información, la transferencia de archivos y las videoconferencias. El problema es que cada vez hay más usuarios y más dispositivos conectados, lo que genera una cantidad enorme de tráfico. Si este tráfico no se maneja bien, empezamos a ver problemas: la red se congestiona, todo

va más lento y se pierden paquetes de datos, lo cual afecta directamente la calidad del servicio que reciben los usuarios.

En redes de alta velocidad, el aumento del tráfico combinado con la falta de políticas claras de administración puede crear cuellos de botella que terminan bajando el rendimiento general. Por eso es tan importante implementar políticas que prioricen ciertos tipos de tráfico y mantener un monitoreo constante para asegurar que todo funcione de manera estable.

Al final del día, las redes IP no son solo el canal por donde pasa la información entre sistemas, sino que son un elemento estratégico fundamental que define si las operaciones pueden continuar sin problemas y si los servicios tecnológicos de una institución educativa funcionan de manera eficiente.

2.2.2 Tráfico de Red

El tráfico de red es básicamente todo el flujo de datos que se mueve por una infraestructura tecnológica en un momento dado. Hablamos de diferentes tipos de información que viajan al mismo tiempo: voz, video, archivos, contenido multimedia, y más, todos compitiendo por los mismos recursos del sistema. Como señala S. Saha, 2022 We investigated and evaluated the performance of different statistical prediction models for real IP network traffic; and showed a significant improvement in prediction using the rolling prediction technique.

En las redes de instituciones como universidades, el tráfico puede cambiar drásticamente según la hora del día, cuánta gente está conectada y qué aplicaciones están usando. Por ejemplo, en la UPEC durante las horas más ocupadas, la red puede saturarse porque todos están usando plataformas al mismo tiempo. Esto no solo hace que todo vaya más lento, sino que afecta directamente la experiencia de los usuarios y puede incluso impactar el rendimiento académico de estudiantes y docentes.

Para entender qué está pasando en la red, se usan herramientas de monitoreo como Wireshark, NetFlow, MRTG o Zabbix. Estas permiten ver en tiempo real cómo está funcionando la red, identificar dónde se están formando cuellos de botella, detectar si se están perdiendo paquetes de datos, medir las variaciones en la latencia (lo que se conoce como jitter) y encontrar comportamientos raros que podrían ser señal de problemas de seguridad (IBM, 2023).

Tener un buen control del tráfico es fundamental para que las redes modernas funcionen de manera eficiente y estable, especialmente cuando hay muchos dispositivos conectados. En el caso de la UPEC, analizar el tráfico no solo ayuda a entender mejor cómo se comporta la red, sino que también permite crear una base sólida para implementar políticas de optimización que sean sostenibles a largo plazo.

2.2.3 Calidad de Servicio (QoS)

La calidad de servicio, o QoS (Quality of Service), se refiere básicamente a todas esas técnicas y mecanismos que usa una red para ofrecer un rendimiento estable y apropiado según el tipo de tráfico que esté manejando. La idea principal es asegurar que las aplicaciones más delicadas, como las llamadas por Internet, las videoconferencias o los sistemas que funcionan en tiempo real, reciban la prioridad que necesitan para operar sin problemas. Como bien lo explica Fortinet, "la QoS es el uso de mecanismos o tecnologías que funcionan en una red para controlar el tráfico y garantizar el rendimiento de aplicaciones críticas con capacidad de red limitada" (Fortinet, s. f.).

En la práctica, lo que hace la QoS es permitir que la red reserve ancho de banda para ciertos servicios, reduzca los retrasos (latencia) y las variaciones en esos retrasos (jitter), y evite que se pierdan paquetes de datos. Todo esto hace que la experiencia del usuario se mantenga fluida incluso cuando hay mucha gente usando la red al mismo tiempo. Esto es particularmente importante en lugares como la UPEC, donde miles de dispositivos y usuarios están conectados simultáneamente realizando actividades académicas, administrativas y de investigación.

Por eso, la calidad de servicio se considera un indicador clave de cómo está funcionando realmente la red. Al monitorear cosas como cuánto ancho de banda se está usando (medido en Mbps), cuántos paquetes por segundo está procesando la red (pps), la latencia (en milisegundos) y el jitter, podemos saber si la red está cumpliendo con lo que se espera de ella. Cuando la QoS es buena, las aplicaciones funcionan sin problemas, las videollamadas no se cortan y todos los servicios están disponibles. Pero cuando la QoS es mala, empiezan a aparecer retrasos, la calidad del audio y video baja, hay desconexiones y todo tipo de interrupciones molestas.

En el contexto del monitoreo con herramientas como Zabbix, la QoS cobra aún más importancia. Con sus paneles de control, gráficos que muestran lo que está pasando en tiempo real y mapas de la red, se puede detectar cuándo hay congestión,

identificar comportamientos extraños en el tráfico y anticiparse a posibles fallos que podrían dejar servicios fuera de línea. Esto le permite al equipo de TIC actuar rápido, ya sea ajustando las prioridades del tráfico, aplicando nuevas políticas de gestión o reservando los recursos que hacen falta.

Dado que estamos hablando de la variable "Calidad de Servicio (QoS)", tiene mucho sentido usar indicadores como latencia, jitter, pérdida de paquetes, disponibilidad del servicio y uso del ancho de banda. Cada uno de estos refleja directamente el nivel de desempeño real que está experimentando el usuario final.

En resumen, la QoS no es solo un concepto técnico más, sino que se convierte en algo fundamental para garantizar una experiencia educativa digital confiable. Esto es especialmente cierto en instituciones como la UPEC, que cada vez dependen más de plataformas virtuales, servicios en línea y una conectividad estable para llevar adelante sus actividades del día a día.

2.2.4 Relación entre Tráfico IP y Calidad de Servicio

La relación entre el tráfico IP y la calidad de servicio (QoS) es realmente estrecha y crucial, porque la forma en que se comporta el tráfico en la red afecta directamente lo que experimentan los usuarios. Conforme aumenta el número de dispositivos conectados, se diversifican las aplicaciones que usamos y crece el volumen de datos que se transmiten, la red puede empezar a mostrar señales de saturación, la velocidad puede volverse irregular o la latencia puede aumentar. Todo esto impacta inmediatamente la QoS, especialmente en aplicaciones delicadas como las videollamadas, las plataformas educativas en línea, las transmisiones en vivo o los sistemas institucionales que necesitan estabilidad y tiempos de respuesta rápidos.

Como señala Cisco (2020), "el crecimiento del tráfico IP exige mecanismos eficientes de gestión y priorización para asegurar que los servicios críticos mantengan niveles aceptables de rendimiento". Esto pone de relieve que el tráfico IP no es solo la cantidad de información que viaja por la red, sino también la calidad con la que los usuarios realmente experimentan los servicios digitales.

Cuando el tráfico se mantiene dentro de los límites que la red puede manejar, todo funciona con fluidez y la QoS se mantiene en buenos niveles. Sin embargo, cuando la demanda supera la capacidad disponible del ancho de banda o se concentra en ciertos momentos (como pasa en las horas pico en instituciones educativas), empiezan a aparecer problemas: congestión, pérdida de paquetes, aumentos en la

latencia y jitter. Todo esto termina afectando directamente la calidad del servicio y la experiencia que tienen los usuarios.

Por eso es tan importante hacer un monitoreo constante del tráfico IP. Este seguimiento permite anticipar a los picos de carga, detectar comportamientos raros o inusuales, y aplicar estrategias de administración que distribuyan los recursos de la red de manera más eficiente. Herramientas como Zabbix juegan un papel fundamental aquí, ya que entregan información en tiempo real sobre el volumen de datos, cómo se está usando el ancho de banda, el estado de las conexiones y el desempeño general de los dispositivos. Con esta información, los equipos de tecnología pueden tomar mejores decisiones, como ajustar las prioridades del tráfico, ampliar la capacidad de ciertos enlaces o modificar las políticas de gestión para mantener la QoS en niveles aceptables.

En conclusión, mientras el tráfico IP muestra el flujo de información que circula por la red, la QoS indica qué tan bien la infraestructura está respondiendo a esa demanda. Ambas variables están completamente interconectadas: un tráfico elevado sin una gestión adecuada puede deteriorar significativamente la calidad del servicio, pero con un monitoreo eficiente y políticas de control bien implementadas, es posible mantener la QoS estable incluso cuando hay mucha demanda.

2.2.5 Herramientas y Técnicas de Gestión del Tráfico con QoS

La gestión del tráfico es algo fundamental para asegurar una buena Calidad de Servicio (QoS) en las redes IP. Básicamente, su trabajo consiste en organizar, priorizar y controlar cómo fluyen los datos por la red, evitando que se congestione, reduciendo los retrasos y asegurando que las aplicaciones más delicadas puedan funcionar sin problemas. A medida que las redes crecen con más usuarios, más dispositivos y más aplicaciones, se vuelve cada vez más necesario tener técnicas y herramientas que permitan administrar todo ese tráfico de manera eficiente y adaptada a lo que realmente necesita el entorno.

En este sentido, Juniper Networks (2021) señala que "la gestión de tráfico basada en QoS permite asignar prioridades y recursos de red de forma inteligente, asegurando que los servicios esenciales mantengan un rendimiento estable incluso bajo condiciones de alta demanda". Esto resalta que la QoS no es solo medir cómo está funcionando la red, sino también aplicar mecanismos que garanticen que los datos circulen de forma ordenada y eficiente.

Entre las técnicas más utilizadas están las siguientes:

2.2.5.1 Clasificación y marcado de paquetes

Esta técnica permite identificar qué tipo de tráfico está pasando por la red y ponerle etiquetas como DSCP o CoS. Así, los dispositivos que se encargan de dirigir ese tráfico pueden reconocer fácilmente qué paquetes necesitan mayor prioridad.

2.2.5.2 Priorización del tráfico

Una vez que el tráfico está clasificado, se crean colas de prioridad para asegurar que los paquetes más sensibles (como las videollamadas, las llamadas por Internet o los sistemas institucionales importantes) reciban un trato preferencial. Esto ayuda a reducir cortes, retrasos y problemas de calidad.

2.2.5.3 Control de congestión y modelado del tráfico

El traffic shaping controla la velocidad de transmisión para evitar que la red se sature y para suavizar los picos de uso, mientras que el policing se asegura de que no se sobrepase el ancho de banda asignado. Estas técnicas ayudan a que la red se mantenga estable.

2.2.5.4 Asignación de ancho de banda

Esto consiste en reservar una parte del ancho de banda específicamente para servicios esenciales. Es especialmente útil en instituciones que dependen de plataformas educativas en línea, reuniones virtuales o servicios administrativos que no pueden fallar.

2.2.5.5 Enrutamiento basado en rendimiento

Algunas redes tienen la capacidad de elegir rutas más eficientes según la latencia, la pérdida de paquetes o el nivel de congestión que haya en ese momento, buscando siempre mejorar el rendimiento final del servicio.

2.2.5.6 Monitoreo en tiempo real

Herramientas como Zabbix, NetFlow, SNMP o sFlow proporcionan información actualizada constantemente sobre cómo se está comportando el tráfico y en qué estado está la red. Con estas métricas (latencia, jitter, uso de ancho de banda, pérdida de paquetes) es posible detectar anomalías y ajustar las políticas de tráfico justo cuando se necesita.

En conjunto, todas estas técnicas y herramientas permiten mantener redes más equilibradas, estables y adaptadas a lo que necesitan sus usuarios. En entornos institucionales, donde conviven múltiples aplicaciones y servicios al mismo tiempo, la gestión del tráfico basada en QoS se convierte en algo esencial para garantizar una experiencia digital confiable, continua y de alto rendimiento.

2.2.6 Debian

Debian se ha ganado un lugar muy respetado dentro del mundo tecnológico como una de las distribuciones de GNU/Linux más confiables, gracias a su estabilidad, seguridad y a la filosofía comunitaria que hay detrás de su desarrollo. Su arquitectura está diseñada para funcionar en entornos donde la fiabilidad no es negociable, como servidores de producción, infraestructuras institucionales y sistemas de monitoreo que necesitan estar disponibles todo el tiempo. Este enfoque se refleja en su política de actualizaciones, que es bastante cautelosa: incorpora nuevas versiones de software solo cuando ya han sido probadas a fondo, lo que garantiza un sistema predecible, seguro y que no falla de manera inesperada. Por todo esto, Debian es muy usado en administraciones públicas, universidades y centros de datos que necesitan entornos robustos y en los que puedan confiar.

Una de sus características más destacadas es su sistema de gestión de paquetes basado en APT, una herramienta que hace muy fácil instalar, actualizar y administrar software sin tener que detener servicios importantes. Esta ventaja es particularmente útil cuando el sistema soporta herramientas de monitoreo como Zabbix, ya que el sistema operativo tiene que coordinar servicios web, bases de datos y procesos de red sin poner en riesgo la estabilidad del servidor. A esto se le suma su fuerte enfoque en la seguridad, respaldado por un equipo que se dedica a analizar vulnerabilidades, aplicar parches y mantener repositorios confiables, lo que ayuda a preservar la integridad del sistema en entornos críticos.

La documentación oficial destaca que «Debian is renowned for being a very stable and secure operating system, suitable for servers and critical environments» (Debian Project, 2024). Este reconocimiento se basa en su amplia comunidad de desarrolladores, su ciclo de soporte prolongado y la transparencia en todo su proceso de desarrollo. Todas estas características hacen de Debian una plataforma sólida para sistemas de monitoreo de red, donde mantener las operaciones funcionando

es fundamental para capturar métricas de disponibilidad, tráfico y desempeño en tiempo real.

En conclusión, Debian se posiciona como una opción muy recomendable para servidores de monitoreo. Su estabilidad probada, combinada con ciclos de actualización controlados y un sistema de administración eficiente, proporciona una base sólida para que plataformas como Zabbix funcionen bien. Estas cualidades reducen los riesgos operativos y aseguran que los procesos de supervisión se ejecuten de manera continua, incluso cuando hay mucha demanda.

2.2.7 PostgreSQL

PostgreSQL es un sistema de gestión de bases de datos relacional de código abierto que se ha ganado una sólida reputación gracias a su arquitectura comprobada, su fiabilidad y su capacidad para mantener la integridad de los datos, incluso en entornos críticos. Según su sitio oficial, «PostgreSQL has earned a strong reputation for its proven architecture, reliability, data integrity, robust feature set, extensibility, and the dedication of the open-source community behind the software to consistently deliver performant and innovative solutions».

Desde la conformidad con el modelo ACID, la posibilidad de extenderla con tipos de datos personalizados y funciones definidas por el usuario, hasta su soporte para sistemas operativos variados, PostgreSQL ofrece un marco sólido para la gestión de la información. En su uso en contextos de monitoreo de red como el que se implementa para la variable "Tráfico de redes IP" y su impacto en la "Calidad de Servicio (QoS)", estas cualidades resultan fundamentales: permiten capturar grandes volúmenes de métricas con consistencia, almacenarlas con integridad, procesarlas mediante consultas complejas y soportar un acceso simultáneo por múltiples usuarios sin degradación significativa del rendimiento.

Al definir indicadores como Mbps, paquetes por segundo, tipos de protocolo y horas pico, y al emplear herramientas como Zabbix para la supervisión, la elección de PostgreSQL permite garantizar que los datos recopilados sean almacenados, consultados y presentados de manera confiable. La capacidad de particionar tablas, optimizar consultas, manejar replicación y soportar cargas elevadas contribuye directamente a asegurar que la infraestructura de monitoreo funcione de forma robusta y emplee los datos como un pilar para mejorar la QoS.

Por lo tanto, PostgreSQL no solo cumple con los requisitos técnicos de un entorno de monitoreo, sino que también ofrece una plataforma escalable, flexible y orientada a entornos institucionales de gran demanda, como es el caso de una universidad que gestiona redes intensivas y busca mejorar el servicio a estudiantes, facultad y administración.

2.2.7.1 Tabla comparativa PostgreSQL

Tabla 1. Tabla comparativa PostgreSQL

Criterio	MySQL/MariaDB	PostgreSQL	Referencias
Rendimiento en cargas altas	Bueno	Excelente	Zabbix LLC. (2024)
Concurrencia	Media	Alta	Zabbix LLC. (2024)
Escalabilidad	Aceptable	Superior	Zabbix LLC. (2024)
Integridad de datos	Buena	Muy alta	Zabbix LLC. (2024)
Funciones avanzadas	Limitadas	Completas	Zabbix LLC. (2024)
Compatibilidad Zabbix	Compatible	Altamente recomendada	Zabbix LLC. (2024)
Consumo de recursos	Bajo-Medio	Medio	Zabbix LLC. (2024)
Facilidad administración	Fácil	Media	Zabbix LLC. (2024)
Respaldo y recuperación	Buenas	Muy robustas	Zabbix LLC. (2024)
Uso empresarial	Popular	Estándar crítico	Zabbix LLC. (2024)

La razón por la que PostgreSQL se erige como la mejor opción para un sistema de monitoreo es que combina tres factores esenciales: rendimiento, integridad de datos y escalabilidad. Gracias a su arquitectura orientada a transacciones, su excelente manejo de concurrencia y su capacidad para gestionar grandes volúmenes de métricas sin perder estabilidad, PostgreSQL garantiza que los datos de tráfico de red sean tratados con fiabilidad. En un entorno universitario donde la calidad del servicio depende de la correcta supervisión de la red, elegir PostgreSQL significa contar con una base sólida que respalde procesos de recolección, análisis e interpretación de datos y que así la variable dependiente "Calidad de Servicio (QoS)" sea medida con precisión, consistencia y bajo riesgo de fallo o latencia.

2.2.8 Nginx

Nginx es un servidor web de alto rendimiento que se usa muchísimo en infraestructuras modernas, principalmente por su arquitectura ligera y eficiente. A diferencia de otros servidores que funcionan con procesos o hilos, Nginx utiliza un modelo orientado a eventos que le permite manejar miles de conexiones al mismo tiempo sin consumir demasiados recursos. Esta característica lo posiciona como una solución ideal para plataformas de monitoreo de red, donde se requiere rapidez, estabilidad y capacidad para atender múltiples solicitudes al mismo tiempo.

Dentro de sistemas como Zabbix, el servidor web juega un papel esencial, ya que es responsable de entregar gráficos, paneles, alertas y reportes que se actualizan constantemente. En este contexto, Nginx contribuye a mejorar el rendimiento general al servir contenido estático como imágenes, hojas de estilo y scripts con gran rapidez, a la vez que trabaja eficientemente junto a PHP-FPM, tecnología necesaria para ejecutar el frontend de Zabbix. Su diseño optimizado reduce la latencia, minimiza el uso de memoria y evita bloqueos que puedan afectar la visualización de las métricas en tiempo real.

La documentación oficial destaca estas ventajas al señalar que «Nginx was built to offer low memory usage and high concurrency, and it has been used to run some of the largest sites on the Internet» (NGINX, 2024). Este principio de diseño se refleja directamente en entornos institucionales y empresariales donde varios usuarios consultan simultáneamente información relacionada con el tráfico de red, la disponibilidad de servicios y la calidad del funcionamiento general de la infraestructura tecnológica. Gracias a su eficiencia, Nginx mantiene una respuesta estable incluso frente a cargas elevadas, lo que lo convierte en un componente estratégico para garantizar la fiabilidad del monitoreo.

2.2.8.1 Tabla comparativa Nginx

Tabla 2. Tabla comparativa Nginx

Criterio	Apache	Nginx	Referencias
Modelo de procesamiento	Procesos/Hilos	Eventos	Sysoev, I. (2024)
Rendimiento bajo carga	Bueno	Excelente	Sysoev, I. (2024)
Consumo de recursos	Alto	Muy bajo	Sysoev, I. (2024)
Velocidad estática	Buena	Muy alta	Sysoev, I. (2024)
Compatibilidad Zabbix	Compatible	Recomendado	Sysoev, I. (2024)
Escalabilidad	Media	Alta	Sysoev, I. (2024)
Facilidad configuración	Alta	Media	Sysoev, I. (2024)
Seguridad	Buena	Muy alta	Sysoev, I. (2024)
Uso moderno	Menor	Muy común	Sysoev, I. (2024)

Nginx es considerado la mejor opción para implementar un sistema de monitoreo como Zabbix debido a su capacidad para manejar un alto número de conexiones con un bajo consumo de recursos. Su arquitectura moderna facilita tiempos de respuesta más rápidos, mayor estabilidad en la entrega de dashboards y un rendimiento constante aun cuando la plataforma procesa múltiples métricas en tiempo real. Estas ventajas aseguran una experiencia de monitoreo más fluida y confiable, especialmente en instituciones que requieren supervisión continua del tráfico de red y de la calidad del servicio.

2.2.9 Versión SNMP

El protocolo Simple Network Management Protocol (SNMP) constituye un estándar universal para la gestión y supervisión de dispositivos de red como routers, switches, servidores, impresoras y enlaces de comunicación en entornos IP. Gracias a él, los administradores pueden recopilar métricas en tiempo real, detectar fallos, analizar el rendimiento y centralizar la administración de los equipos bajo una visión única. SNMP trabaja mediante agentes instalados en cada dispositivo y un sistema de monitoreo por ejemplo, Zabbix que consulta periódicamente dicha información con el fin de generar alertas y reportes para garantizar la operatividad de la red.

"In typical uses of SNMP … administrative computers called managers have the task of monitoring or managing a group of hosts or devices on a computer network. Each managed system executes a software component called an agent that reports information via SNMP to the manager." (Wikipedia, 2025)

2.2.9.1 SNMPv2c para Zabbix

2.2.9.1.1 Facilidad de configuración en Zabbix

SNMPv2c requiere únicamente una community string, lo que permite configurarlo de manera rápida y sencilla en distintos dispositivos sin necesidad de ajustes avanzados. Esta simplicidad resulta especialmente útil en entornos donde se manejan equipos variados.

2.2.9.1.2 Mayor compatibilidad con la infraestructura actual

Gran parte de los dispositivos institucionales incluidos switches, routers y equipos con varios años de uso mantienen un mejor funcionamiento con SNMPv2c que con SNMPv3, lo cual facilita su integración dentro del sistema de monitoreo.

2.2.9.1.3 Menor consumo de recursos

Al no incorporar procesos de cifrado, SNMPv2c demanda menos procesamiento en los dispositivos. Esto es relevante en equipos que aún están en proceso de actualización y cuyos recursos deben administrarse con eficiencia.

2.2.9.1.4 Compatibilidad total con Zabbix

Zabbix ofrece soporte nativo para SNMPv2c en la mayoría de sus plantillas y funciones, lo que permite obtener métricas sin complicaciones adicionales y con un alto nivel de estabilidad.

2.2.9.1.5 La naturaleza del proyecto es técnica, no de seguridad

El propósito de la tesis se centra en monitorear parámetros como tráfico y estado de las interfaces. Por ello, SNMPv2c es suficiente para cumplir los objetivos, ya que no se busca implementar un sistema avanzado de seguridad de red.

2.2.9.2 Tabla comparativa SNMP

Tabla 3. Tabla comparativa SNMP

Característica	SNMPv1	SNMPv2c	SNMPv3	Referencia
Año de lanzamiento	1988	1993	1998	Zabbix LLC (2024)
Seguridad	Muy baja (solo "community string")	Baja (mismo mecanismo que v1)	Alta (autenticación + encriptación)	Zabbix LLC (2024)
Rendimiento	Básico	Mejor rendimiento: soporte para *bulk requests*	Similar a v2c	Zabbix LLC (2024)
Facilidad de configuración	Muy fácil	Fácil y ampliamente soportado	Más compleja: requiere usuarios, claves y configuración adicional	Zabbix LLC (2024)
Compatibilidad con dispositivos antiguos	Alta	Muy alta	Media (no todos los equipos antiguos lo soportan)	Zabbix LLC (2024)
Uso actual	Poco usado	Muy usado en redes institucionales	Estandar recomendado para seguridad	Zabbix LLC (2024)
Idoneidad para monitoreo básico (Zabbix)	Aceptable	Excelente	Excelente	Zabbix LLC (2024)
Idoneidad para redes con políticas de seguridad estrictas	No recomendado	No recomendado	Recomendado	Zabbix LLC (2024)
Encriptación	No	No	Sí	Zabbix LLC (2024)
Autenticación fuerte	No	No	Sí	Zabbix LLC (2024)

Aunque SNMPv3 ofrece el nivel más alto de seguridad dentro del protocolo, su implementación exige configuraciones más complejas, como la creación de usuarios, la gestión de autenticación y el uso de encriptación. Estos requisitos todavía no están implementados en la infraestructura actual de la UPEC, lo que hace complicado desplegarlos de inmediato.

Por eso se decidió usar SNMPv2c, ya que funciona perfectamente con los equipos que ya existen, es fácil de configurar y Zabbix lo soporta de forma nativa. Esta versión permite lograr los objetivos del monitoreo de manera eficiente, sin añadir una carga operativa o técnica que no sea necesaria.

2.2.10 Zabbix como herramienta de monitoreo de red

Zabbix es una plataforma de monitoreo de red de código abierto que se ha posicionado como una de las soluciones más completas y confiables para supervisar infraestructuras tecnológicas modernas. Su objetivo principal es dar una visión clara y en tiempo real de cómo se están comportando los recursos de red, servidores, servicios y dispositivos críticos, permitiendo que las instituciones puedan detectar fallos, analizar tendencias y asegurar que todo siga funcionando.

Una de las cosas que distingue a Zabbix de otras herramientas de monitoreo es su capacidad de adaptarse según las necesidades de cada organización. Esto significa que puede usarse tanto en redes pequeñas, como laboratorios o departamentos, como en infraestructuras grandes y distribuidas, como universidades, empresas públicas o centros de datos. Esta versatilidad es posible gracias a su diseño modular y a que soporta múltiples formas de recolectar datos, como SNMP, ICMP, agentes, APIs, scripts personalizados, entre otros.

La propia documentación oficial de Zabbix resalta esta capacidad al afirmar que: "Zabbix is designed to scale from small environments to enterprise-level deployments, capable of processing millions of metrics per second depending on hardware and configuration." (Zabbix Documentation, 2024)

Esta cita confirma que Zabbix no solo es flexible, sino también lo suficientemente potente para manejar cantidades enormes de información. Esta capacidad es especialmente importante cuando se monitorea tráfico IP, ya que implica registrar constantemente métricas como el uso de ancho de banda, paquetes enviados y recibidos, latencia, jitter, disponibilidad de dispositivos, carga de CPU, saturación de interfaces, entre otros indicadores clave para evaluar la calidad del servicio (QoS).

Otro aspecto fundamental de Zabbix es su enfoque preventivo. A través de alertas inteligentes, la herramienta puede identificar comportamientos raros o valores que superan los límites establecidos, avisando de inmediato al equipo técnico. Esto permite actuar antes de que ocurra una falla mayor o antes de que los usuarios finales noten que el servicio está fallando. Por ejemplo, si una interfaz de red empieza a registrar un aumento inusual de tráfico o pérdidas de paquetes, Zabbix puede generar una alerta que permita investigar y corregir el problema a tiempo.

Zabbix también ofrece una gran variedad de herramientas visuales, como dashboards, gráficos históricos y mapas de red interactivos. Estas representaciones

facilitan entender datos complejos y permiten identificar patrones o picos de tráfico en horarios específicos, lo cual es vital para gestionar eficientemente el rendimiento de la red. En instituciones educativas como la UPEC, donde miles de usuarios pueden conectarse al mismo tiempo, este tipo de análisis resulta esencial para detectar congestión, planificar ampliaciones de capacidad o verificar si las políticas de QoS están funcionando como deberían.

Además, Zabbix permite centralizar todo el monitoreo en un solo panel, lo que simplifica la gestión de la infraestructura, ya que evita tener que usar múltiples sistemas independientes y mejora la coordinación del equipo técnico. Su carácter open source trae otro beneficio importante: no hay que pagar licencias, lo cual favorece a instituciones públicas que deben trabajar con presupuestos ajustados, sin sacrificar calidad ni funcionalidad.

En resumen, Zabbix se convierte en un pilar fundamental dentro de este estudio, ya que no solo permite observar los indicadores técnicos del tráfico y la QoS, sino que también impulsa una gestión inteligente y preventiva de la red. Su uso contribuye a fortalecer la estabilidad de los servicios institucionales, mejorar la experiencia digital de los usuarios y promover una administración tecnológica basada en datos reales y decisiones oportunas. En definitiva, su implementación en la UPEC representa un paso decisivo hacia una infraestructura de red más eficiente, confiable y moderna.

2.2.10.1 Tabla comparativa de herramientas comerciales

Zabbix se ha consolidado como una de las herramientas de monitoreo más completas porque ofrece libertad total de uso, gran capacidad de control y un desempeño profesional sin necesidad de pagar licencias. A diferencia de plataformas comerciales como LogicMonitor o Dynatrace, su naturaleza open source permite modificarla, ampliarla o integrarla según las necesidades específicas de cada institución, sin depender de terceros ni asumir costos por cada dispositivo que se monitorea. Esto representa una ventaja significativa para organizaciones que manejan presupuestos limitados o que buscan mantener independencia tecnológica.

En términos de rendimiento, Zabbix compite al mismo nivel que las soluciones de pago. Su arquitectura, basada en agentes, proxies y un servidor central, está diseñada para procesar volúmenes enormes de información, alcanzando millones de métricas por segundo sin comprometer la estabilidad. Esta capacidad lo hace

adecuado incluso para sectores muy exigentes, como la banca, las telecomunicaciones o infraestructuras críticas.

Otro de sus puntos más destacados es la flexibilidad. Zabbix permite trabajar con múltiples protocolos y métodos de recolección de datos, como SNMP, agentes propios, IPMI, HTTP, APIs e incluso scripts personalizados. Gracias a esto, es posible supervisar desde servidores y routers hasta aplicaciones, servicios en la nube o equipos especializados, todo desde una sola plataforma.

Su comunidad global también es un pilar importante. Miles de profesionales aportan plantillas, mejoras y soluciones prácticas que enriquecen constantemente la herramienta. A ello se suma el respaldo oficial de Zabbix SIA, la empresa que desarrolla el software, y que ofrece soporte profesional para quienes lo necesiten.

Finalmente, Zabbix brinda un nivel de transparencia y seguridad que muchas herramientas comerciales no pueden igualar. Al operar de manera local, los datos permanecen bajo control institucional, sin pasar por servidores externos ni depender de servicios en la nube para su funcionamiento.

Tabla 4. Tabla comparativa de herramientas comerciales

Criterio	Zabbix (Mejor)	LogicMonitor	Dynatrace	Referencia
Arquitectura	On-prem / open-source, muy flexible (agente + SNMP).	SaaS híbrido (on-prem + multicloud) con >3.000 integraciones.	Plataforma SaaS full-stack con IA Davis y visibilidad profunda.	Zabbix LLC. (2024)
Descubrimiento	Descubrimiento de red y reglas por rangos/IP; plantillas predefinidas.	Auto-descubrimiento y topología en tiempo real.	Descubrimiento automático y mapeo de dependencias (OneAgent).	Zabbix LLC. (2024)
Protocolos y cobertura de red	SNMP nativo + agentes y plantillas; amplio soporte de dispositivos.	Monitorización completa de red y correlación con IA.	Cobertura de red integrada con observabilidad total.	Zabbix LLC. (2024)
Mapas / Topología	Mapas personalizables, requiere algo más de configuración.	Mapeo automático y dashboards modernos.	Visualizaciones modernas y dependencias detalladas.	Zabbix LLC. (2024)
Alertas & AIOps	Alertas potentes y personalizables; sin IA nativa, pero integrable.	Correlación y reducción de ruido con IA avanzada.	Davis AI: detección y root-cause automático.	Zabbix LLC. (2024)
Escalabilidad	Probado para millones de métricas/segundo.	SaaS elástico, escalable mediante paquetes.	Escalabilidad enterprise global.	Zabbix LLC. (2024)
Velocidad de despliegue	Requiere instalación y tuning, pero control total del entorno.	Despliegue rápido y sencillo, sin infraestructura local.	Rápido con OneAgent, curva de aprendizaje alta.	Zabbix LLC. (2024)

Coste / Licencia	Sin coste de licencia, solo mantenimiento interno.	Licencia comercial; precio medio-alto.	Comercial premium, coste elevado.	Zabbix LLC. (2024)
Reconocimientos 2025	Muy usado globalmente, destaca por bajo TCO y flexibilidad.	Top #1 en comparativas 2025 por automatización.	Altamente valorado para observabilidad enterprise.	Zabbix LLC. (2024)
Mejor para…	Equipos técnicos que buscan máximo control y bajo costo.	Empresas medianas/grandes que buscan SaaS listo e IA.	Grandes organizaciones con entornos complejos.	Zabbix LLC. (2024)

En síntesis, Zabbix se posiciona como la mejor alternativa para el monitoreo de redes porque combina libertad, capacidad, seguridad y una comunidad activa, sin sacrificar funcionalidades ni requerir pagos adicionales. Mientras otras herramientas sobresalen por la automatización, Zabbix destaca por algo más valioso: el control total sobre la infraestructura y los datos, con la posibilidad de crecer y adaptarse a futuro sin límites

2.2.10.2 Tabla comparativa de herramientas de monitoreo en el mercado actual

Zabbix se posiciona como la mejor herramienta de monitoreo porque reúne ventajas que las demás soluciones solo ofrecen parcialmente. A diferencia de PRTG, que incrementa sus costos con cada sensor, Zabbix permite crecer sin pagar licencias ni limitar el número de dispositivos. Frente a Nagios XI, que depende de numerosos plugins y requiere mayor experiencia técnica, Zabbix ofrece una plataforma más completa, flexible y sencilla de escalar. En comparación con OpManager, cuya funcionalidad depende de ediciones comerciales, Zabbix brinda libertad total y un monitoreo integral sin restricciones económicas. Y, en contraste con Pandora FMS, que mantiene una comunidad más reducida y un enfoque híbrido entre versiones libres y comerciales, Zabbix cuenta con una comunidad internacional sólida, amplia documentación y un ecosistema en constante crecimiento. Gracias a esta combinación de costo cero, alta escalabilidad, flexibilidad avanzada y fuerte respaldo comunitario, Zabbix se convierte en la opción más conveniente y sostenible para cualquier organización que necesite un monitoreo confiable y de largo plazo.

Tabla 5. Tabla de herramientas de monitoreo en el mercado actual

Criterio	Zabbix	PRTG Network Monitor	Nagios XI	OpManager	Pandora FMS
Tipo de licencia / coste base	Open source, sin coste de licencia base.	Comercial por sensores/dispositivos; coste crece con escala.	Comercial (basado en Nagios Core).	Comercial, con ediciones según dispositivos.	Community + Comercial; solución integral.

Escalabilidad / grandes entornos	Alta, soporta proxies/distribuido, ideal para grandes entornos.	Adecuada, pero costos elevados en entornos grandes.	Escalable pero con complejidad alta.	Buena para redes y entornos híbridos.	Escalable y orientada a entornos grandes.
Flexibilidad / personalización	Muy alta, flexible y personalizable mediante templates y API.	Buena, interfaz amigable pero menos flexible.	Alta personalización pero requiere conocimientos técnicos.	Personalización equilibrada, interfaz moderna.	Muy flexible, pero más compleja de configurar.
Facilidad de uso / curva de aprendizaje	Curva de aprendizaje más pronunciada pero muy potente.	Muy fácil de usar e implementar.	Interfaz tradicional, requiere experiencia.	Instalación rápida y sencilla.	Curva media, interfaz menos intuitiva.
Comunidad / soporte / ecosistema	Amplia comunidad, excelente soporte y documentación.	Soporte comercial, comunidad limitada en versión gratuita.	Gran comunidad y muchos plugins.	Buen soporte empresarial.	Comunidad más pequeña que Zabbix.
Cobertura funcional	Muy amplia: redes, servidores, contenedores, servicios, logs, etc.	Buena cobertura centrada en sensores de red y hardware.	Buena cobertura de infraestructura con plugins adicionales.	Excelente para red y virtualización.	Cobertura completa: infraestructura, apps, negocio, IoT.
Coste total de propiedad (TCO)	Muy favorable, solo requiere recursos de operación y mantenimiento.	Coste aumenta con sensores/licencias.	TCO alto por licencias y configuración.	Coste moderado pero con licencias.	Coste inicial más alto, inversión en configuración.
Justificación por qué sería "mejor"	Licencia libre, flexibilidad, escalabilidad y gran comunidad.	Fácil de instalar, interfaz amigable.	Histórico y personalizable, pero más complejo.	Equilibrio entre facilidad y potencia.	Enfoque integral pero con mayor coste.

En conjunto, Zabbix resulta la mejor alternativa porque combina libertad de uso, escalabilidad, flexibilidad técnica, una comunidad sólida y un bajo coste de operación, manteniendo un rendimiento de nivel empresarial sin las limitaciones que imponen las soluciones comerciales.

III. METODOLOGÍA

3.1. ENFOQUE METODOLÓGICO

3.1.1. Enfoque

Metodología Mixta

El presente estudio adopta una metodología de enfoque mixto, la cual integra de manera complementaria los métodos cuantitativos (CUAN) y cualitativo (CUAL). Esta combinación permite obtener una comprensión más completa del fenómeno investigado, articulando tanto los datos numéricos y medibles como las percepciones y experiencias de los actores involucrados.

Como lo expresa Campos Arenas (2021), el enfoque de métodos mixtos articula los aspectos propios de la investigación cuantitativa y cualitativa, pero al mismo tiempo posibilita desarrollar una teorización propia, así como sus propios diseños de investigación y estrategias de recolección, tratamiento y análisis de datos. De esta manera, se construye una visión más amplia e integrada que combina la precisión del análisis cuantitativo con la riqueza interpretativa del análisis cualitativo.

En el enfoque cualitativo, se busca comprender las particularidades de los medios y tecnologías que intervienen en la gestión del tráfico de red dentro de la Universidad Politécnica Estatal del Carchi. Para ello, se aplicarán entrevistas semiestructuradas dirigidas a los administradores de red y a los usuarios del sistema, con el propósito de conocer sus experiencias, percepciones y opiniones sobre cómo está funcionando la red institucional. Esta información permitirá contextualizar los resultados y aportar una perspectiva más humana al análisis técnico.

Por su parte, el enfoque cuantitativo se usará para medir el impacto del tráfico de red en el rendimiento general de la infraestructura tecnológica. Se analizarán métricas como el ancho de banda utilizado, la tasa de pérdida de paquetes, la latencia promedio y el número de conexiones simultáneas. Estos datos se obtendrán mediante encuestas estructuradas y herramientas de monitoreo de red,

especialmente el sistema Zabbix, que permitirá registrar y procesar información numérica en tiempo real.

En conjunto, este enfoque mixto ofrece una visión completa del problema, donde la profundidad del análisis cualitativo aporta contexto y comprensión, mientras que la precisión de los datos cuantitativos garantiza objetividad y confiabilidad en los resultados. Así, se obtendrá una descripción integral del comportamiento del tráfico de red, lo que permitirá identificar las carencias que existen y proponer soluciones concretas para optimizar la calidad del servicio (QoS) dentro del entorno universitario.

3.1.2. Tipo de Investigación

3.1.2.1 Investigación aplicada

Este estudio se clasifica como aplicado porque no se queda solo en observar o describir lo que ocurre en la red de la Universidad Politécnica Estatal del Carchi (UPEC). Su intención es ir más allá: comprender el problema y proponer soluciones que realmente puedan implementarse para mejorar el funcionamiento de la red. Como explican Hernández, Fernández y Baptista (2022), la investigación aplicada se enfoca en resolver necesidades concretas apoyándose en conocimientos teóricos y prácticos. En este caso, el propósito es aportar mejoras visibles en la infraestructura tecnológica de la universidad y ofrecer una experiencia más estable a toda la comunidad académica.

3.1.2.2 Alcance Investigación descriptiva–correlacional

El alcance del estudio es descriptivo correlacional. Esto significa que, primero, se describe cómo se comporta el tráfico de red en su estado natural: cuánto ancho de banda se consume, cómo varía la latencia, cuándo se presentan picos de uso, entre otros aspectos técnicos.

Luego, se analiza cómo se relaciona ese comportamiento con la calidad del servicio que perciben los usuarios. Tal como plantean Hernández-Sampieri, R., Fernández-Collado, C., & Baptista-Lucio, M. del P. (2014). este tipo de alcance permite entender los vínculos entre variables sin necesidad de intervenirlas. En esta investigación, esa correlación es clave para identificar qué factores están afectando el rendimiento de la red.

3.1.2.3 Diseño

3.1.2.3.1 Diseño no experimental

El estudio es no experimental, porque no se modifican las condiciones en las que funciona la red. No se alteran equipos, no se cambian configuraciones ni se provocan escenarios artificiales. Lo que se busca es observar la red tal como opera diariamente, para obtener un diagnóstico fiel sobre los problemas que presenta.

3.1.2.3.2 Diseño de corte transversal

Además, se trata de un estudio de corte transversal, ya que la información se recopiló en un periodo específico. Este tipo de enfoque permite obtener una visión clara y puntual del estado actual de la red, lo que resulta ideal cuando el objetivo es conocer la situación real y usar esos datos como base para decisiones de mejora.

3.1.2.4 Enfoque metodológico

3.1.2.4.1 Enfoque mixto

El trabajo utiliza un enfoque mixto, combinando dos perspectivas que se complementan entre sí.

Por un lado, está el análisis cuantitativo, que permite interpretar métricas objetivas como el tráfico, la latencia o la pérdida de paquetes. Por otro lado, está la parte cualitativa, que recoge experiencias y opiniones de los usuarios y administradores sobre el rendimiento de la red.

Al integrar ambas visiones, se obtiene una comprensión más completa del problema, tanto desde lo técnico como desde lo humano.

3.1.2.5 Conclusión metodológica

En resumen, esta investigación se caracteriza por ser aplicada, descriptiva correlacional, no experimental, de corte transversal y con un enfoque mixto. Todo este conjunto metodológico permite estudiar el comportamiento real del tráfico en la red de la UPEC y, al mismo tiempo, plantear soluciones prácticas que contribuyan a mejorar la calidad del servicio. Es un enfoque que combina análisis, evidencia y acción, con la finalidad de brindar beneficios directos a la comunidad universitaria.

3.2. IDEA A DEFENDER

La congestión del tráfico de red perjudica el desempeño de las conexiones afectando la calidad de servicio en la Universidad Politécnica Estatal del Carchi.

¿Cómo afecta el crecimiento del tráfico digital en la calidad de los servicios y qué soluciones de monitoreo en tiempo real podrían optimizar el rendimiento de la red en la Universidad Politécnica Estatal del Carchi?

3.3. DEFINICIÓN Y OPERACIONALIZACIÓN DE LAS VARIABLES

En esta investigación se identifican dos variables principales: la variable independiente, que corresponde al tráfico de redes IP, y la variable dependiente, que es la calidad de servicio (QoS). Ambas están directamente relacionadas, porque cuando aumenta el tráfico, esto afecta el rendimiento general de la red y la experiencia que tienen los usuarios.

3.3.1 Variable independiente VI = Tráfico de redes IP

El tráfico de redes IP representa el movimiento constante de datos entre los dispositivos que están conectados a una red. Básicamente refleja cuánta información se está transmitiendo y en qué momentos hay mayor congestión.

Para analizarlo se consideran indicadores como cuánto ancho de banda se está consumiendo, el número de paquetes por segundo que circulan y los horarios en que la red se satura. Todo esto se mide mediante herramientas de monitoreo como Zabbix, Wireshark, NetFlow y MRTG.

El tráfico IP es fundamental para entender cómo está funcionando una red, ya que cuando aumenta demasiado puede causar lentitud, pérdida de datos y una disminución general en la eficiencia.

3.3.2 Variable dependiente VD= Calidad de Servicio (QoS)

La calidad de servicio (QoS) se refiere a la capacidad que tiene la red para mantener una conexión estable, continua y eficiente, asegurando que los datos lleguen a su destino sin interrupciones.

Esta variable se mide a través de indicadores como la latencia, el jitter, la pérdida de paquetes, qué tan disponible está el servicio y qué tan satisfechos están los usuarios.

Una buena gestión de QoS permite darles prioridad a los servicios más críticos y mantener una transmisión fluida incluso cuando hay mucha demanda.

3.3.3 Relación entre las variables

Existe una relación inversa entre ambas variables:

"A mayor tráfico de redes IP, menor calidad de servicio en términos de latencia y pérdida de paquetes."

Cuando el tráfico crece sin control, la congestión puede reducir el rendimiento general de la red hasta en un 40%, lo que refuerza la necesidad de implementar herramientas de monitoreo y políticas de optimización en instituciones como la UPEC

Tabla 6. Tabla de variables

Variable	Definición	Dimensión	Indicadores	Técnica	Instrumento
VI: Tráfico de redes IP	Es el flujo de datos que viaja por la red y que Zabbix supervisa en cantidad, velocidad y comportamiento de los paquetes.	Ancho de banda	Promedio de Mbps utilizados en los enlaces monitoreados	Observación técnica	Plataforma Zabbix
		Cantidad de paquetes	Promedio de paquetes por segundo (pps) registrados	Observación técnica	Zabbix (gráficos de tráfico)
		Tipo de tráfico	Protocolos predominantes detectados (TCP, UDP, ICMP)	Análisis de tráfico	Zabbix – monitoreo de servicios
		Horas pico	Intervalos horarios con mayor nivel de uso de red	Revisión de registros	Reportes históricos de Zabbix
		Reglas de monitoreo	Número de ítems y disparadores configurados	Revisión documental	Configuración interna de Zabbix
		Alertas generadas	Frecuencia de alertas por congestión o caída de enlace	Observación directa	Panel de alertas de Zabbix
VD: Calidad de servicio (QoS)	Es el desempeño de la red evaluado por latencia, pérdida de paquetes y estabilidad, junto con la percepción de los usuarios sobre la calidad del servicio.	Latencia	Tiempo promedio de respuesta (ms) de los hosts monitoreados	Medición técnica	Zabbix (ping y disponibilidad)
		Pérdida de paquetes	Porcentaje de paquetes no entregados según métricas de Zabbix	Medición técnica	Zabbix (chequeos ICMP)
		Disponibilidad	Porcentaje de tiempo en línea de los dispositivos	Medición técnica	Reportes de disponibilidad de Zabbix
		Jitter	Variación del retardo promedio entre paquetes	Observación técnica	Gráficos de latencia en Zabbix
		Satisfacción del usuario	Nivel de percepción del rendimiento de la red	Encuesta	Cuestionario

3.4. MÉTODOS UTILIZADOS

Para el desarrollo del presente Trabajo de Integración Curricular se aplicaron métodos cuantitativos y cualitativos, en coherencia con el enfoque mixto adoptado en la investigación. La utilización conjunta de ambos métodos permitió obtener una visión integral del comportamiento del tráfico de red en la Universidad Politécnica Estatal del Carchi (UPEC), combinando la precisión numérica de los datos técnicos con las percepciones y experiencias de los usuarios del sistema.

3.4.1 Método cualitativo

El método cualitativo se empleó para comprender las causas y percepciones relacionadas con los problemas de conectividad y calidad de servicio dentro de la institución. Para esto, se realizó una entrevista semiestructurada al Magíster Javier Torres, responsable del Departamento de Tecnologías de la Información y Comunicación (TIC) en el área de redes.

Esta entrevista permitió conocer cómo se administra actualmente el tráfico, qué limitaciones técnicas existen, qué políticas de monitoreo están implementadas y cuál es la percepción institucional sobre qué tan efectivo es el sistema de gestión de red.

La información obtenida se analizó mediante categorización temática, identificando los principales factores que están causando la congestión del tráfico y afectando la estabilidad del servicio.

3.4.2 Método cuantitativo

El método cuantitativo se aplicó con el fin de obtener datos medibles y verificables sobre el estado actual de la red institucional y cómo percibe su rendimiento la comunidad universitaria.

Se aplicaron encuestas estructuradas a tres grupos de usuarios: estudiantes, docentes y personal administrativo de la UPEC.

Las encuestas se diseñaron usando una escala tipo Likert de cinco niveles (1: muy insatisfecho a 5: muy satisfecho), abordando aspectos como la velocidad de conexión, la estabilidad de la red, las interrupciones del servicio y la satisfacción general con el acceso a plataformas institucionales.

Al mismo tiempo, se utilizaron los registros técnicos generados por la herramienta de monitoreo Zabbix, que permitió obtener métricas precisas sobre ancho de banda,

latencia, pérdida de paquetes y disponibilidad de los enlaces de red. Estos datos cuantitativos se compararon con las respuestas de los usuarios, con el fin de establecer correlaciones entre los indicadores técnicos y cómo perciben el servicio.

3.4.3 Integración de métodos

Finalmente, los resultados cualitativos y cuantitativos se integraron en una matriz de análisis comparativo, lo que permitió contrastar la información técnica obtenida por Zabbix con las percepciones humanas recogidas en entrevistas y encuestas. Esta triangulación metodológica fortaleció la validez de los resultados, garantizando una comprensión más completa del fenómeno estudiado y facilitando la formulación de propuestas concretas para optimizar la calidad del servicio de red en la UPEC.

3.4.4 Metodología Ágil Complementaria (Lean IT)

Además del enfoque mixto que guía este estudio, se incorporan los principios de la metodología ágil Lean IT, la cual se centra en mejorar continuamente los servicios tecnológicos reduciendo desperdicios, optimizando procesos y entregando valor real al usuario final. Lean IT resulta especialmente pertinente en el análisis del tráfico IP y la calidad del servicio (QoS), ya que permite ver la red como un flujo de valor continuo, identificar dónde se generan las fallas y aplicar mejoras graduales sin interrumpir las operaciones institucionales. Como señala el Lean IT Association (2017), "Lean IT enables organizations to optimize the value delivered by IT services by eliminating waste, improving processes and increasing quality for the end user" (p. 12).

Esta perspectiva coincide plenamente con la necesidad de la UPEC de fortalecer su red institucional y mejorar la experiencia digital de su comunidad.

En este trabajo, Lean IT se aplica a través de una serie de pasos que se alinean directamente con el diagnóstico del tráfico de red y las necesidades de conectividad de la institución:

3.4.4.1 Identificación del valor

Se determina qué es lo verdaderamente importante para la comunidad universitaria: contar con una red estable, rápida y disponible durante clases, actividades administrativas y uso de plataformas académicas. Este paso permite definir los indicadores esenciales del estudio (como estabilidad percibida, velocidad y patrones de congestión) y orienta la toma de decisiones hacia lo que genera valor real para los usuarios.

3.4.4.2 Mapeo del flujo de valor

Se analiza cómo circula el tráfico dentro de la red institucional, desde los edificios con mayor afluencia hasta los enlaces críticos. Mediante las gráficas de Zabbix se visualizan los momentos donde la red se satura, permitiendo reconstruir el "flujo" real de los datos y comprender cómo este impacto se refleja en la calidad del servicio.

3.4.4.3 Detección de desperdicios

Lean IT llama "desperdicio" a todo elemento que genera retrasos o afecta el valor del servicio. En la red de la UPEC, esto incluye congestión en horas pico, equipos sobrecargados, configuraciones ineficientes y puntos donde se pierde rendimiento. Las encuestas y la entrevista TIC ayudan a identificar estos desperdicios desde la mirada técnica y desde la experiencia del usuario.

3.4.4.4 Medición de indicadores clave

Con herramientas como Zabbix y, cuando existe disponibilidad, Wireshark o NetFlow se registran métricas objetivas (ancho de banda consumido, picos de tráfico, fluctuaciones del enlace). Esta medición construye una línea base que permite comparar el estado inicial de la red con cualquier mejora aplicada posteriormente.

3.4.4.5 Análisis de causa raíz y priorización

Con los datos obtenidos se analizan las verdaderas causas de la saturación o inestabilidad. Lean IT promueve priorizar las intervenciones según su impacto: por ejemplo, mejorar la capacidad del switch de core, gestionar el uso ineficiente del ancho de banda o atender las zonas con mayor congestión señaladas por los usuarios.

3.4.4.6 implementación de mejoras iterativas

En lugar de aplicar cambios radicales, Lean IT sugiere mejoras pequeñas, continuas y progresivas que no afecten la disponibilidad del servicio. En el contexto de la UPEC, esto se traduce en ajustes de configuración, optimización de tráfico, uso más eficiente de las VLAN o mejoras puntuales en la infraestructura según la saturación detectada.

3.4.4.7 Verificación de resultados

Luego de implementar acciones, se comparan las métricas nuevas con las iniciales: si disminuyen los picos de tráfico, si mejora la estabilidad percibida o si aumentan los

periodos de fluidez. Esta verificación es clave para saber si las intervenciones realmente están mejorando la calidad del servicio.

3.4.4.8 Estandarización

Las mejoras que resultan efectivas se documentan para que puedan mantenerse en el tiempo y replicarse en otros segmentos de la red. De esta forma, el equipo TIC puede aplicar procedimientos estandarizados que aseguren un funcionamiento estable.

3.4.4.9 Mejora continua

Lean IT plantea que la optimización nunca termina: cada ciclo de medición, análisis e intervención permite que la red institucional siga adaptándose a las necesidades de sus usuarios. En una universidad donde el uso de plataformas digitales crece continuamente, este enfoque asegura que la gestión del tráfico se mantenga vigente y responda a las demandas reales.

En síntesis, Lean IT no solo complementa la metodología principal del estudio, sino que fortalece el enfoque aplicado de la investigación, proporcionando un marco práctico y flexible para entender, mejorar y sostener el rendimiento de la red institucional. Su integración en este trabajo permite que las propuestas finales no sean únicamente teóricas, sino sostenibles, escalables y alineadas con la realidad tecnológica de la UPEC.

3.5. ANÁLISIS ESTADÍSTICO

El análisis estadístico aplicado en esta investigación tiene como propósito interpretar de manera rigurosa los datos obtenidos a partir de dos fuentes principales:

1. La entrevista al Magíster Javier Torres, Analista de Redes del Departamento de Tecnologías de la Información y Comunicación (TIC) de la UPEC,
2. Las encuestas aplicadas a estudiantes, docentes y personal administrativo de la institución.

El objetivo de este análisis es integrar información cualitativa y cuantitativa para identificar patrones de uso, problemas de desempeño, percepciones de los usuarios y la relación que existe entre el tráfico de redes IP (variable independiente) y la calidad de servicio (QoS) (variable dependiente).

Para el componente cuantitativo, se aplicaron técnicas de estadística descriptiva (frecuencias, porcentajes, promedios y desviaciones estándar), lo que permitió sintetizar la información obtenida en las encuestas y presentarla en gráficos fáciles de interpretar.

En el componente cualitativo, se utilizó el método de análisis de contenido temático, que permitió categorizar y comprender las respuestas obtenidas en la entrevista al responsable del área de redes, aportando una visión técnica que complementa la percepción de los usuarios.

De esta forma, el análisis estadístico de este estudio integra ambas perspectivas, permitiendo un entendimiento más completo de la situación actual de la red institucional y facilitando la formulación de recomendaciones objetivas y fundamentadas.

3.5.1. Fórmula para el cálculo del tamaño de la muestra

Para determinar cuántas encuestas debían aplicarse a la comunidad universitaria, se utilizó la fórmula para el cálculo de muestra en poblaciones finitas.

Esta fórmula permite obtener un número estadísticamente representativo, garantizando que los resultados reflejen de manera confiable la percepción de la población total.

Fórmula general:

$$n = \frac{N \cdot Z^2 \cdot p \cdot q}{E^2(N-1) + Z^2 \cdot p \cdot q}$$

Donde:

- n: tamaño de la muestra
- N: población total (5.197 usuarios en la UPEC)
- Z: nivel de confianza (2.5758 → 99%)
- p: probabilidad de éxito (0.5)
- q: probabilidad de fracaso (0.5)
- E: margen de error permitido (0.05 → 5%)

Sustituyendo los valores utilizados:

$$n = \frac{5197 \cdot (2.5758)^2 \cdot 0.5 \cdot 0.5}{0.05^2(5197-1) + (2.5758)^2 \cdot 0.5 \cdot 0.5}$$

$$n = \frac{8619.6875}{14.64875} = 588.5 \approx 591$$

Posteriormente, la muestra se distribuyó proporcionalmente entre:

- Estudiantes 546 - 92.39%
- Docentes 33 - 5.58%
- Personal administrativo 12 - 2.03%

Esta distribución garantiza representatividad según el peso de cada grupo dentro de la población total.

3.5.2. Análisis cuantitativo: Resultados de las encuestas

A continuación, se presentan los apartados listos para completar con los resultados obtenidos de las encuestas.

1. **Marcar su rol en la institución**

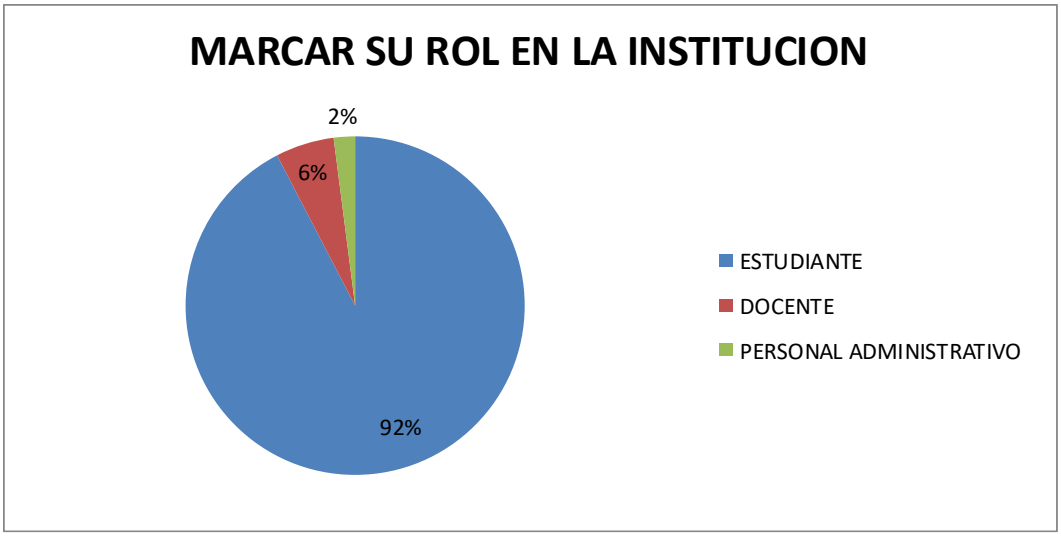


Figura 1. Marcar su rol en la institución

Análisis:

La mayoría de encuestados son estudiantes (92%), seguido de docentes (6%) y personal administrativo (2%), lo que demuestra que la muestra es representativa de la comunidad universitaria.

2. **Edificio en el cual se encuentra frecuentemente: (Puede marcar varias opciones)**

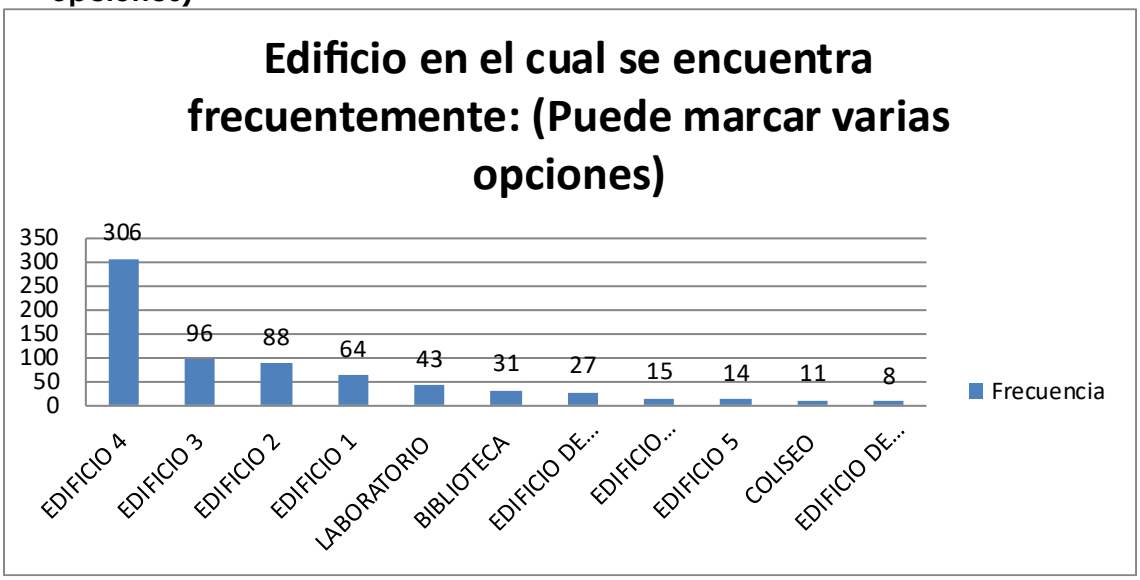


Figura 2. Edificios en los que los usuarios se encuentran con mayor frecuencia.

Análisis:

Este comportamiento evidencia que el Edificio 4 es el punto de mayor demanda de conectividad, lo que implica mayor consumo de ancho de banda y probabilidad de saturación en este sector del campus.

3. **Modalidad de estudio**

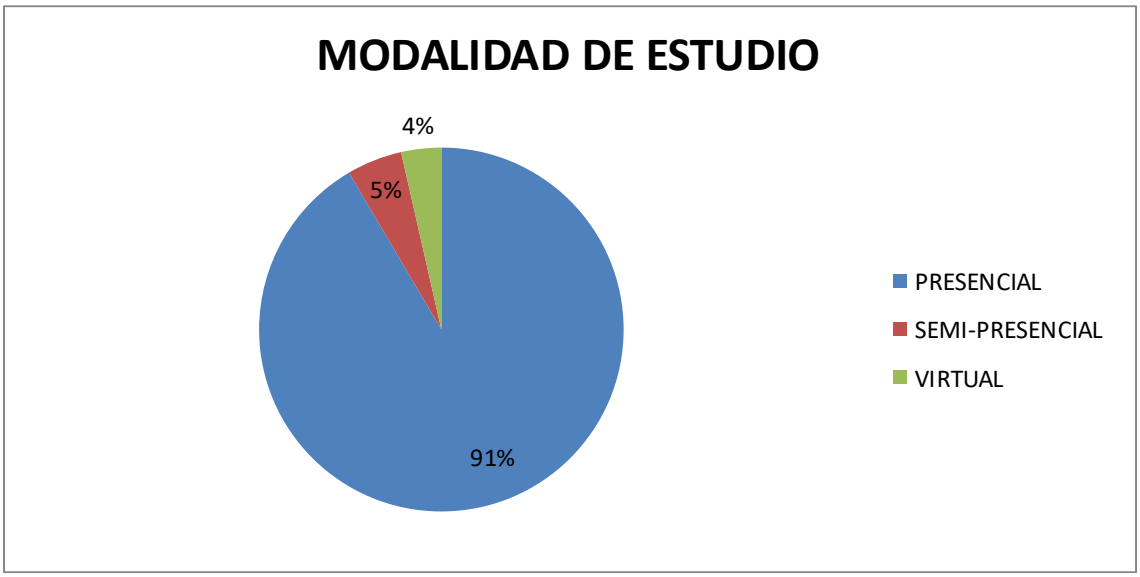


Figura 3. Modalidad de estudio.

Análisis:

Esto confirma que la mayoría de los usuarios que emplean la red universitaria lo hacen desde clases presenciales, lo cual influye directamente en la demanda diaria del tráfico institucional.

4. ¿Con qué frecuencia utiliza los siguientes servicios digitales de la universidad?

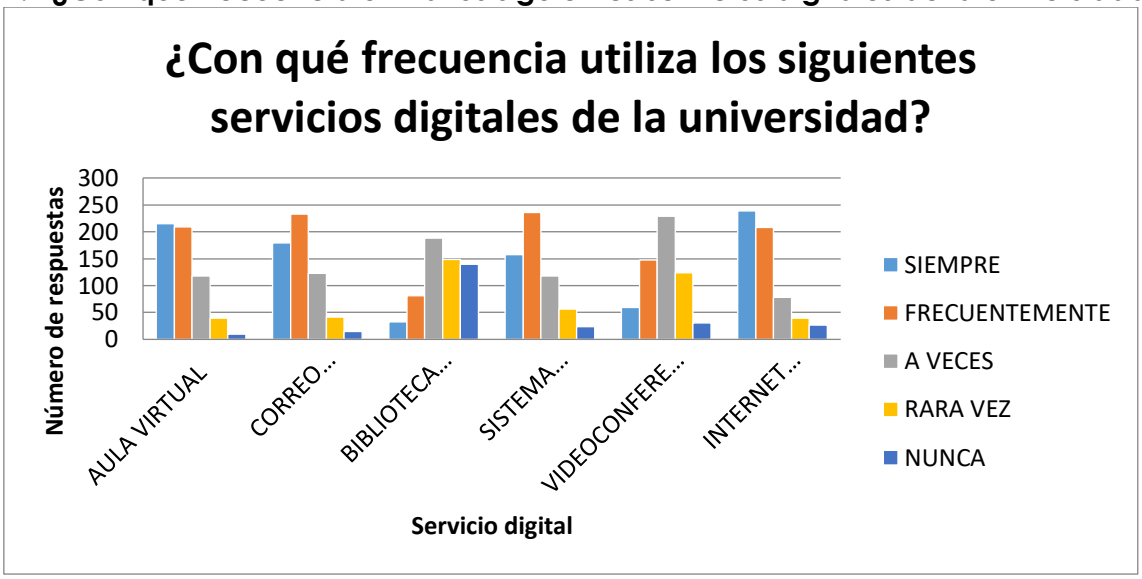


Figura 4. Frecuencia de uso de servicios digitales institucionales.

Análisis:

En conjunto, los resultados evidencian que los servicios esenciales para el desarrollo académico son los que registran mayor demanda, lo cual implica una fuerte carga sobre la infraestructura de red. Estos patrones de uso explican la saturación observada en horas pico y permiten identificar qué plataformas requieren mayor prioridad en políticas de optimización y QoS.

5. ¿Cómo califica la velocidad del internet en la universidad?

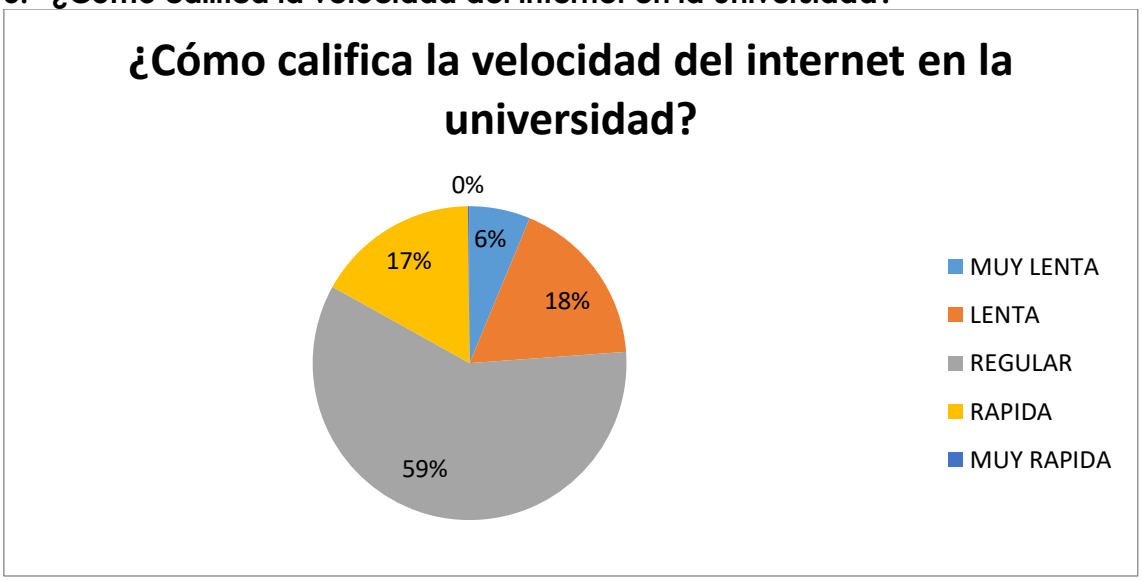


Figura 5. Percepción de la velocidad del internet en la universidad.

Análisis:

En conjunto, los resultados muestran que la mayoría de los usuarios percibe un servicio aceptable pero insuficiente, lo que sugiere la necesidad de optimizar el rendimiento de la red institucional.

6. ¿Cómo califica la estabilidad de la conexión (que no se corte)?

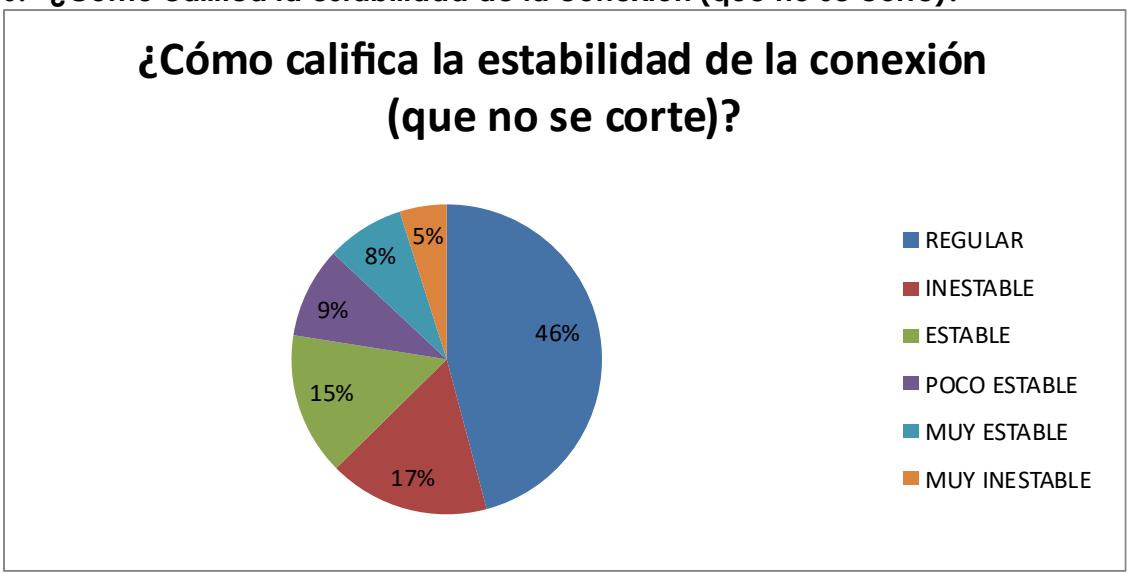


Figura 6. Percepción de la estabilidad de la conexión en la universidad.

Análisis:

Estos resultados muestran que, aunque la mayoría no experimenta cortes graves, la estabilidad del servicio aún presenta fallos que afectan la experiencia de los usuarios, reflejando la necesidad de mejorar la continuidad de la conexión.

7. ¿Con qué frecuencia experimenta problemas de conectividad?

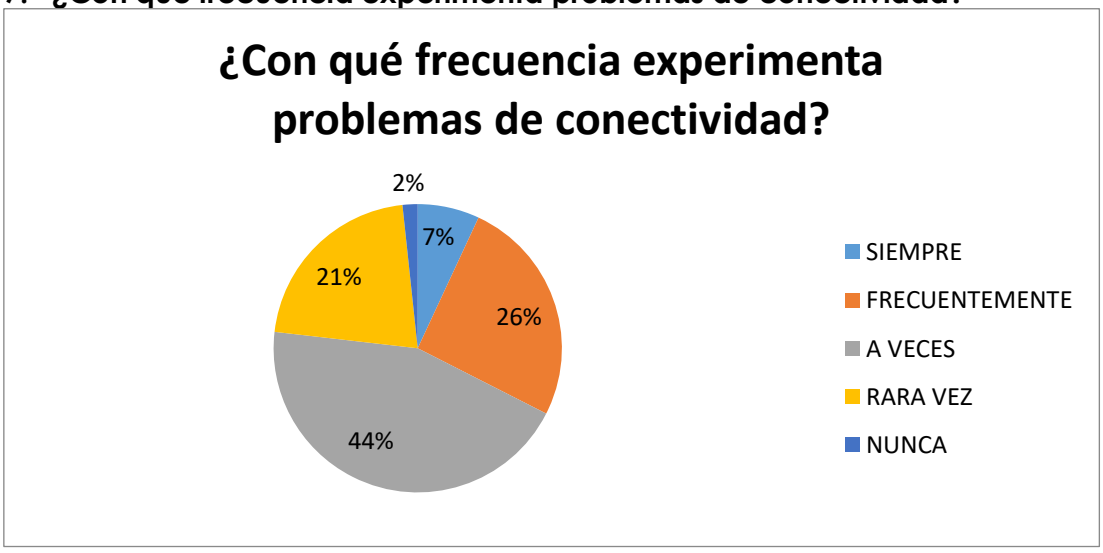


Figura 7. Frecuencia con la que los usuarios experimentan problemas de conectividad.

Análisis:

Estos resultados evidencian que la mayoría de usuarios enfrenta interrupciones ocasionales o recurrentes, reflejando una conectividad inestable que afecta el uso normal de los servicios digitales institucionales.

8. **¿En qué horarios experimenta mayor lentitud en el internet? (Puede marcar varias opciones)**

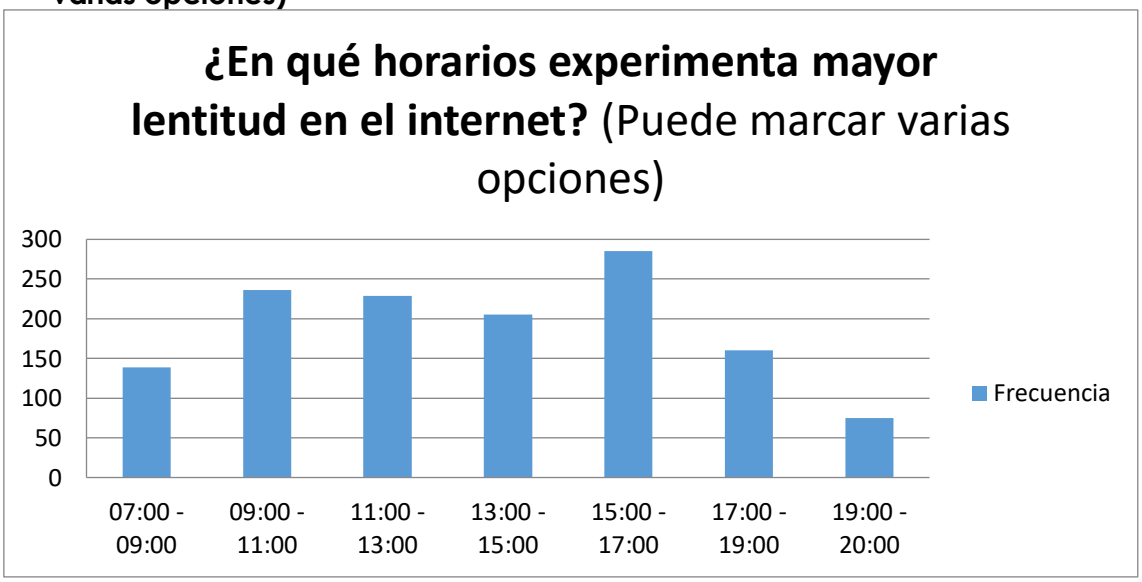


Figura 8. Horarios en los que los usuarios experimentan mayor uso o problemas de conectividad.

Análisis:

Los horarios con menos menciones son 07:00–09:00 y 19:00–20:00, lo que indica menor saturación en estas franjas. En conjunto, la información confirma que la red tiende a saturarse durante los periodos de mayor actividad académica, especialmente en la mañana y noche, lo que coincide con los picos identificados en la entrevista al área TIC.

9. **¿En qué lugares del campus experimenta mayor lentitud? (Puede marcar varias opciones)**

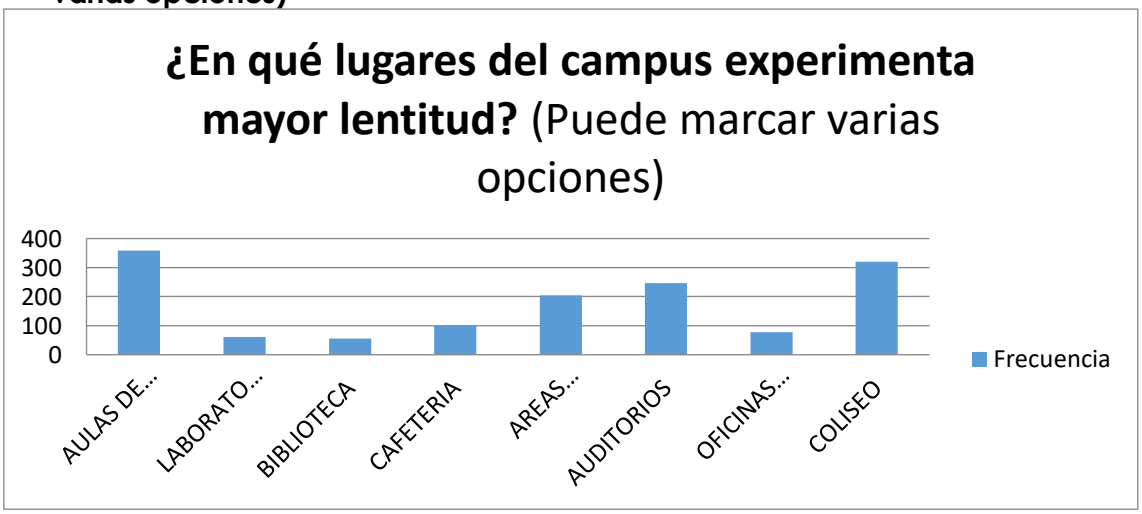


Figura 9. Lugares del campus donde los usuarios experimentan mayor lentitud de conexión.

Análisis:

Los resultados muestran que los lugares donde se experimenta mayor lentitud en la conexión son principalmente las aulas de clase y el coliseo, con las frecuencias más elevadas. En segundo lugar aparecen los auditorios y las áreas comunes, mientras que espacios como los laboratorios, biblioteca, cafetería y oficinas presentan valores más bajos.

Estos datos sugieren que la congestión de la red está directamente relacionada con la concentración de usuarios, siendo los espacios de mayor afluencia estudiantil los que presentan más problemas de velocidad.

10. **¿Cuáles de los siguientes problemas ha experimentado? (Puede marcar varias opciones)**

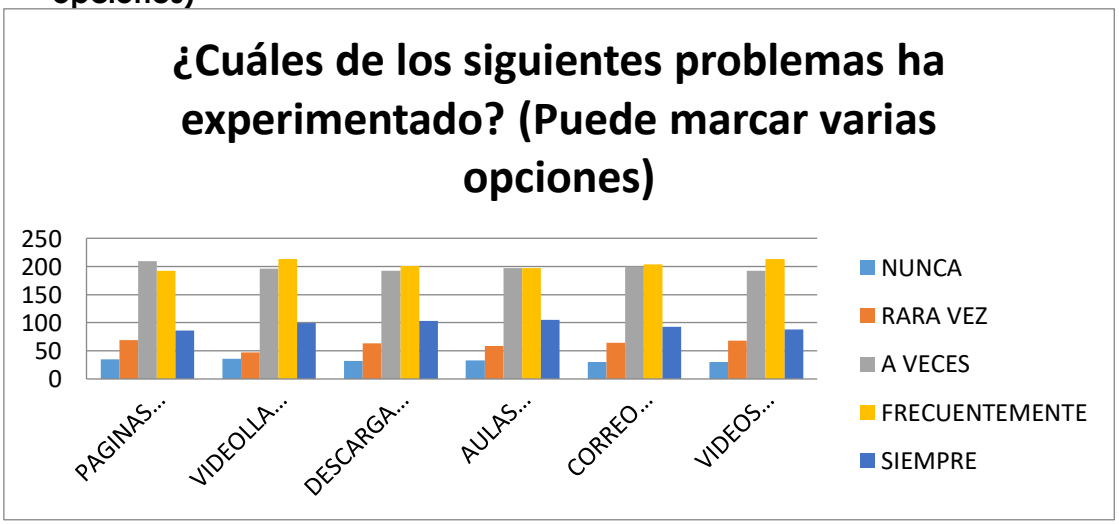


Figura 10. Problemas de conectividad experimentados por los usuarios.

Análisis:

Las videollamadas y las descargas presentan también incidencias relevantes, mostrando que los usuarios enfrentan dificultades en actividades que requieren estabilidad y buen ancho de banda.

En conjunto, los datos reflejan que los problemas de conectividad no son aislados ni esporádicos, sino que afectan a múltiples servicios digitales, lo que confirma la presencia de congestión y limitaciones en el rendimiento de la red institucional.

11. ¿Cómo afectan los problemas de conectividad en su ocupación?

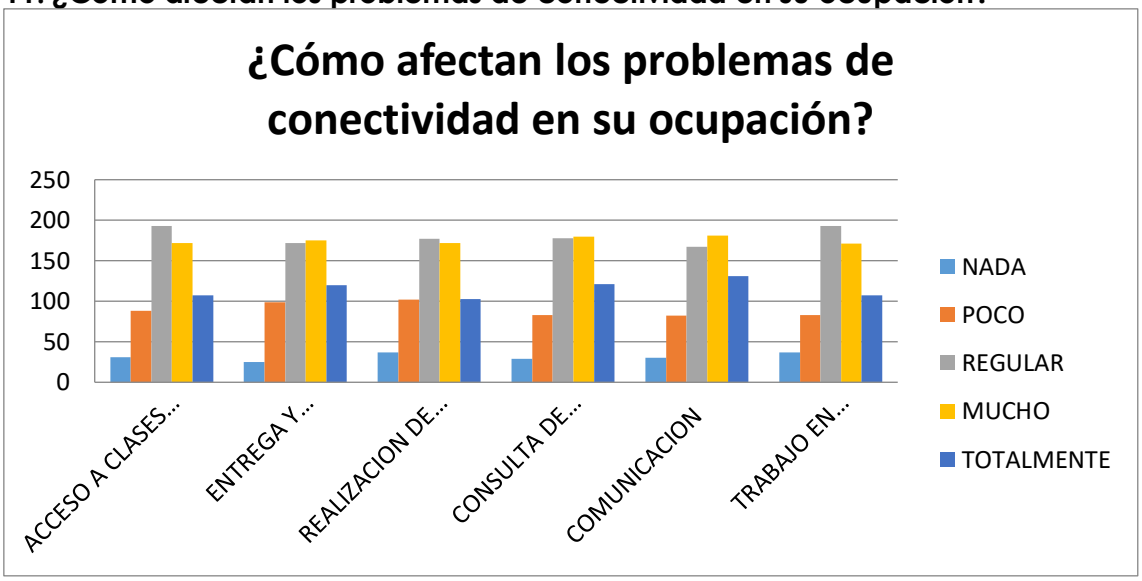


Figura 11. Impacto de los problemas de conectividad en las actividades de los usuarios.

Análisis:

Estos resultados demuestran que la calidad del servicio de red no solo influye en la experiencia de navegación, sino que impacta directamente en el cumplimiento de las responsabilidades académicas y laborales dentro de la institución.

12. **¿Ha tenido que usar internet externo (datos móviles) por problemas con el internet universitario?**

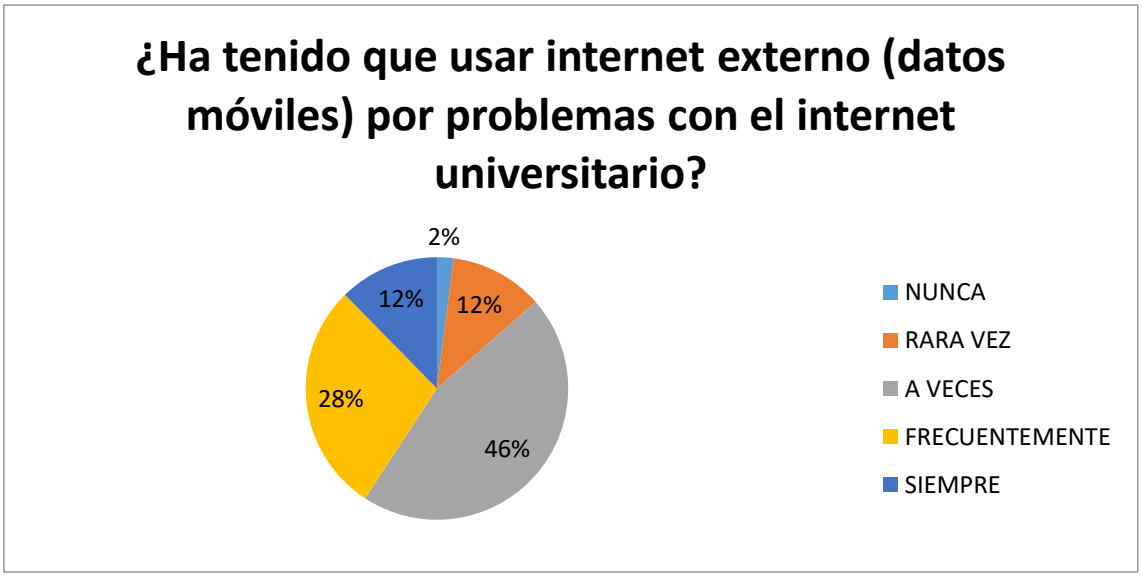


Figura 12. Uso de internet externo por fallas del internet universitario.

Análisis:

Estos resultados muestran que la mayoría de usuarios se ve obligada a depender de sus propios datos móviles para continuar con sus actividades académicas o laborales, lo que evidencia deficiencias importantes en la calidad y disponibilidad del servicio de red institucional

13. **¿Cuál es su nivel de satisfacción general con el servicio de internet de la universidad?**

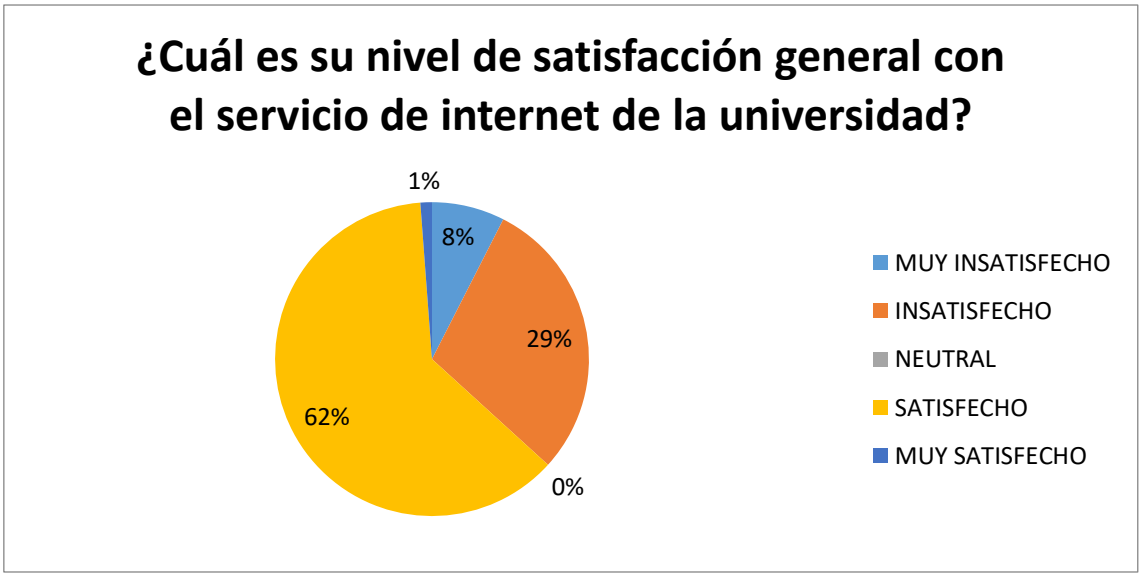


Figura 13. Nivel de satisfacción general con el servicio de internet universitario.

Análisis:

Los datos reflejan que, aunque una mayoría percibe el servicio como aceptable, existe un porcentaje importante de usuarios que experimenta problemas que afectan su satisfacción, lo que evidencia áreas claras de mejora dentro de la infraestructura de red institucional.

14. ¿Recomendaría mejoras en el servicio de internet universitario?

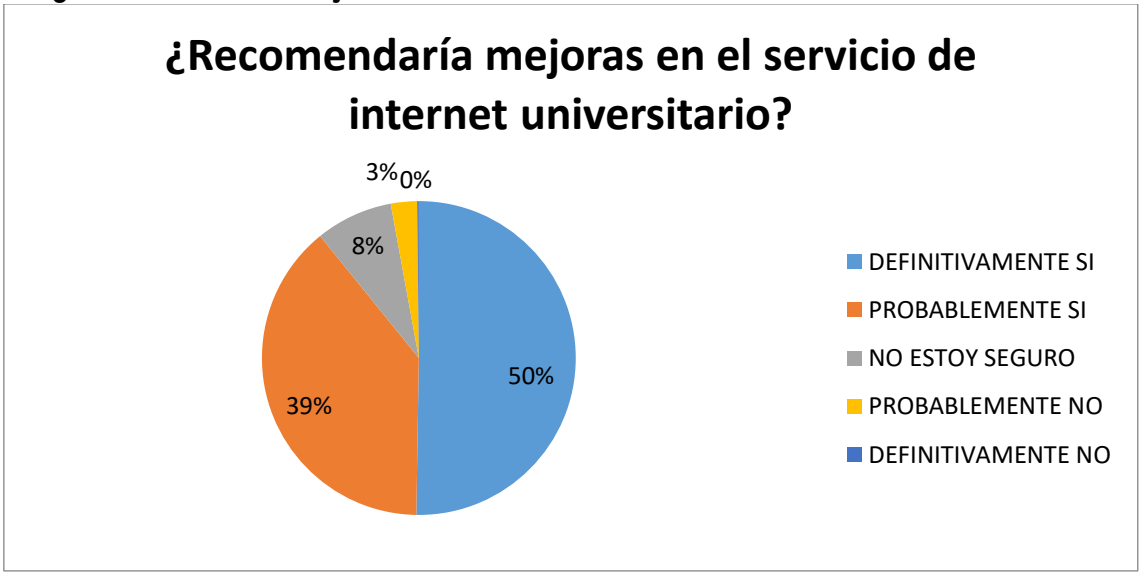


Figura 14. Recomendación de mejoras en el servicio de internet universitario.

Análisis:

Estos resultados reflejan un consenso claro: la gran mayoría de usuarios considera necesario implementar mejoras en la calidad del servicio de internet institucional, lo cual coincide con las percepciones de lentitud e inestabilidad identificadas en preguntas anteriores.

15. ¿Qué mejoras específicas sugiere para el internet universitario? (Pregunta abierta)

Los resultados de la pregunta abierta reflejan que los usuarios de la institución consideran que las mejoras más necesarias para la red universitaria se centran en dos aspectos principales: la velocidad del servicio y la cobertura en los diferentes espacios del campus.

La categoría más mencionada corresponde al incremento de la velocidad o ampliación del ancho de banda (29.1%), lo que evidencia que la capacidad actual del servicio resulta insuficiente para atender la alta demanda de usuarios conectados simultáneamente. Muy cerca, con un 27.4%, aparece la necesidad de extender la

cobertura del internet institucional hacia áreas donde la señal es débil o inexistente, tales como pasillos, canchas, el coliseo y algunos edificios específicos.

Un grupo menor de respuestas (2.2%) señala problemas relacionados con la estabilidad del servicio, refiriéndose a desconexiones, saturación o caídas eventuales. Por otra parte, un 7.8% enfatiza la importancia de actualizar la infraestructura, especialmente routers, puntos de acceso y equipos de red que permitan soportar la demanda creciente.

Algunos usuarios (3.2%) sugieren incrementar la densidad de puntos de acceso, mientras que propuestas vinculadas con la gestión del tráfico (0.2%) y el mantenimiento técnico (0.2%) representan una minoría dentro del conjunto de observaciones.

Finalmente, un 29.8% de las respuestas no aportó sugerencias claras o correspondió a comentarios no aplicables ("Nd", "No sé", etc.).En conjunto, esta información indica que los esfuerzos de mejora deben dirigirse principalmente hacia:

Aumentar la capacidad del servicio (ancho de banda),

Ampliar la cobertura en el campus,

Actualizar infraestructura para reducir saturación.

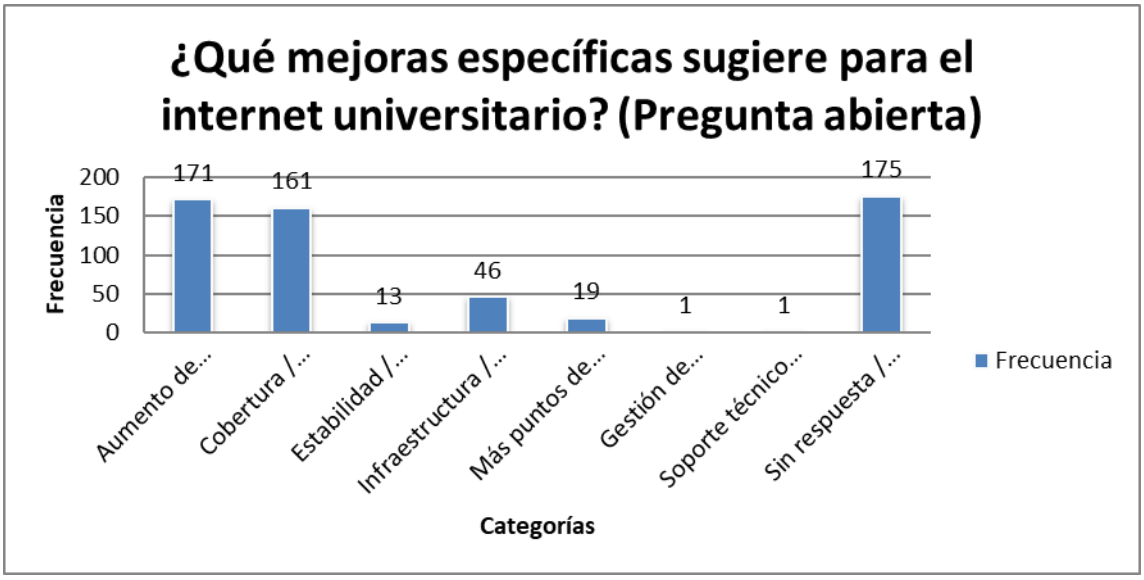


Figura 15. Mejoras específicas sugeridas para el servicio de internet universitario.

3.5.3. Análisis cualitativo: Entrevista al Magíster Javier Torres

A continuación, se presenta un análisis temático de la entrevista realizada al Mag. Javier Torres. Cada pregunta incluye la respuesta brindada y una interpretación que explica su relevancia para el estudio.

Gestión y monitoreo del tráfico de red

1. **¿Podría proporcionar una explicación sobre la red institucional es actualmente segura frente a amenazas externas y cuenta con implementación de firewalls perimetrales, sistemas de detección de intrusiones y segmentación de red adecuada?**

   La red de datos de la UPEC se encuentra segmentada por VLANs, para cada una de las diferentes dependencias: Autoridades, Financiero, Administrativo, Comunicaciones, TIC, Laboratorios WiFi, entre otras. La UPEC además cuenta con un sistema de seguridad perimetral con equipos NGFW tanto propios de la institución como de CEDIA quien es nuestro proveedor de servicios de red avanzada. Esto nos permite mitigar las amenazas externas hacia nuestra red institucional

   La institución cuenta con una base sólida de seguridad gracias a la segmentación en VLANs y al uso de firewalls perimetrales NGFW. Sin embargo, esta seguridad perimetral no garantiza por sí sola un adecuado control del tráfico interno si no se complementa con monitoreo avanzado.

   Análisis:

   La institución cuenta con una base sólida de seguridad gracias a la segmentación en VLANs y al uso de firewalls perimetrales NGFW. Sin embargo, esta seguridad perimetral no garantiza por sí sola un adecuado control del tráfico interno si no se complementa con monitoreo avanzado.

2. **¿Qué tipo de topología se está utilizando en la red institucional?**

   La red de datos que se encuentra implementada es en topología estrella, en donde su nodo central se encuentra en el Switch de Core del Data Center Institucional.

   Análisis:

   El uso de una topología estrella facilita la administración centralizada de la red, pero también concentra la carga en el switch de core, lo cual puede generar puntos de saturación cuando el tráfico aumenta.

3. **¿Cuál es el número de usuarios que forman parte de la red?**

   El número de usuarios llega aproximadamente 5000 usuarios, entre estudiantes, docentes, trabajadores y administrativos. Tomando en cuenta que los mismos en ocasiones usan más de un dispositivo.

   Análisis:

   El elevado número de usuarios y dispositivos conectados simultáneamente incrementa significativamente la demanda sobre la red, lo que explica parte de los problemas de congestión identificados en horas pico.

4. **¿Podría detallar si cuentan actualmente con herramientas de monitoreo de red en tiempo real, si la respuesta es afirmativa puede detallar las herramientas de monitoreo usadas?**

   En este momento como parte de la red de datos de la institución no se cuenta con monitoreo de red en tiempo real para analizar el tráfico de la red.

   Análisis:

   La ausencia de herramientas de monitoreo de tráfico en tiempo real es una debilidad importante, ya que dificulta la detección de cuellos de botella, anomalías y consumos excesivos por parte de aplicaciones no esenciales.

5. **¿Qué herramientas de Sistema de monitoreo de red y protocolos de gestión tienen implementados para el análisis del tráfico de red?**

   Al momento solo disponemos de un monitoreo de uso del Ancho de Banda de la red Avanzada con CEDIA, el mismo que esta implementando en ZABBIX

   Análisis:

   El uso exclusivo del monitoreo del ancho de banda proporcionado por CEDIA mediante Zabbix representa un alcance muy limitado para el análisis integral de la red.

6. **¿Cuál es la periodicidad establecida para realizar análisis de punto de partida del tráfico y evaluaciones de performance en la comunicación de red institucional?**

   No se han establecido las periocidades debido a la ausencia de la herramienta de monitoreo.

   Análisis:

   La falta de una herramienta robusta de monitoreo ha impedido establecer una periodicidad formal para evaluar el rendimiento de la red, lo cual limita la capacidad institucional de anticipar problemas.

7. **¿Han identificado patrones de congestión o picos de utilización del ancho de banda durante intervalos específicos del día? ¿Cuáles son los umbrales críticos de saturación detectados?**

   Si se han detectado horas pico en el uso del Ancho de Banda de la red de datos, la misma que ocurre entre las 08:00 hasta las 09:00 y entre las 14:00 y 15:00

   Análisis:

   Los horarios señalados coinciden con las actividades académicas más intensas, lo que confirma que la red experimenta saturación debido a la alta concurrencia de usuarios en esos periodos.

8. **¿Qué aplicaciones consumen mayor ancho de banda según sus registros?**

   El acceso a internet esta abierto, solo se ha bloqueado páginas prohibidas como: pornografía, criptominado, entre otras; y al tener las redes sociales abiertas estas son las que mas consumen el servicio de internet.

   Análisis:

   El uso libre de redes sociales contribuye al consumo excesivo de ancho de banda, afectando la disponibilidad del servicio para actividades prioritarias como clases virtuales, plataformas institucionales o videoconferencias

Calidad de Servicio (QoS) y seguridad

1. **¿Cuáles políticas de calidad de servicio tienen implementadas mediante clasificación de tráfico por DSCP o configuración de CoS en los switches y routers de la infraestructura actual?**

   Dentro de los equipos activos de red de la institución, se manejan solamente switches capa 3, en los cuales no se han implementado políticas QoS en los mismos.

   Análisis:

   Aunque la infraestructura cuenta con switches capa 3, la ausencia de políticas QoS impide priorizar tráfico crítico, lo cual afecta directamente el desempeño de servicios académicos y administrativos.

2. **¿Qué mecanismos de QoS han desplegado: modelado de tráfico vigilancia del tráfico, colas prioritarias, colas justas ponderadas o implementación de asignación de ancho de banda por clase de servicio?**

   No se han desplegado ningún mecanismo de QoS

Análisis:

La inexistencia de mecanismos QoS evidencia una falta de gestión del tráfico institucional, lo que provoca que todas las aplicaciones compitan por el ancho de banda sin criterios de prioridad.

3. **¿Cada que tiempo se realizan pruebas periódicas de vulnerabilidad, auditorías de seguridad de red y evaluaciones de penetration testing en la infraestructura de red institucional?**

   Se realizan auditorias anuales a toda nuestra infraestructura perimetral de red, donde se muestra las vulnerabilidades que cada servicio dispone. Así mismo contamos con un reporte mensual de los mismos.

   Análisis:

   Si bien se realizan auditorías de seguridad, estas evaluaciones se enfocan en vulnerabilidades y no en el rendimiento del tráfico. Por lo tanto, no reemplazan la necesidad de monitoreo continuo de desempeño.

4. **¿Podría detallar si han implementado diferenciación de servicios para aplicaciones críticas como sistemas académicos, videoconferencias y servicios de voz sobre IP mediante políticas de marcado y clasificación de tráfico?**

   No se ha realizado la clasificación de tráfico en ningún punto de la red de datos.

   Análisis:

   No existe priorización para aplicaciones críticas como plataformas académicas o videollamadas, lo cual contribuye a la inestabilidad y la percepción negativa del servicio por parte de los usuarios.

5. **¿Podría especificar si cuentan con implementación de control de admisión y la asignación de ancho de banda para limitar el impacto de aplicaciones no críticas durante períodos de alta congestión de red?**

   Debido al Ancho de Banda asignado para todo el campus universitario no se ha realizado la segmentación de ancho de banda para aplicaciones o sub redes.

   Análisis:

   La falta de segmentación del ancho de banda provoca que servicios esenciales compitan con aplicaciones recreativas, afectando el rendimiento general en horas de alta demanda.

6. **¿Qué herramientas de análisis y reporte emplean para medir la efectividad de las políticas QoS implementadas y generar informes de cumplimiento de los niveles de servicios de red y aplicaciones que hacen uso de la infraestructura?**
   No se dispone de herramientas para análisis de QoS
   Análisis:

   La ausencia total de herramientas para medir la efectividad de políticas QoS limita la capacidad de evaluar, mejorar y garantizar la calidad del servicio institucional.

Proyección y mejora

1. **¿Cuáles identifica como los principales cuellos de botella en la infraestructura de red actual de la UPEC en términos de sobresuscripción de enlaces troncales, latencia en switches de distribución y pérdida de paquetes en puntos de agregación?**
   El cuello de botella principal es el Switch de Core, debido a que se encuentra con enlaces principales de hasta 1Gbps mientras que los CPE del proveedor ya disponen de enlaces de 10Gbps.
   Análisis:
   El mayor cuello de botella identificado se encuentra en la infraestructura interna (switch de core), cuya capacidad no se ajusta a los niveles ofrecidos por el proveedor, generando un desfase entre oferta y capacidad real.
2. **¿Qué mejoras de optimización considera prioritarias para implementar políticas QoS basadas en la calificación de DSCP, segmentación VLAN por departamentos y configuración de modelado del tráfico en la red institucional?**
   Dentro de la red convergente institucional, se tiene tráfico de datos, voz y video. Lo cual es prioritario brindar políticas QoS al tráfico de voz y video y ciertas dependencias (Departamento Financiero) el tráfico de datos.
   Análisis:
   Las prioridades señaladas coinciden con necesidades reales: voz, video y datos financieros requieren QoS urgente para garantizar continuidad operativa y reducir la congestión en picos.
3. **¿Considera técnicamente viable implementar un sistema de monitoreo en tiempo real que incluya colección de datos vía SNMP v3, análisis de flujos NetFlow y dashboard centralizado con métricas de performance?**

Es viable ya que permitirá visualizar nuestra red de datos de mejor manera y en caso de tener cuellos de botella o algún error tomar los correctivos necesarios y de manera inmediata.

Análisis:

Existe viabilidad técnica para implementar monitoreo avanzado, lo cual permitiría visibilizar el comportamiento del tráfico y tomar decisiones oportunas para mejorar el rendimiento de la red.

4. **¿Cuántos técnicos del equipo actual de telecomunicaciones poseen conocimiento especializado y certificado en configuración avanzada de equipos de red?**

   En este momento solamente mi persona como Analista de Redes de Datos y Telecomunicaciones.

   Análisis:

   La dependencia de un solo técnico especializado representa un riesgo importante en términos de soporte, mantenimiento y gestión eficiente de la red universitaria

5. **¿Cree necesario implementar un sistema de medición que evalúe métricas de QoS del usuario final contra estándares de la industria educativa?**

   Si es necesario la implementación de un sistema que analice las métricas de QoS lo que nos permitirá garantizar que se optimice los recursos de la red de datos en las diferentes VLANS.

   Análisis:

   Existe conciencia institucional sobre la importancia de medir parámetros de QoS, lo que abre la puerta a implementar sistemas de evaluación que permitan mejorar el servicio según estándares educativos

6. **¿Desea proporcionar comentarios técnicos adicionales sobre el estado actual del cableado estructurado, necesidades de actualización de equipos y recomendaciones para la institución?**

   El cableado estructurado aun cuenta con años de vida útil ya que esta implementado con cable FUTP cat6a, así también los equipos activos de red están en un proceso de actualización debido a que ya estaban con tiempo de vida útil obsoleta. Cabe indicar que todos los equipos de networking son de la marca Huawei, CCTV son de la marka Hikvision, la central telefónica es

bajo la plataforma ISSABEL y los teléfonos son Cisco y GrandStream y el firewall institucional es de la marca Fortinet.

Análisis:

La infraestructura física de cableado es adecuada, pero la actualización de equipos activos es necesaria para mejorar la capacidad, estabilidad y rendimiento del servicio de internet institucional.

IV. RESULTADOS Y DISCUSIÓN

4.1. RESULTADOS

Los resultados que se han conseguido a partir de las técnicas utilizadas en la investigación, la información se irá agrupando en secciones de acuerdo con las fuentes de datos trabajadas: Zabbix, encuestas y entrevista.

4.1.1 Resultados del monitoreo en Zabbix

En esta sección se exponen objetivamente los datos recogidos a partir de la herramienta elegida: Zabbix. Los resultados se muestran en análisis y figuras de los dos agentes de mayor importancia de la UPEC Switch Core y Switch DMZ, siguiendo lo requerido por la guía metodológica.

4.1.1.1 Dashboard Switch de core

4.1.1.1. 1 Interface Gi6/20 DMZ ASA

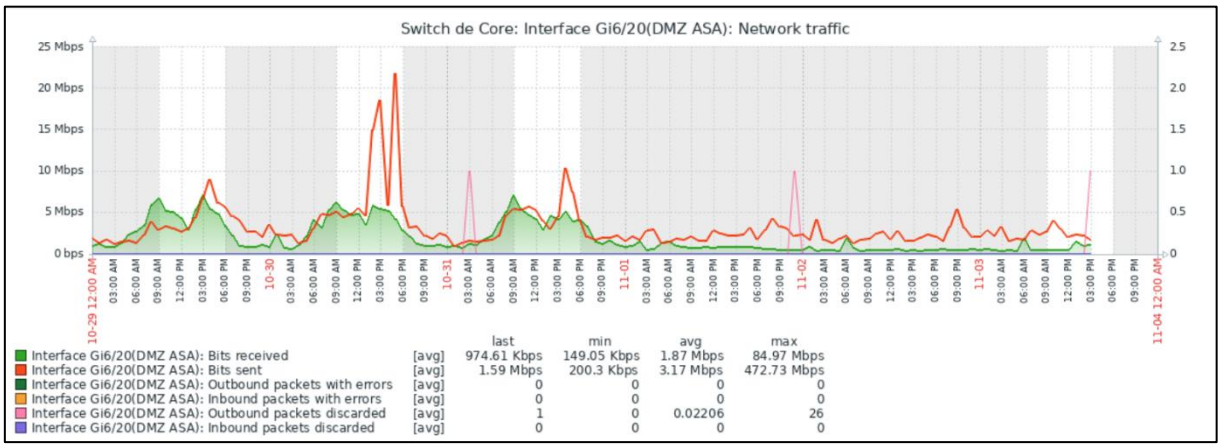


Figura 16. Interface Gi6/20 DMZ ASA

Este gráfico representa el comportamiento del tráfico de red en una interfaz Gigabit Ethernet (Gi6/20) del switch de core, específicamente en el segmento que conecta con la zona DMZ del firewall ASA. El período analizado corresponde a un ciclo completo de 24 horas.

Representación gráfica:

- La línea verde con relleno indica el tráfico entrante (bits recibidos por la interfaz)
- La línea roja representa el tráfico saliente (bits transmitidos desde la interfaz)

El eje vertical izquierdo muestra la velocidad de transferencia expresada en Mbps, con un rango de 0 a 25 Mbps para la ventana de tiempo visible.

Análisis del Comportamiento del Tráfico

Período de madrugada (00:30 - 06:00): El tráfico se mantiene en niveles mínimos, consistente con la baja actividad operacional durante horas no laborales.

Horario matutino (09:00 aproximadamente): Se observa el pico más significativo del período visible, alcanzando aproximadamente 20 Mbps en tráfico entrante y 10 Mbps en tráfico saliente. Este comportamiento es característico del inicio de jornada laboral, cuando se producen autenticaciones simultáneas de usuarios, sincronización de aplicaciones y posiblemente ejecución de procesos programados.

Jornada laboral (09:00 - 20:00): El tráfico se estabiliza en un rango de 2-5 Mbps, lo cual representa la carga operacional normal.

Período nocturno (20:00 en adelante): El tráfico decrece significativamente, manteniéndose en niveles basales consistentes con operaciones automatizadas mínimas.

Análisis Estadístico Detallado

Tráfico entrante (Bits received):

- Promedio: 974.81 Kbps (~0.97 Mbps)
- Valor mínimo: 149.05 Kbps
- Valor actual: 1.87 Mbps
- Valor máximo registrado: 84.97 Mbps

Tráfico saliente (Bits sent):

- Promedio: 1.59 Mbps
- Valor mínimo: 200.3 Kbps
- Valor actual: 3.17 Mbps
- Valor máximo registrado: 472.73 Mbps

Evaluación de Integridad de la Interfaz

Indicadores de salud:

Paquetes con errores:

- Salientes: 1 paquete
- Entrantes: 1 paquete
- Evaluación: Tasa de error prácticamente nula, dentro de parámetros normales

Paquetes descartados:

- Salientes: 0.02206 promedio, con 26 paquetes descartados en total
- Entrantes: 0 paquetes descartados
- Evaluación: Nivel de descarte insignificante, indicando ausencia de congestión

Observaciones Relevantes

Punto crítico de atención:

El valor máximo registrado de 472.73 Mbps en tráfico saliente merece análisis especial. Aunque este pico no es visible en la ventana temporal del gráfico, representa aproximadamente el 47% de la capacidad nominal de la interfaz Gigabit (1000 Mbps).

4.1.1.1.2 Interface Gi6/40 ENLACE-WLC-HUAWEI

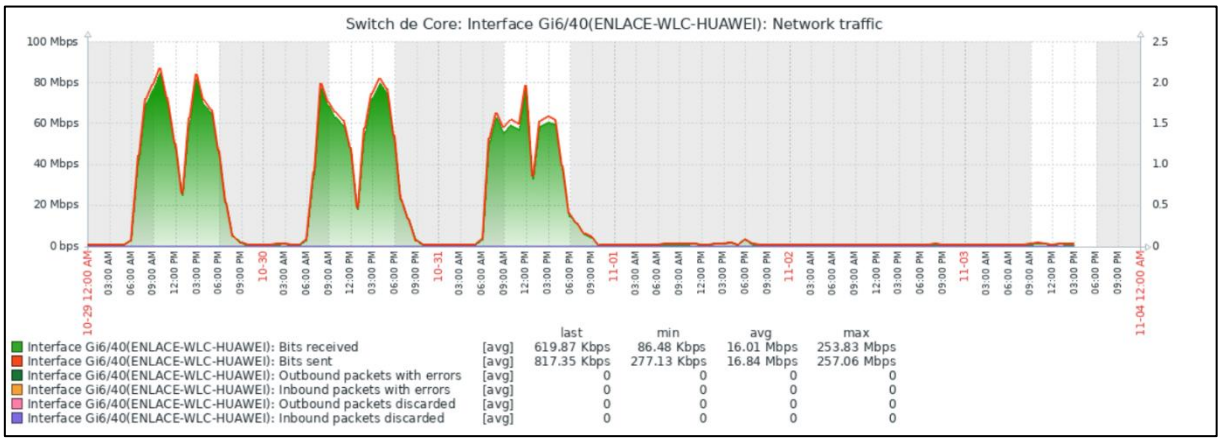


Figura 17. Interface Gi6/40 ENLACE-WLC-HUAWEI

Este gráfico muestra el tráfico de red en la interfaz Gi6/40 del switch de core, correspondiente al enlace WLC (Wireless LAN Controller) de Huawei. El análisis abarca

un período de 24 horas y refleja el comportamiento del tráfico inalámbrico de la organización.

Representación gráfica:

La línea verde con relleno representa el tráfico entrante (bits recibidos)

La línea roja indica el tráfico saliente (bits transmitidos)

El eje vertical izquierdo muestra velocidades de hasta 100 Mbps, evidenciando que esta interfaz maneja volúmenes considerablemente superiores a la interfaz DMZ.

Análisis del Comportamiento del Tráfico

Características distintivas del patrón:

Primer pico (aproximadamente 03:00 - 04:00):

Alcanza cerca de 90 Mbps en tráfico entrante

Tráfico saliente alcanza aproximadamente 80 Mbps

Duración: aproximadamente 1-2 horasPatrón: Aumento abrupto y descenso gradual

Segundo pico (aproximadamente 09:00 - 10:00):

Magnitud similar al primer pico (~80 Mbps entrante)

Coincide con horario de inicio de jornada laboral

Comportamiento esperado por conexión masiva de dispositivos móviles

Tercer pico (aproximadamente 13:00 - 15:00):

Tráfico entrante alcanza aproximadamente 60-70 Mbps

Duración más prolongada que los picos anteriores

Posiblemente relacionado con actividad de medio día y post almuerzo

Período de calma (16:00 en adelante): El tráfico se reduce drásticamente a niveles casi imperceptibles, manteniéndose prácticamente plano el resto del día.

Análisis Estadístico Detallado

Tráfico entrante (Bits received):

Promedio: 619.87 Kbps (~0.62 Mbps)

Valor mínimo: 86.13 Kbps

Valor actual: 16.01 Mbps

Valor máximo registrado: 253.88 Mbps

Tráfico saliente (Bits sent):

Promedio: 817.35 Kbps (~0.82 Mbps)

Valor mínimo: 277.13 Kbps

Valor actual: 16.84 Mbps

Valor máximo registrado: 257.68 Mbps

Evaluación de Integridad de la Interfaz

Paquetes con errores:

Salientes: 0 paquetes

Entrantes: 0 paquetes

Evaluación: Ausencia total de errores

Paquetes descartados:

Salientes: 0 paquetes

Entrantes: 0 paquetes

Evaluación: Sin pérdida de paquetes

Conclusión: La interfaz presenta métricas impecables, lo que indica una ausencia de problemas de capacidad o congestión.

Observaciones Relevantes

El pico registrado entre las 03:00-04:00 es atípico para tráfico de usuarios y requiere investigación

4.1.1.1.3 Interface Gi6/46 INSIDE ASA

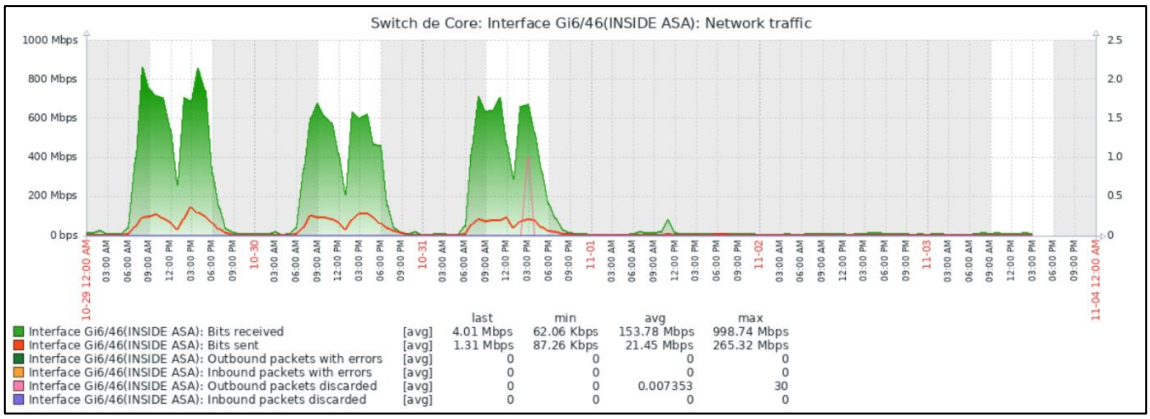


Figura 18. Interfaz Gi6/46 INSIDE ASA

Este gráfico representa el tráfico de red en la interfaz Gi6/46 del switch de core, correspondiente al enlace INSIDE ASA (interfaz interna del firewall). Esta es una interfaz crítica que conecta el firewall con la red corporativa interna, manejando todo el tráfico entre la red interna y las zonas protegidas.

Interpretación de las Métricas Visuales

Representación gráfica:

La línea verde con relleno representa el tráfico entrante (desde la red interna hacia el firewall)

La línea roja indica el tráfico saliente (desde el firewall hacia la red interna)

Escala crítica: El eje vertical alcanza 1000 Mbps (1 Gbps), la capacidad máxima de la interfaz Gigabit, lo que indica que esta interfaz maneja volúmenes sustancialmente mayores que todas las interfaces analizadas previamente.

Características distintivas del patrón:

Este gráfico presenta el comportamiento más intenso y robusto de todas las interfaces analizadas:

Tres períodos de alta actividad claramente definidos:

Primer período (00:30 - 03:30):

Tráfico entrante alcanza aproximadamente 850-900 Mbps

Representa el 85-90% de la capacidad total de la interfaz

Picos extremadamente pronunciados y sostenidos

Tráfico saliente (rojo) relativamente bajo (~100-200 Mbps)

Segundo período (08:00 - 11:00):

Tráfico entrante alcanza 600-700 Mbps

Coincide con horario de inicio de jornada laboral

Duración más extendida que el primer período

Comportamiento más variable con múltiples picos

Tercer período (14:00 - 16:00):

Tráfico entrante alcanza 700-750 Mbps

Menor intensidad que los períodos anteriores

Duración más corta

Posible actividad relacionada con horario vespertino

Período de calma (16:30 en adelante):

Tráfico se reduce drásticamente a niveles casi nulos

Línea prácticamente plana cerca de 0 Mbps

Ausencia total de la actividad intensa previa

Asimetría del tráfico extremadamente marcada:

La característica más notable de esta interfaz es la predominancia absoluta del tráfico entrante (verde): Indica flujo masivo de datos desde la red interna hacia el firewall

Análisis Estadístico Detallado

Tráfico entrante (Bits received):

Promedio: 4.01 Mbps (sorprendentemente bajo dado los picos)

Valor mínimo: 62.06 Kbps

Valor actual: 153.78 Mbps

Valor máximo registrado: 908.74 Mbps esto se determina como critico.

Tráfico saliente (Bits sent):

Promedio: 1.31 Mbps

Valor mínimo: 87.26 Kbps

Valor actual: 21.45 Mbps

Valor máximo registrado: 265.32 Mbps

Evaluación de Integridad de la Interfaz

Indicadores de salud:

Paquetes con errores:

Salientes: 0 paquetes

Entrantes: 5 paquetes

Evaluación: Nivel de errores prácticamente nulo considerando el volumen de tráfico

Paquetes descartados:

Salientes: 0.007353 promedio, con 30 paquetes descartados

Entrantes: 0 paquetes descartados

Evaluación: Descarte mínimo, sin indicios de congestión significativa

Observación crítica: A pesar de operar cerca del 90% de capacidad durante los picos, la interfaz mantiene tasas de error y descarte excepcionalmente bajas, lo que indica dimensionamientos adecuados.

4.1.1.2 Dashboard DMZ

4.1.1.2.1 Interfaz Gi0/1 ENLACE-CORE-DMZ

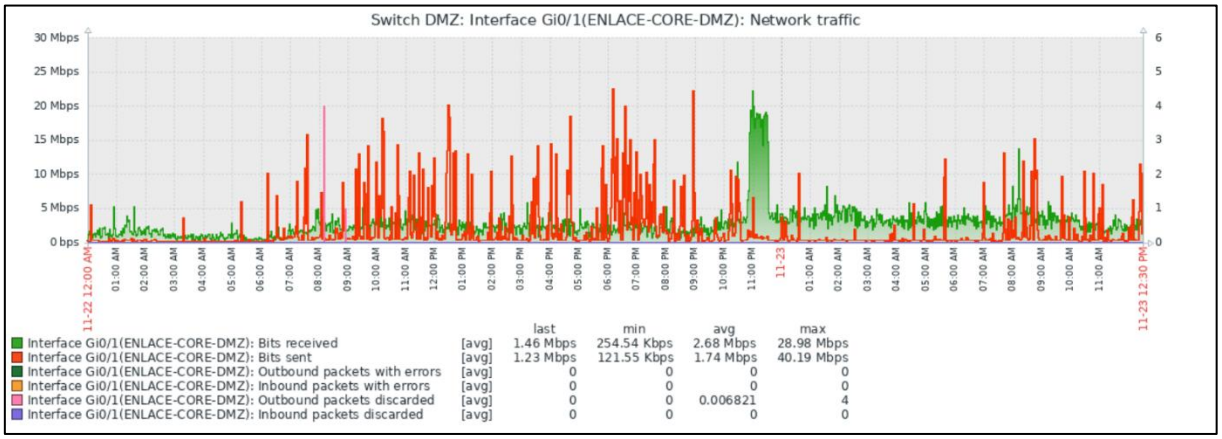


Figura 19. Interfaz Gi0/1 ENLACE-CORE-DMZ

Este gráfico corresponde al tráfico de red en la interfaz Gi0/1 del switch DMZ, específicamente el enlace CORE-DMZ. Esta interfaz representa un punto crítico de conectividad entre la zona desmilitarizada y el núcleo de la red corporativa.

Interpretación de las Métricas Visuales

Representación gráfica:

La línea verde con relleno representa el tráfico entrante (bits recibidos desde la DMZ hacia el core)

La línea roja indica el tráfico saliente (bits enviados desde el core hacia la DMZ)

El eje vertical izquierdo muestra velocidades de hasta 30 Mbps, con una escala más modesta que las interfaces anteriores.

Características distintivas del patrón:

Este gráfico presenta un comportamiento radicalmente diferente a los dos anteriores, mostrando un patrón de tráfico altamente irregular y esporádico.

Patrón de "ráfagas constantes":

A diferencia de las interfaces previas que mostraban picos bien definidos y períodos de calma, esta interfaz exhibe:

Múltiples picos cortos y frecuentes de tráfico rojo (saliente) durante todo el día

Picos que alcanzan consistentemente entre 10-22 Mbps

Ausencia de períodos prolongados de calma

Actividad prácticamente continua durante las 24 horas

Anomalía destacada (aproximadamente 11:15):

Se observa el único pico verde significativo de todo el período

Alcanza aproximadamente 22 Mbps de tráfico entrante

Contrasta notablemente con el patrón general donde predomina el tráfico saliente (rojo)

Duración breve pero intensidad considerable

Comportamiento del tráfico saliente (rojo):

Picos constantes y repetitivos durante todo el día

Mayor actividad entre 06:00 y 20:00 horas

Los picos individuales son breves pero frecuentes

Altura de picos: mayormente entre 10-20 Mbps

Comportamiento del tráfico entrante (verde):

Predominantemente bajo (línea base cerca de 0-2 Mbps)

Excepción notable en el pico de las 11:15

Sugiere que el flujo principal es desde el core hacia la DMZ

Análisis Estadístico Detallado

Tráfico entrante (Bits received):

Promedio: 1.46 Mbps

Valor mínimo: 254.54 Kbps

Valor actual: 2.68 Mbps

Valor máximo registrado: 28.98 Mbps

Tráfico saliente (Bits sent):

Promedio: 1.23 Mbps

Valor mínimo: 121.55 Kbps

Valor actual: 1.74 Mbps

Valor máximo registrado: 40.19 Mbps

Evaluación de Integridad de la Interfaz

Indicadores de salud:

Paquetes con errores:

Salientes: 0 paquetes

Entrantes: 0 paquetes

Evaluación: Ausencia total de errores en transmisión

Paquetes descartados:

Salientes: 0.006821 promedio, con 4 paquetes descartados en total

Entrantes: 0 paquetes descartados

Evaluación: Nivel de descarte virtualmente nulo, sin indicios de congestión

Conclusión de integridad: La interfaz mantiene métricas de calidad excepcionales a pesar del patrón de tráfico irregular.

4.1.1.2.2 interfaz Gi0/17

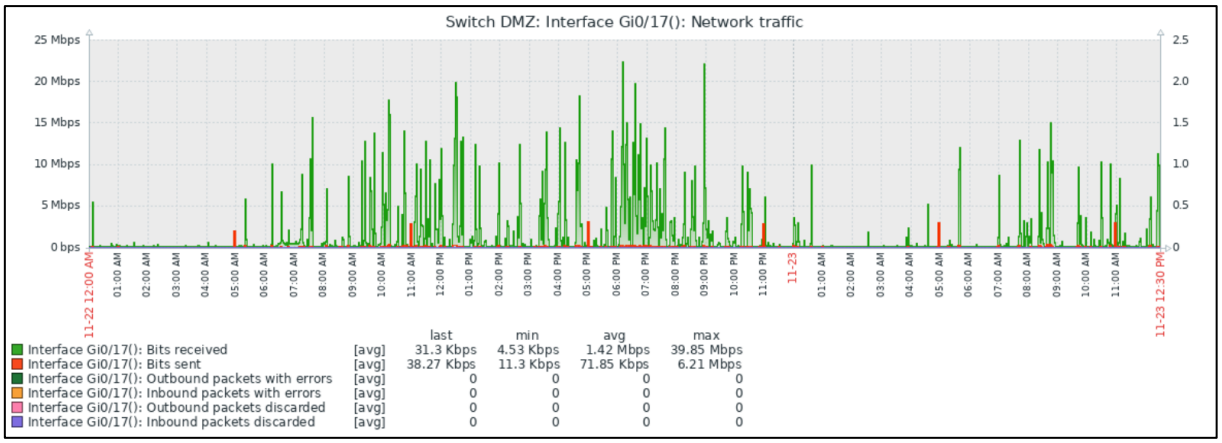


Figura 20. interfaz Gi0/17

Este gráfico corresponde al tráfico de red en la interfaz Gi0/17/1 del switch DMZ. Esta interfaz presenta un comportamiento particular que difiere significativamente de las interfaces analizadas previamente.

Interpretación de las Métricas Visuales

Representación gráfica:

- La línea verde representa el tráfico entrante (bits recibidos)
- La línea roja indica el tráfico saliente (bits transmitidos)

Escala: El eje vertical muestra velocidades de hasta 25 Mbps, una escala modesta que indica volúmenes relativamente bajos comparados con otras interfaces críticas.

Análisis del Comportamiento del Tráfico

Características distintivas del patrón:

Este gráfico presenta un comportamiento extremadamente asimétrico con características únicas:

Predominancia absoluta del tráfico entrante (verde):

- El tráfico verde domina completamente el gráfico
- La línea roja (saliente) es prácticamente invisible durante todo el período
- Picos de tráfico entrante alcanzan hasta 22-23 Mbps
- Tráfico saliente apenas visible, con esporádicos picos mínimos de ~2 Mbps

Patrón de actividad durante el día:

Período de madrugada (00:00 - 06:00):

- Tráfico muy bajo, línea prácticamente plana
- Actividad mínima o nula

Incremento gradual (06:00 - 08:00):

- Comienza a aparecer actividad
- Picos pequeños de 5-10 Mbps

Período de alta actividad (08:00 - 10:30):

- Mayor concentración de picos intensos
- Múltiples picos alcanzando 15-22 Mbps
- Frecuencia alta de ráfagas

Actividad sostenida (10:30 - 20:00):

- Picos regulares de 10-15 Mbps
- Actividad consistente pero variable
- Patrón de "sierra" con múltiples picos agudos

Declive nocturno (20:00 en adelante):

- Reducción progresiva de la actividad
- Retorno a niveles basales mínimos

Características del patrón de picos:

Picos tipo "aguja":

- Picos muy estrechos y pronunciados
- Subida y bajada extremadamente rápida
- Duración breve (minutos, no horas)
- Sugiere transferencias puntuales de datos

Frecuencia irregular:

- No hay periodicidad estrictamente definida
- Distribución variable durante el día
- Mayor concentración en horario laboral

Análisis Estadístico Detallado

Tráfico entrante (Bits received):

- Promedio: 31.3 Kbps (extremadamente bajo)
- Valor mínimo: 4.53 Kbps
- Valor actual: 1.42 Mbps
- Valor máximo registrado: 39.85 Mbps

Tráfico saliente (Bits sent):

- Promedio: 38.27 Kbps (también muy bajo)
- Valor mínimo: 11.3 Kbps
- Valor actual: 71.85 Kbps
- Valor máximo registrado: 6.21 Mbps

Relación crítica: El máximo entrante (39.85 Mbps) es 6.4 veces mayor que el máximo saliente (6.21 Mbps), confirmando la asimetría extrema.

Evaluación de Integridad de la Interfaz

Indicadores de salud perfectos:

Paquetes con errores:

- Salientes: 0 paquetes
- Entrantes: 0 paquetes
- Evaluación: Ausencia total de errores

Paquetes descartados:

- Salientes: 0 paquetes
- Entrantes: 0 paquetes
- Evaluación: Sin pérdida de paquetes

Conclusión de integridad: La interfaz presenta métricas impecables, indicando operación óptima sin problemas de capacidad o configuración.

4.1.1.2.3 interfaz V1 SWITCHING

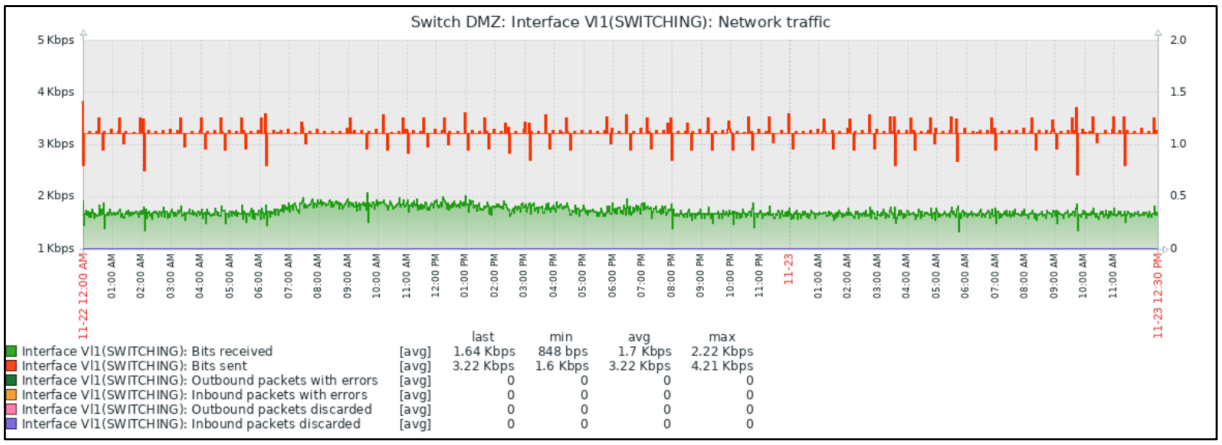


Figura 21. interfaz V1 SWITCHING

Este gráfico representa el tráfico de red en la interfaz Vl1 (SWITCHING) del switch DMZ. Esta es una interfaz lógica VLAN (no física), lo que indica tráfico de gestión del propio switch o comunicación inter-VLAN.

Interpretación de las Métricas Visuales

Representación gráfica:

- La línea verde con relleno representa el tráfico entrante (bits recibidos)
- La línea roja indica el tráfico saliente (bits transmitidos)

Escala crítica: El eje vertical muestra valores en Kbps (kilobits por segundo), con un máximo de apenas 5 Kbps. Esta es la escala más pequeña de todas las interfaces analizadas, indicando volúmenes extremadamente bajos.

Análisis del Comportamiento del Tráfico

Características distintivas del patrón:

Este gráfico presenta el comportamiento más estable y predecible de todas las interfaces analizadas:

Patrón de "línea plana con ruido mínimo":

Tráfico saliente (rojo):

- Línea prácticamente horizontal durante las 24 horas completas
- Valor constante alrededor de 3-3.5 Kbps
- Pequeñas oscilaciones mínimas (picos bajando a ~2.5 Kbps)
- Ausencia total de variaciones significativas

- No hay correlación con horarios laborales o actividad de usuarios

Tráfico entrante (verde):

- Línea igualmente estable alrededor de 1.5-1.8 Kbps
- Oscilaciones mínimas, aún menores que la línea roja
- Comportamiento prácticamente plano
- Sin picos o valles notables

Estabilidad temporal:

- Idéntico comportamiento 24/7 sin cambios día/noche
- No hay períodos de "alta" o "baja" actividad
- Completamente independiente de actividad de usuarios

Análisis Estadístico Detallado

Tráfico entrante (Bits received):

- Promedio: 1.64 Kbps
- Valor mínimo: 848 bps (~0.85 Kbps)
- Valor actual: 1.7 Kbps
- Valor máximo registrado: 2.22 Kbps

Tráfico saliente (Bits sent):

- Promedio: 3.22 Kbps
- Valor mínimo: 1.6 Kbps
- Valor actual: 3.22 Kbps
- Valor máximo registrado: 4.21 Kbps

Evaluación de Integridad de la Interfaz

Paquetes con errores:

- Salientes: 0 paquetes
- Entrantes: 0 paquetes
- Evaluación: Ausencia total de errores

Paquetes descartados:

- Salientes: 0 paquetes
- Entrantes: 0 paquetes
- Evaluación: Sin pérdida de paquetes

Conclusión de integridad: La interfaz presenta métricas impecables con operación perfecta.

4.1.1.3 Comparación Interfaz DMZ y Switch de CORE

4.1.1.3.1 Volumen de tráfico

El switch de core es donde se concentra la mayor parte del tráfico de toda la red de la institución. Sus interfaces llegan a manejar picos que fácilmente superan los 800–900 Mbps, sobre todo en enlaces internos importantes como INSIDE ASA o ENLACE-WLC. Esto tiene sentido porque por el core pasa prácticamente todo el flujo principal de la red: las conexiones a servicios internos, el tránsito entre VLANs, autenticaciones, la movilidad de los usuarios que se conectan por WiFi, los servidores y el acceso hacia la DMZ.

En cambio, las interfaces de la DMZ manejan mucho menos tráfico. La mayoría se mueven entre valores bastante modestos que rara vez pasan de los 20 a 40 Mbps, e incluso hay casos donde el tráfico es todavía más bajo, quedándose en rangos de 1 a 6 Mbps según lo que haga cada enlace. Solo en momentos muy específicos alguna interfaz sube un poco su actividad, pero aun así no se compara con las cargas que maneja el core.

4.1.1.3.2 Comportamiento y estabilidad

En el switch de core, el tráfico tiene patrones bastante claros: picos fuertes en ciertos horarios y bajadas marcadas entre cada periodo de actividad. Se ven bloques de tráfico alto que muestran los momentos donde la red está siendo muy usada, especialmente en horarios de trabajo y actividades académicas.

En la DMZ, el comportamiento es más irregular y fragmentado. Muchas interfaces tienen picos pequeños y frecuentes, pero no duran mucho. Esto tiene lógica con lo que hace la DMZ: ahí están los servicios externos, páginas web, autenticaciones hacia internet, aplicaciones que están expuestas y el tráfico que viene del firewall. Es normal que aparezcan variaciones cortas y repetitivas, pero sin cargas masivas.

Por ejemplo:

- El enlace Gi0/1 (CORE–DMZ) muestra picos dispersos que no se sostienen en el tiempo.
- Interfaces como la Gi0/17 trabajan con tráfico muy bajo, casi todo alrededor de 1–2 Mbps o menos.
- Las interfaces de switching interno en la DMZ (V1) tienen tráfico mínimo, casi siempre por debajo de 5 Kbps.

Esto confirma que la DMZ maneja tráfico ligero y orientado más hacia servicios externos, mientras que el core es el que sostiene el mayor peso de todo el funcionamiento de la institución.

4.1.1.3.3 Calidad del tráfico

En ambos lados se ve algo positivo: no hay errores ni paquetes descartados en la mayoría de las interfaces.

Esto dice que, aunque hay diferencias en la carga y en cómo varía el tráfico, tanto el core como la DMZ están operando de forma estable, sin pérdidas importantes de paquetes.

4.1.2 Políticas de QoS recomendadas

A partir del análisis realizado con Zabbix (donde se identificaron picos de tráfico, variaciones de latencia, episodios de congestión y momentos de saturación en las interfaces monitoreadas), se estableció un conjunto de políticas de Calidad de Servicio (QoS) que se ajustan de manera directa a las necesidades de la red institucional. Estas políticas permiten no solo optimizar el uso del ancho de banda, sino también garantizar que los servicios académicos y administrativos funcionen de manera estable y predecible.

En primer lugar, se recomienda implementar priorización del tráfico, ya que durante las horas de mayor demanda los servicios sensibles al retardo (como videoconferencias, plataformas educativas y telefonía IP) compiten con el tráfico general de navegación. Al darles prioridad, se asegura que continúen funcionando bien incluso cuando la red está experimentando altos niveles de uso.

Para complementar esto, es necesario aplicar clasificación y marcado del tráfico (DSCP). Esta política permite identificar qué tipo de paquetes circulan por la red y asignarles un valor según su importancia. Con esto, los servicios institucionales pueden

diferenciarse del tráfico recreativo y recibir un tratamiento adecuado en las siguientes etapas del proceso de QoS.

Otra política fundamental es la gestión de colas, especialmente durante situaciones de congestión. Los datos obtenidos muestran momentos donde la interfaz alcanza niveles de saturación que elevan la latencia y generan pérdida de paquetes. El uso de colas especializadas, como LLQ o CBWFQ, ayudaría a organizar el tráfico y garantizar que los servicios críticos mantengan un retardo mínimo incluso en horas pico.

Asimismo, los resultados evidencian que sería conveniente implementar mecanismos de control de congestión como WRED. Este tipo de políticas permite prevenir que las colas se llenen por completo, reduciendo el número de paquetes que se descartan y mejorando la fluidez del tráfico cuando la red está trabajando cerca de su capacidad máxima.

De igual forma, se recomienda considerar técnicas de shaping del ancho de banda, especialmente en los enlaces donde se observaron picos bruscos de uso. El shaping ayuda a suavizar el tráfico enviándolo de manera más uniforme, lo que disminuye los momentos de saturación sin necesidad de bloquear o descartar paquetes.

Finalmente, los resultados de Zabbix confirman lo importante que es mantener un monitoreo continuo como parte integral de cualquier política de QoS. La identificación de patrones de tráfico, tendencias de consumo y eventos de latencia solo es posible gracias al monitoreo permanente, lo que convierte a esta práctica en algo imprescindible para tomar buenas decisiones. Del mismo modo, se recomienda fortalecer las políticas de disponibilidad y redundancia, ya que una red con enlaces alternos y mecanismos de failover ofrece mayor estabilidad y reduce los tiempos en que el servicio no está disponible.

En conjunto, estas políticas permiten construir un enfoque de gestión más eficiente, basado en datos reales y ajustado a las necesidades operativas de la institución. Su aplicación contribuiría significativamente a mejorar la calidad del servicio que perciben estudiantes, docentes y personal administrativo.

4.1.3 Análisis general de encuestas y de la entrevista al personal TIC

A partir de la combinación del análisis de las encuestas dirigidas a la comunidad de usuarios y la entrevista que se realizó en la sección TIC con el responsable del área,

se extrajo un patrón homogéneo en relación con la percepción existente sobre el estado del servicio de red institucional. En los resultados obtenidos es fácilmente apreciable que una gran mayoría de los usuarios percibe la existencia de problemas relacionados con la lentitud, inestabilidad y caídas del servicio, constatadas, sobre todo, en los horarios de mayor carga académica. La mayoría de los encuestados indica que la velocidad para navegar por la red es considerada como regular o mala, dejando patente que los mayores problemas se producen en el contexto de las clases virtuales, de los usos de las plataformas institucionales y del acceso a la descarga de documentos académicos.

En consonancia con la percepción que existe, la entrevista técnica realizada deja patente que la infraestructura hace uso de un ancho de banda de forma limitada y, al mismo tiempo está sometida a un crecimiento del número de dispositivos conectados y a nuevas demandas digitales que obligan a la institución a cambiar su enfoque. El responsable TIC afirmó que hay interfaces y que hay equipos que alcanzan niveles altos de saturación en algunos momentos del día, dando lugar a cuellos de botella que afectan la Calidad de Servicio (QoS). También se deja patente que las incidencias relacionadas con la lentitud, reconexiones y pérdidas de paquetes han crecido en el tiempo, lo que pone de manifiesto la necesidad de aumentar la capacidad y la forma en que se gestiona el tráfico.

En general, usuarios y personal técnico coinciden en que la actual red institucional necesita ser optimizada, bien sea incrementando el ancho de banda, bien si invirtiendo en nuevos equipos digitales, reorganizando el tráfico o bien, implementando herramientas de monitoreo y gestión más potentes. La percepción del usuario y la evaluación del técnico confluyen en que la demanda actual supera la capacidad instalada, que se refleja, de manera directa, en la conexión dentro de la universidad

4.1.4 Análisis de la Red Existente

Analizar la red que ya existe ayuda a entender cómo está organizada toda la infraestructura tecnológica de la UPEC, qué equipos están involucrados en el tráfico, cómo se distribuye la conectividad por todo el campus y de qué forma se conectan los servicios internos con los externos. Esta revisión es clave para poder interpretar bien los resultados del monitoreo que se hizo con Zabbix y para identificar en qué puntos se está concentrando la mayor carga de tráfico.

4.1.4.1 Diagrama Físico y Lógico (hibrido).

Permite entender la red desde dos puntos de vista que se complementan: cómo están ubicados físicamente los equipos en la institución y cómo se relacionan entre sí a nivel lógico. Esta combinación da una visión completa del funcionamiento real de la infraestructura, y hace más fácil identificar las rutas del tráfico, las conexiones más importantes, cómo se distribuye todo por edificios y la forma en que están conectados los equipos en el data center, el core y los diferentes bloques.

Además, un diagrama así ayuda a interpretar con más precisión los resultados del monitoreo que se hizo con Zabbix, porque se observa el recorrido que hace el tráfico y entender por qué ciertas interfaces tienen más carga que otras. En conjunto, este enfoque que combina lo físico con lo lógico fortalece el análisis técnico y le da más solidez con una representación clara y coherente de toda la red institucional.

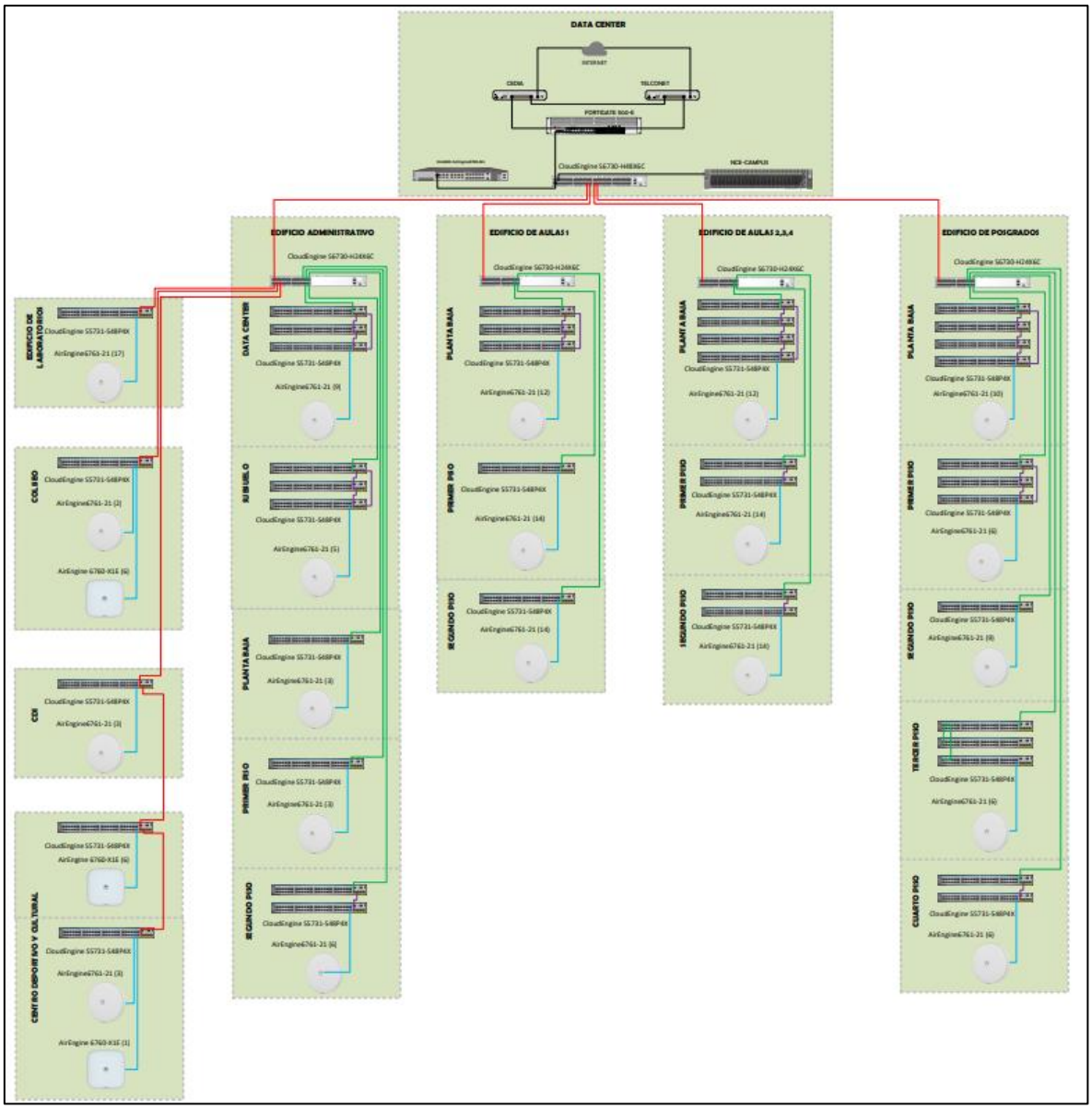


Figura 22. Diagrama Lógico y físico

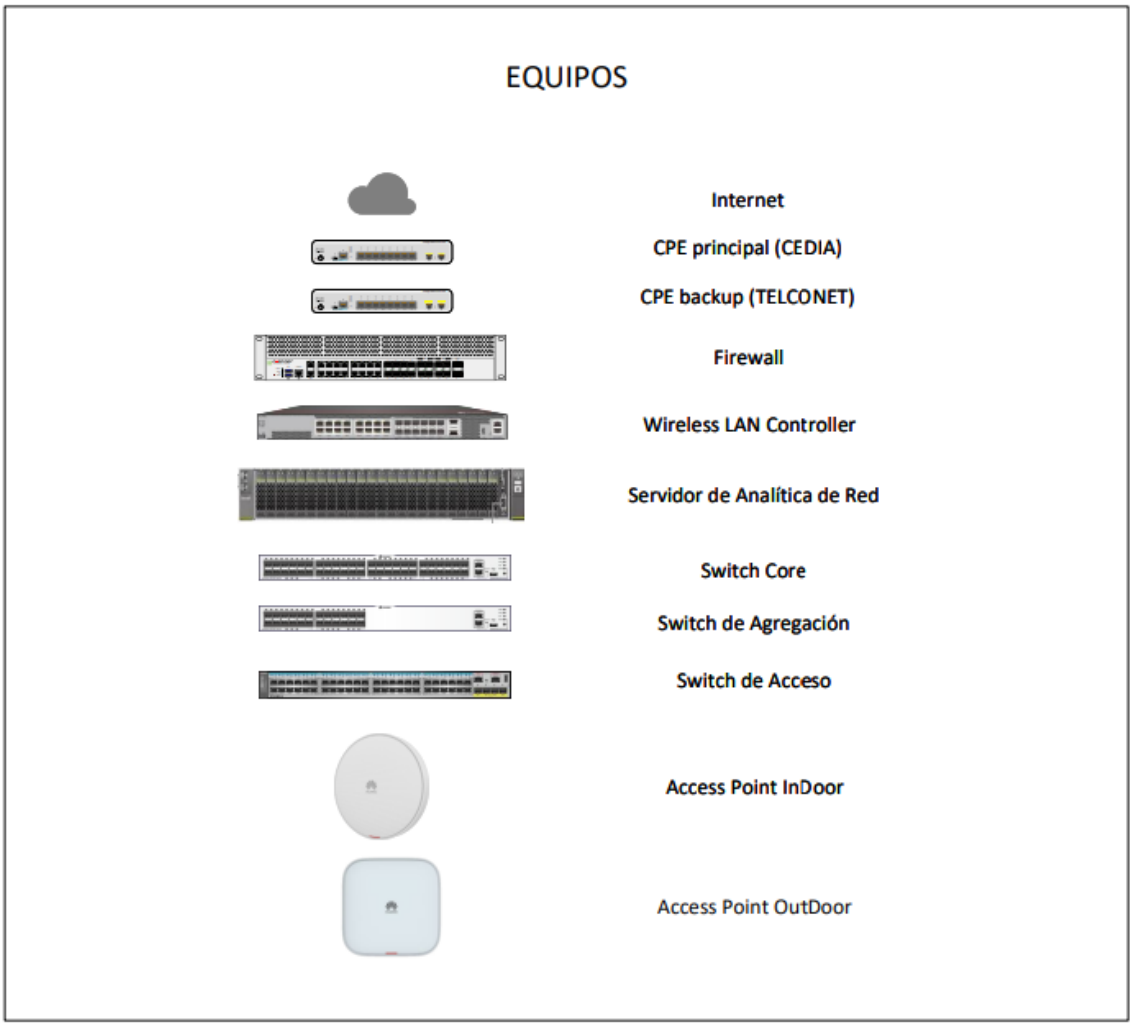


Figura 23. Equipos

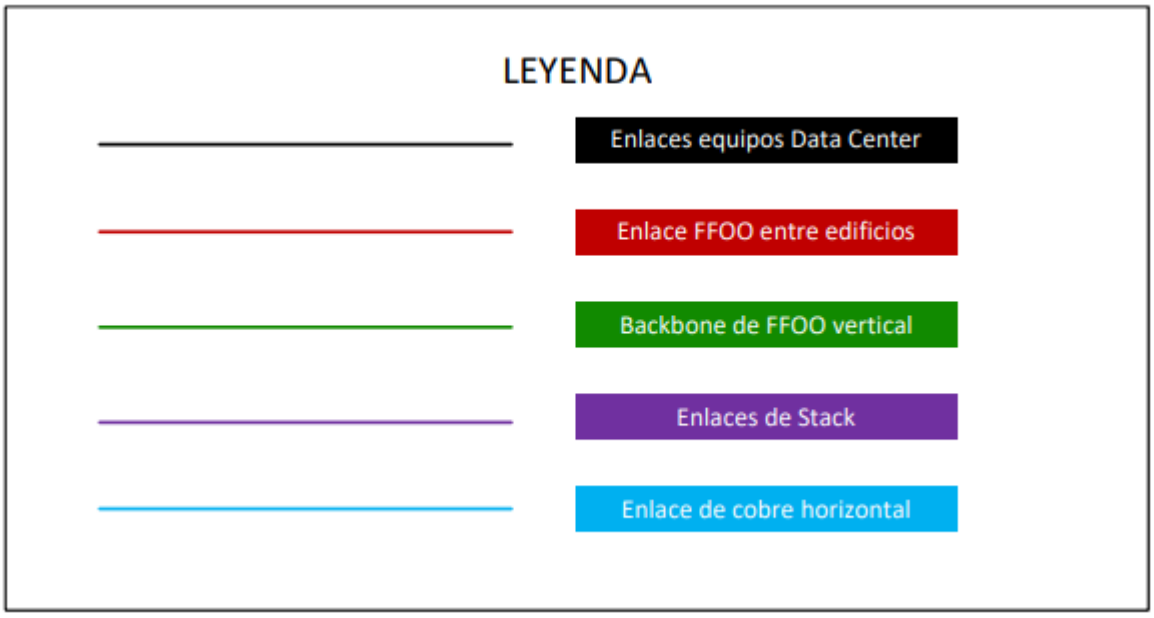


Figura 24.Leyenda

4.2. DISCUSIÓN

Al analizar los datos recopilados con Zabbix, se pudo entender mucho mejor cómo se comporta realmente el tráfico de internet en la red de la UPEC. Durante el tiempo que se estuvo observando, se notó que el flujo de información no es constante, sino que cambia bastante según las horas del día. Especialmente cuando hay clases o cuando más personas están conectadas, los gráficos mostraron subidas importantes en el uso del ancho de banda. Estos aumentos reflejan que la red está trabajando bajo mucha presión, ya que tiene que aguantar que cientos de dispositivos estén conectados al mismo tiempo.

También se descubrió que esta sobrecarga no afecta por igual a todos los puntos de la red. Algunos enlaces, sobre todo los que dan servicio a zonas con más usuarios, llegaron a niveles de uso bastante altos. Esto provocó problemas como demoras en la conexión, pérdida de paquetes de datos y bajones en la disponibilidad del servicio. Estas variaciones confirman que la red enfrenta momentos de saturación cuando aumenta el tráfico, lo que termina afectando la estabilidad y la experiencia de quienes usan las plataformas de la universidad, aplicaciones en línea o sistemas administrativos.

Algo importante que se logró con este monitoreo fue identificar qué zonas, equipos o conexiones tienen más actividad, lo cual da pistas muy útiles para planificar mejoras a futuro. Eso sí, hay que aclarar que Zabbix, con la configuración que tiene ahora, no puede decir exactamente qué tipo de tráfico está circulando. Por eso, aunque se pudo ver claramente cuánto y cómo se mueve la información, no fue posible saber qué aplicaciones o servicios específicos son los que generan mayor demanda. Aún así, esto no impide que se identifique un patrón claro: cuando muchos usuarios y dispositivos se conectan al mismo tiempo, especialmente en horas pico, eso contribuye directamente a la congestión que se detectó.

En conjunto, estos resultados permiten afirmar que la red de la UPEC trabaja con niveles de carga que varían mucho y que, en ciertos momentos, sobrepasan su capacidad ideal. Esto se refleja en esa sensación de lentitud, cortes en la navegación y problemas para acceder a los recursos de la universidad, cosas que también salieron a la luz en las encuestas que se aplicaron. El hecho de que los datos técnicos coincidan con lo que sienten los usuarios refuerza la necesidad de mejorar la gestión del tráfico, ampliar la capacidad en los puntos críticos y mantener un monitoreo

constante que permita prevenir problemas antes de que afecten las actividades académicas y administrativas.

En resumen, este estudio demuestra que la infraestructura actual, aunque funciona, necesita ajustes y estrategias de mejora para responder mejor a la creciente demanda de conectividad en el campus. El monitoreo continuo con Zabbix se vuelve una herramienta clave para esto, porque da información precisa sobre cómo se comporta el tráfico y ayuda a tomar decisiones más acertadas para mejorar la calidad del servicio de red.

V. CONCLUSIONES Y RECOMENDACIONES

5.1. CONCLUSIONES

Cuando el tráfico se dispara algo que se miró reflejado en Zabbix la red simplemente no aguanta bien. Durante esas horas pico, lo que pasa es que todo se vuelve más lento, empiezan a perderse paquetes de datos y algunas interfaces terminan completamente saturadas. Básicamente, hay partes de la red que no tienen la capacidad suficiente para manejar toda la carga que llega en ciertos momentos del día.

Con la instalación de Zabbix, se logró conseguir información bastante precisa sobre cómo se estaba moviendo el tráfico, qué tan disponible estaba la red y cuánta latencia había. Esto dio una imagen completa y al día de cómo se comportaba toda la infraestructura. La herramienta resultó muy útil porque permitió detectar cambios conforme iban sucediendo y dejó registro de las métricas clave que se necesitaban para poder evaluar el estado real de la red de forma objetiva.

A partir de la información que se recopiló, se logró identificar cuáles interfaces y partes de la red estaban llegando a niveles altos de uso. Sin embargo, no se pudo precisar exactamente qué tipo de tráfico estaba causando esa saturación, ya que Zabbix no tiene forma de clasificar qué aplicaciones o servicios están generando toda esa carga por no contar con políticas de Qos. Lo que sí quedó confirmado es que hay un aumento generalizado en el consumo durante ciertas horas del día, y ese uso tan intensivo del ancho de banda termina provocando congestión en la red.

Los datos dejaron ver una conexión clara entre esos picos de tráfico y cómo se deteriora el servicio: la latencia sube, se pierden paquetes y la disponibilidad baja temporalmente. Esto confirmó que cuando hay demasiado tráfico, el rendimiento de la red se ve afectado, sobre todo en aquellas interfaces donde la demanda rebasa lo que realmente pueden soportar.

El monitoreo dejó ver patrones bastante claros: el tráfico se incrementa durante las horas de clases y en las zonas donde hay más gente conectada. Estas variaciones se detectaron de manera repetida en varias interfaces, lo que demostró que la

demanda de conectividad no es pareja en todo momento y está directamente relacionada con las actividades que se desarrollan día a día en el campus.

***Tabla 7**. Comparativa Final*

Criterio	Antecedentes de la investigación	Tesis actual (UPEC – Tráfico IP y QoS)
Problema central estudiado	Congestión de red, saturación del tráfico, anomalías en entornos universitarios o IoT; falta de monitoreo continuo.	Saturación del tráfico IP en la UPEC y su impacto en la Calidad de Servicio (QoS).
Contexto de estudio	Universidades, centros de datos, redes IoT o infraestructuras tecnológicas generales.	Red institucional real de la UPEC con datos propios.
Herramientas usadas	Capsa, sistemas de predicción, IDS, modelos de IA, protocolos SNMP.	Zabbix completo: SNMPv2c, agentes, dashboards, triggers, reportes.
Limitaciones identificadas	Falta de sistemas especializados; poca detección de anomalías; monitoreo insuficiente; infraestructura limitada.	Ausencia histórica de monitoreo integral en la UPEC; interfaces saturadas; horas pico críticas.
Aportes principales	Demuestran la importancia de monitorear tráfico, prever congestión y aplicar técnicas de gestión.	Genera datos reales, correlación tráficoQoS y propuestas prácticas.
Variables analizadas	Tráfico IP, uso de ancho de banda, detección de anomalías, latencia, congestión.	Tráfico IP (VI) y Calidad de Servicio (VD): latencia, jitter, pérdida de paquetes, disponibilidad y satisfacción del usuario.
Tipo de evidencia	Datos históricos, simulaciones y estudios en redes no pertenecientes a la UPEC.	Datos reales en tiempo real (Zabbix), encuestas y entrevista al responsable TIC.
Metodología	Descriptivos, experimentales, predictivos o análisis generales de red.	Aplicada, descriptiva–correlacional, no experimental, corte transversal y enfoque mixto.
Relevancia para la UPEC	Sustentan la importancia del monitoreo y problemas globales.	Diagnóstico verificado, métricas reales y soluciones específicas para la UPEC.
Propuestas de mejora	Uso de IDS, modelos predictivos, técnicas QoS, gestión inteligente del tráfico.	Implementación de QoS, segmentación VLAN, ampliación de capacidad, alertas inteligentes.

5.2. RECOMENDACIONES

5.2.1. Implementar políticas de Calidad de Servicio según las necesidades de la UPEC

Dado que actualmente no hay ningún mecanismo formal de QoS funcionando en la infraestructura institucional, se recomienda ir aplicando poco a poco las políticas que se identificaron durante la investigación. Esto implica establecer una priorización del tráfico, de manera que los servicios críticos como las plataformas educativas, la telefonía IP y los sistemas administrativos puedan mantener un rendimiento estable cuando hay picos de uso. Al implementar estas políticas, se logrará que la red funcione de manera más predecible y que la congestión no termine afectando las actividades que son realmente esenciales.

5.2.2. Fortalecer la capacidad de las interfaces más críticas

Las interfaces que mostraron niveles altos de uso necesitan ser revisadas y mejoradas. Esto podría significar aumentar su capacidad, repartir mejor la carga entre los enlaces disponibles o cambiar el hardware que ya quedó obsoleto. Al atender estos puntos críticos, se logrará reducir esa saturación que se detectó y mejorar bastante la calidad del servicio, especialmente en esas horas pico cuando hay más actividad académica y administrativa.

5.2.3. Complementar Zabbix con la herramienta de seguridad que ya tiene la UPEC

Aunque Zabbix permite monitorear el tráfico y ver cómo está la red en tiempo real, no puede identificar qué tipo de tráfico es ni aplicar controles sobre las aplicaciones. Por eso, sería conveniente integrarlo con la herramienta o plataforma de seguridad que ya está instalada en la UPEC puede ser un firewall con políticas de filtrado, control de aplicaciones o inspección más profunda. Con esta combinación no solo se podría monitorear, sino también gestionar el tráfico de manera más efectiva para evitar congestiones y mejorar la protección de toda la red institucional.

5.2.4. Implementar una segmentación de red basada en VLAN

Organizar la red con VLAN ayudaría a distribuir el tráfico de forma más balanceada entre las áreas administrativas, de docentes y de estudiantes. Esta división reduciría las congestiones que no tienen por qué ocurrir y mejoraría cómo se maneja el ancho de banda cuando hay mucha demanda. Además, facilitaría dar prioridad a los servicios más importantes, sobre todo en días de exámenes, clases en línea o actividades institucionales que necesitan que la conexión sea estable.

5.2.5. Configurar alertas inteligentes en Zabbix

Para poder anticiparse a problemas de saturación, convendría configurar alertas automáticas que avisen al equipo de TIC cuando el uso del ancho de banda pase del 80% o cuando haya cambios raros en el tráfico. Estas alertas permitirían reaccionar a tiempo, acortando el tiempo de respuesta cuando algo falle, evitando caídas largas y asegurando que los servicios institucionales sigan funcionando sin interrupciones.

5.2.6. Capacitar a la comunidad universitaria en buenas prácticas de uso de la red

El rendimiento de la red también tiene que ver con cómo la usan las personas. Sería útil hacer campañas internas para concientizar y promover prácticas responsables

como no hacer descargas innecesarias, cerrar las sesiones que no se están usando, aprovechar bien las plataformas institucionales y evitar consumir ancho de banda sin motivo. Estas acciones ayudarían directamente a mantener un flujo de tráfico más óptimo y a reducir la congestión en las horas más complicadas.

VI. REFERENCIAS BIBLIOGRÁFICAS

Altmemi, D. K. (2022). A new approach based on intelligent method to classify Quality of Service. *Informatica*, 46(4), 603–614. https://doi.org/10.15388/23-INFOR504

Campos Arenas, A. (2021). Métodos mixtos de investigación: Integración de la investigación cuantitativa y la investigación cualitativa. Bogotá, Colombia: Editorial Magisterio.

Cisco. (2020). Managing IP Network Traffic for Quality of Service. Cisco Press.
Cita textual incluida: "Lean IT enables organizations to optimize the value delivered by IT services by eliminating waste, improving processes and increasing quality for the end user." (p. 12).

Cristobo, L., Ibarrola, E., Casado-O'Mara, I., & Zabala, L. (2024). *Global Quality of Service (QoX) management for wireless networks*. Electronics, 13(16), 3113. https://doi.org/10.3390/electronics13163113

Debian Project. (2024). *About Debian*. https://www.debian.org/intro/about
https://www.vanharen.store/lean-it-foundation-courseware

Fortinet. (s. f.). *¿Qué es la calidad de servicio (QoS) en las redes?* https://www.fortinet.com/lat/resources/cyberglossary/qos-quality-of-service

Fotopoulou, E., Mamais, G., Michalakelis, C., & Varvarigou, T. (2021). *Adaptive QoS monitoring in complex IP networks*. Journal of Network and Systems Management, 29(4), 1–20. https://doi.org/10.1007/s10922-021-09625-4

Guinea Cabrera, M. A. (2023). *Implementación de un sistema de detección de intrusos (IDS) mediante la inspección de tráfico a través de la red* (Trabajo de fin de máster). Universitat Oberta de Catalunya.

Guo, Y., Li, J., Liu, X., & Yang, Y. (2023). *Traffic Management in IoT Backbone Networks Using GNN*. Sensors, 23(16), 7091. https://doi.org/10.3390/s23167091

Hernández, R. V. (2024). *Analysis of Ecuador's higher education processes*. Sapienza: International Journal of Interdisciplinary Studies, 3(2), 45–60. https://doi.org/10.51798/sijis.v3i2.421

Hernández-Sampieri, R., Fernández-Collado, C., & Baptista-Lucio, M. del P. (2014). Metodo logía de la investigación (6ta ed.). México D.F.: McGRAW-HILL / Interamericana Editores, S.A. DE C.V.

Hernández-Sampieri, R., Fernández-Collado, C., & Baptista-Lucio, P. (2022). Metodología de la investigación (7.ª ed.). McGraw-Hill Interamericana.

IBM. (2023). *¿Qué es la detección y respuesta de red (NDR)?*. IBM. https://www.ibm.com/mx-es/topics/ndr

Juniper Networks. (2021). *Quality of Service (QoS) Overview*. Juniper Documentation.

Lean IT Association. (2017). Lean IT Foundation Courseware. Van Haren Publishing.

Lwin, S. S., Myint, C. C., & Maw, W. W. (2019). *Network Monitoring System for University*. International Journal of Trend in Scientific Research and Development, 3(3), 793–798. https://www.ijtsrd.com/papers/ijtsrd22768.pdf

Morán, J. A. C. (2024). Evaluación de la calidad de los sitios web de universidades en Ecuador durante 2023 mediante análisis de componentes principales. *Revista Científica y Tecnológica UPSE*, 11(2), 112–120. https://doi.org/10.26423/rctu.v11i2.925

Moreno Muro, F.-J., Skorin-Kapov, N., & Pavon-Marino, P. (2019). Revisiting core traffic growth in the presence of expanding CDNs. Computer Networks, 154, 1–11. https://doi.org/10.1016/j.comnet.2019.03.005

PostgreSQL Global Development Group. (s. f.). *About PostgreSQL*. https://www.postgresql.org/about/

Pranata, R., Rizky, D., & Sasmita, A. (2023). *Performance evaluation of WiFi networks in university dormitory halls*. Journal of ICT Research and Applications, 17(1), 1–12. https://doi.org/10.5614/itbj.ict.res.appl.2023.17.1.1

Saha, S. (2022). *An empirical study on Internet traffic prediction using real IP network traffic*. arXiv. https://arxiv.org/abs/2205.01590

Vigoya Morales, L. V. (2023). Aplicación de algoritmos de aprendizaje automático para la detección de anomalías de tráfico en entornos IoT (Tesis doctoral). Universidade da Coruña.

Yaseen, N., Arzani, B., Chintalapudi, K., Ranganathan, V., Frujeri, F., Hsieh, K., Berger, D., Liu, V., & Kandula, S. (2021). *Towards a cost vs. quality sweet spot for monitoring networks*. HotNets '21.

Zabbix Documentation. (2024). *Zabbix Overview*. https://www.zabbix.com/documentation/current/en/manual/introduction/overview

VII. ANEXOS

Anexo 1. Certificado del abstract por parte de idiomas

UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI FOREIGN AND NATIVE LANGUAGES CENTER

ABSTRACT- EVALUATION SHEET

NAME: STEFFANY DAYANA REVELO MONTENEGRO
DATE: Miércoles, 21 de enero de 2026
Topic: : "Trafico de redes IP y calidad de servicio."

MARKS AWARDED **QUANTITATIVE AND QUALITATIVE**

VOCABULARY AND WORD USE	Use new learnt vocabulary and precise words related to the topic	Use a little new ocabulary and some appropriate words related to the topic	Use basic vocabulary and simplistic words related to the topic	Limited vocabulary and inadequate words related to the topic
	EXCELLENT: 2 ☐	GOOD: 1,5 ■	AVERAGE: 1 ☐	LIMITED: 0,5 ☐
WRITING COHESION	Clear and logical progression of ideas and supporting paragraphs.	Adequate progression of ideas and supporting paragraphs.	Some progression of ideas and supporting paragraphs.	Inadequate ideas and supporting paragraphs.
De	EXCELLENT: 2 ■	GOOD: 1,5 ☐	AVERAGE: 1 ☐	LIMITED: 0,5 ☐
ARGUMENT	The message has been communicated very well and identify the type of text	The message has been communicated appropriately and identify the type of text	Some of the message has been communicated and the type of text is little confusing	The message hasn't been communicated and the type of text is inadequate
	EXCELLENT: 2 ■	GOOD: 1,5 ☐	AVERAGE: 1 ☐	LIMITED: 0,5 ☐
CREATIVITY	Outstanding flow of ideas and events	Good flow of ideas and events ■	Average flow of ideas and events	Poor flow of ideas and events
	EXCELLENT: 2 ☐	GOOD: 1,5	AVERAGE: 1 ☐	LIMITED: 0,5 ☐
SCIENTIFIC SUSTAINABILITY	Reasonable, specific and supportable opinion or thesis statement	Minor errors when supporting the thesis statement	Some errors when supporting the thesis statement	Lots of errors when supporting the thesis statement
	EXCELLENT: 2 ■	GOOD: 1,5 ☐	AVERAGE: 1 ☐	LIMITED: 0,5 ☐
TOTAL/AVERAGE	9 - 10: EXCELLENT 7 - 8,9: GOOD 5 - 6,9: AVERAGE 0 - 4,9: LIMITED	TOTAL 9		

UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI- FOREIGN AND NATIVE LANGUAGES CENTER

Informe sobre el Abstract de Artículo Científico o Investigación.

Autor: STEFFANY DAYANA REVELO MONTENEGRO
Fecha de recepción del abstract: Domingo, 18 de diciembre de 2025
Fecha de entrega del informe: Miércoles, 21 de enero de 2026

El presente informe validará la traducción del idioma español al inglés si alcanza un porcentaje de: 9 – 10 Excelente.

Si la traducción no está dentro de los parámetros de 9 – 10, el autor deberá realizar las observaciones presentadas en el ABSTRACT, para su posterior presentación y aprobación.

Observaciones:

Después de realizar la revisión del presente abstract, éste presenta una apropiada traducción sobre el tema planteado en el idioma Inglés. Según la rúbrica de evaluación de la traducción en Inglés, ésta alcanza un valor de 9; por lo cual se valida dicho trabajo.

Atentamente

MA. Jairo Guevara
DIRECTOR DE CENTROS ACADÉMICOS Y DE FORMACIÓN COMPLEMENTARIA

Anexo 2. Manual de Instalación Zabbix

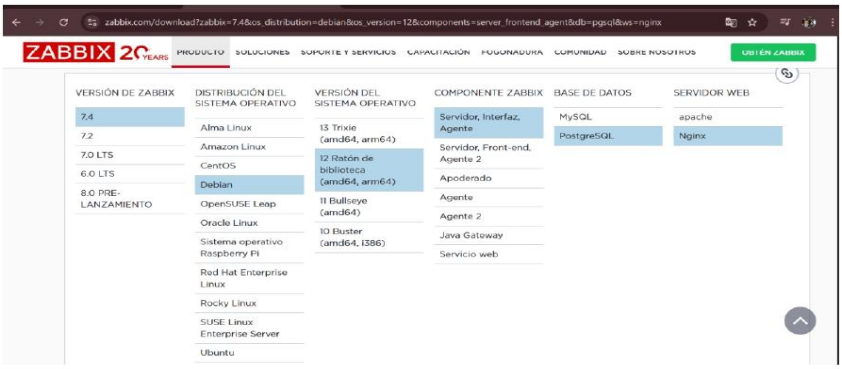
UNIVERSIDAD POLITECNICA ESTATAL DEL CARCHI

FACULTAD DE INDUSTRIAS AGROPECUARIAS Y CIENCIAS AMBIENTALES

CARRERA DE COMPUTACION

Educamos para transformar el mundo

MANUAL DE INSTALLACION ZABBIX



Zabbix es una herramienta de monitoreo de red que permite supervisar, en tiempo real, el funcionamiento de servidores, equipos y servicios dentro de una institución. Su propósito es detectar fallos o lentitud en la red antes de que afecten a los usuarios, ofreciendo una visión clara del rendimiento y del uso de los recursos tecnológicos.

A diferencia de otras soluciones comerciales, Zabbix es completamente open source, lo que significa que no requiere licencias y puede adaptarse a las necesidades de cada organización. Gracias a su interfaz web, los administradores pueden observar el estado general de la red, recibir alertas automáticas y tomar decisiones preventivas para mantener la estabilidad del sistema.

Según TechRadar (2025), Zabbix se destaca como una de las herramientas de monitoreo de red más completas y potentes del mercado, gracias a su carácter open source, su alta capacidad de personalización y su escalabilidad, lo que la convierte en una opción ideal para entornos institucionales y educativos donde se requiere control total sin costos de licencia.

Este manual de instalación de Zabbix 7.4. Zabbix es una herramienta poderosa de monitoreo de infraestructura que permitirá supervisar el rendimiento y disponibilidad de los servidores, aplicaciones y servicios de red.

En este tutorial, se aprende a instalar Zabbix 7.4 en un sistema Debian 12 utilizando PostgreSQL como base de datos.

Paso 1: Verificar Conectividad de Red

Lo primero es asegurar que el servidor tiene conectividad. Desde la máquina Windows, verificar que se puede hacer ping al servidor:

ping 10.100.100.108

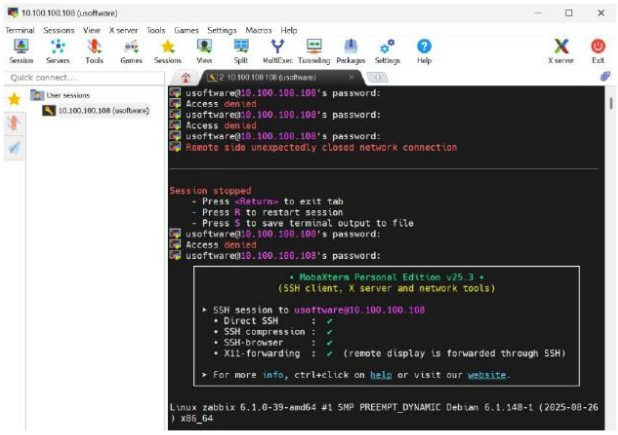
```
C:\Users\Steffy Revelo>ping 10.100.100.108

Haciendo ping a 10.100.100.108 con 32 bytes de datos:
Respuesta desde 10.100.100.108: bytes=32 tiempo=6ms TTL=62
Respuesta desde 10.100.100.108: bytes=32 tiempo=7ms TTL=62
Respuesta desde 10.100.100.108: bytes=32 tiempo=8ms TTL=62
Respuesta desde 10.100.100.108: bytes=32 tiempo=8ms TTL=62

Estadísticas de ping para 10.100.100.108:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 6ms, Máximo = 8ms, Media = 7ms

C:\Users\Steffy Revelo>
```

Ver respuestas exitosas sin pérdida de paquetes. Esto confirma que la red está funcionando correctamente.

Paso 2: Conectarse al Servidor

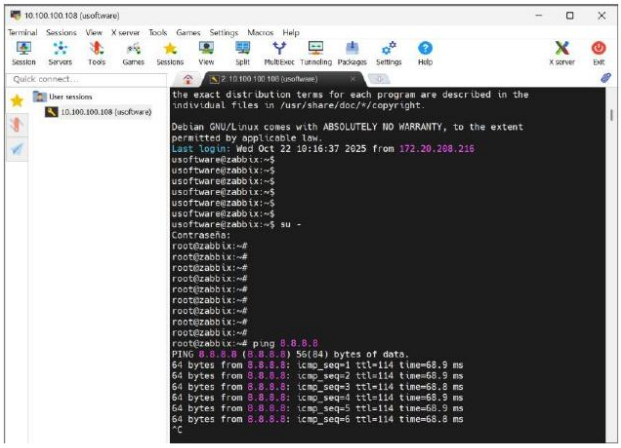
Utilizar un cliente SSH como MobaXterm o PuTTY para conectar al servidor Debian:

ssh usoftware@10.100.100.108



Una vez conectado, elevar privilegios a root:

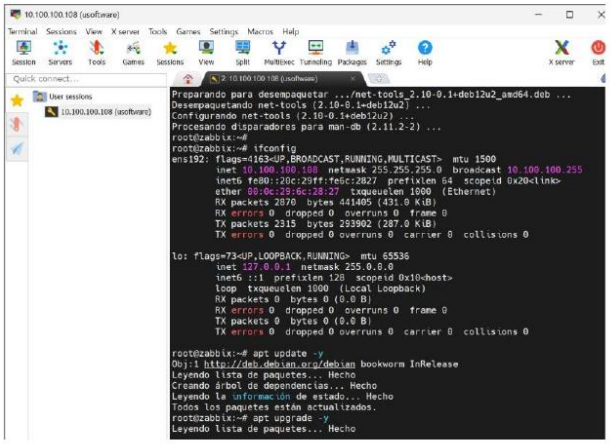
su -



Paso 3: Actualizar el Sistema

Antes de instalar cualquier paquete, es fundamental actualizar el sistema operativo:

apt update && apt upgrade -y

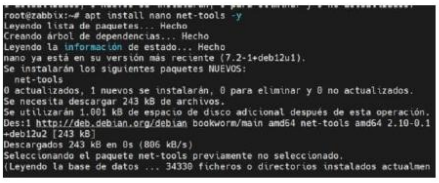


Este comando descargará e instalará todas las actualizaciones disponibles. Puede tomar unos minutos dependiendo de tu conexión.

Paso 4: Instalar Herramientas de Red

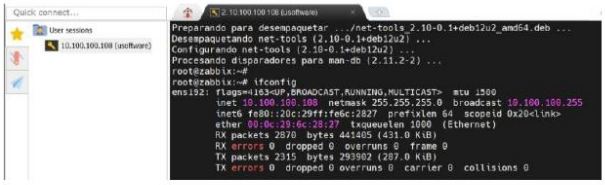
Instalar herramientas útiles como net-tools para diagnóstico de red:

apt install nano net-tools -y



Verificar la configuración de red con:

ifconfig

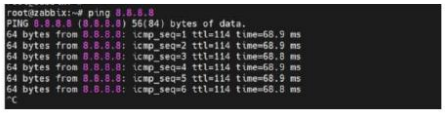


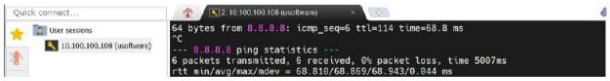
Confirmar que el servidor tiene la IP correcta (en este caso 10.100.100.108).

Paso 5: Verificar Conectividad a Internet

Realizar un ping a un servidor DNS público para confirmar que hay acceso a Internet:

ping 8.8.8.8





Paso 6: Descargar e Instalar el Repositorio de Zabbix

Descargar el paquete de repositorio oficial de Zabbix 7.4:

wget https://repo.zabbix.com/zabbix/7.4/release/debian/pool/main/z/zabbix-release/zabbix-release_latest_7.4+debian12_all.deb

Instalar el paquete descargado:

dpkg -i zabbix-release_latest_7.4+debian12_all.deb

```
root@zabbix:~# dpkg -i zabbix-release_latest_7.4+debian12_all.deb
Seleccionando el paquete zabbix-release previamente no seleccionado.
(Leyendo la base de datos ... 34385 ficheros o directorios instalados actualmen
te.)
Preparando para desempaquetar zabbix-release_latest_7.4+debian12_all.deb ...
Desempaquetando zabbix-release (1:7.4-1+debian12) ...
Configurando zabbix-release (1:7.4-1+debian12) ...
```

Actualizar la lista de paquetes:

apt update

```
root@zabbix:~# apt update
Obj:1 http://deb.debian.org/debian bookworm InRelease
Des:2 https://repo.zabbix.com/zabbix/7.4/release/debian bookworm InRelease [2.4
59 B]
Des:3 https://repo.zabbix.com/zabbix-tools/debian-ubuntu bookworm InRelease [2.
476 B]
Des:4 https://repo.zabbix.com/zabbix/7.4/stable/debian bookworm InRelease [4.65
4 B]
Des:5 https://repo.zabbix.com/zabbix/7.4/release/debian bookworm/main Sources [
932 B]
Des:6 https://repo.zabbix.com/zabbix/7.4/release/debian bookworm/main all Packa
ges [628 B]
Des:7 https://repo.zabbix.com/zabbix-tools/debian-ubuntu bookworm/main Sources
[1.367 B]
Des:8 https://repo.zabbix.com/zabbix-tools/debian-ubuntu bookworm/main all Pack
ages [866 B]
```

Paso 7: Instalar Componentes de Zabbix

Instalar el servidor Zabbix, el frontend web, el agente y los scripts SQL necesarios:

apt install zabbix-server-pgsql zabbix-frontend-php php8.2-pgsql zabbix-nginx-conf zabbix-sql-scripts zabbix-agent -y

```
root@zabbix:~# apt install zabbix-server-pgsql zabbix-frontend-php php8.2-pgsql
 zabbix-nginx-conf zabbix-sql-scripts zabbix-agent
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
  fontconfig-config fonts-dejavu fonts-dejavu-core fonts-dejavu-extra fping
  libabsl20220623 libaom3 libavif15 libc-ares2 libcurl4 libdav1d5 libde265-0
  libdeflate0 libevent-core-2.1-7 libevent-extra-2.1-7
  libevent-pthreads-2.1-7 libfontconfig1 libgav1-1 libgd3 libheif1 libjbig0
  libjpeg62-turbo liblerc4 liblzd17 libmodbus5 libncurses6 libnuma1 libodbc2
  libonig5 libopenipmi0 libpq5 libravle0 libsensors-config libsensors5
  libsnmp-base libsnmp40 libsodium23 libssh-4 libsvtav1enc1 libtiff6 libwebp7
  libx265-199 libxpm4 libyuv0 nginx nginx-common php-bcmath php-common
```

Este proceso instalará todos los componentes necesarios junto con sus dependencias. Tomará varios minutos.

Paso 8: Configurar PostgreSQL

8.1 Crear Usuario de Base de Datos

Primero, crear el usuario zabbix en PostgreSQL:

sudo -u postgres createuser --pwprompt zabbix

```
Configurando postgresql-contrib (15+248+deb12u1) ...
Configurando postgresql (15+248+deb12u1) ...
Procesando disparadores para man-db (2.11.2-2) ...
Procesando disparadores para libc-bin (2.36-9+deb12u13) ...
root@zabbix:~# sudo -u postgres createuser --pwprompt zabbix
```

Cuando se solicite la contraseña, ingresar una segura y recordarla.

8.2 Crear Base de Datos

Crear la base de datos para Zabbix:

sudo -u postgres createdb -O zabbix zabbix

```
root@zabbix:~# postgres createuser --pwprompt zabbix
-bash: postgres: orden no encontrada
```

8.3 Importar el Esquema Inicial

Importar las tablas y datos iniciales a la base de datos:

zcat /usr/share/zabbix/sql-scripts/postgresql/server.sql.gz | sudo -u zabbix psql zabbix

```
# zcat /usr/share/zabbix/sql-scripts/postgresql/server.sql.gz | sudo -u zabbix psql zabbix
```

Este proceso puede tomar unos minutos. Se vera muchos mensajes de creación de tablas y configuración.

8.4 Verificar la Base de Datos

Conéctarse a PostgreSQL y verificar que las tablas se crearon correctamente:

psql -U zabbix -d zabbix

```
postgres=# psql -U zabbix -d zabbix
postgres-# show database
postgres-# show tables
postgres-# psql \l
postgres-# \c zabbix
You are now connected to database "zabbix" as user "postgres".
zabbix-# \dt
zabbix-# \d users
zabbix-# SELECT * FROM users;
```

Ver las tablas creadas y los usuarios por defecto (Admin y guest).

Paso 9: Configurar el Servidor Zabbix

Editar el archivo de configuración del servidor:

nano /etc/zabbix/zabbix_server.conf

Buscar la línea DBPassword y añadir la contraseña que se configuro para el usuario zabbix:

DBPassword=tu_contraseña_aquí

```
Edit file /etc/zabbix/zabbix_server.conf

DBPassword=password
```

Guardar el archivo (Ctrl + O, Enter) y sal (Ctrl + X).

Paso 10: Configurar Nginx

Editar el archivo de configuración de Nginx para Zabbix:

nano /etc/zabbix/nginx.conf

Descomentar y configura las siguientes líneas:

listen 8080;

server_name tu_dominio_o_ip;

Guardar los cambios.

Paso 11: Iniciar los Servicios

Reiniciar y habilitar los servicios para que inicien automáticamente:

systemctl restart zabbix-server zabbix-agent nginx php8.2-fpm

systemctl enable zabbix-server zabbix-agent nginx php8.2-fpm

Verificar que los servicios estén corriendo:

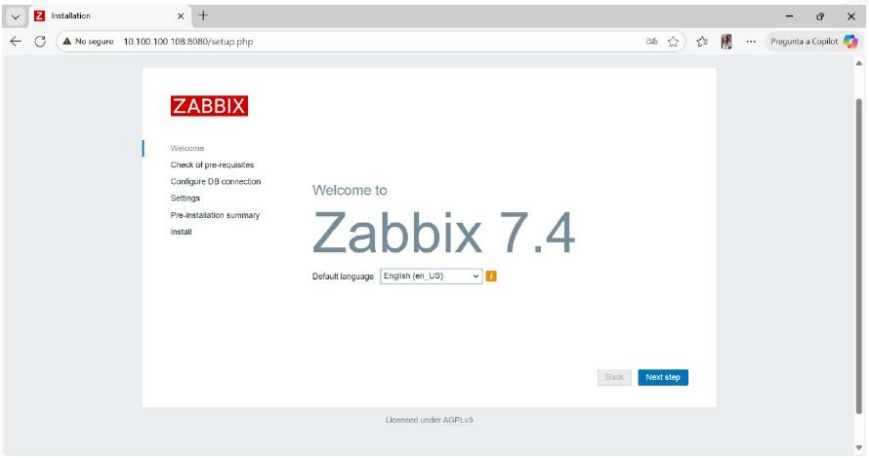
systemctl status zabbix-server

Paso 12: Configurar Zabbix desde la Interfaz Web

12.1 Acceder a la Interfaz

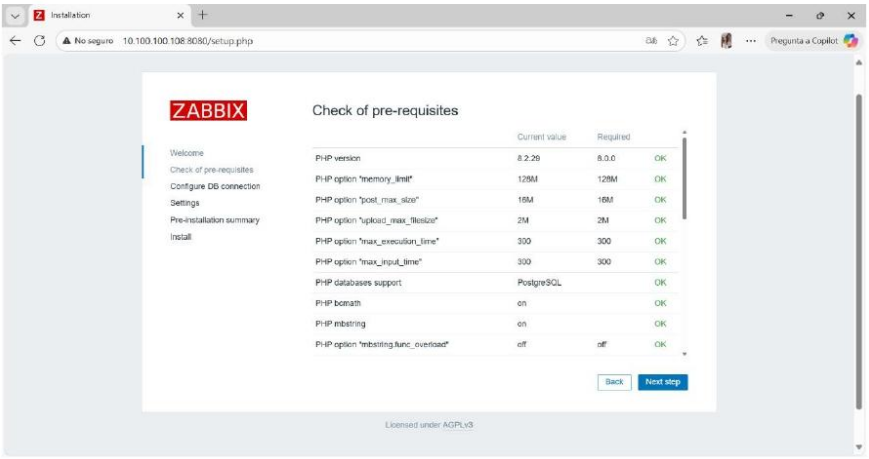
Abrir navegador web y acceder a:

http://10.100.100.108:8080



12.2 Verificar Pre-requisitos

Zabbix verificará automáticamente que todos los requisitos estén cumplidos:



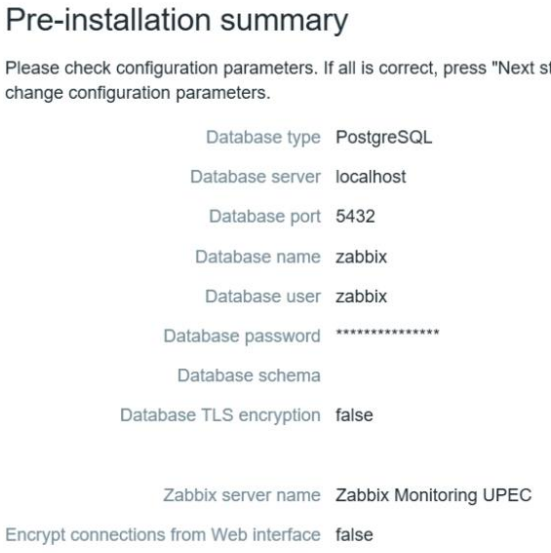
Si todo está en verde con "OK", clic en **Next step**.

12.3 Configurar Conexión a la Base de Datos

Completar los datos de conexión:

- **Database type**: PostgreSQL

12.5 Resumen de Pre-instalación



Revisar todos los parámetros configurados:

Si todo es correcto, clic en **Next step** para completar la instalación.

12.6 Instalación Completada

La instalación se ha completado exitosamente. Clic en **Finish**.

Paso 13: Acceder a Zabbix

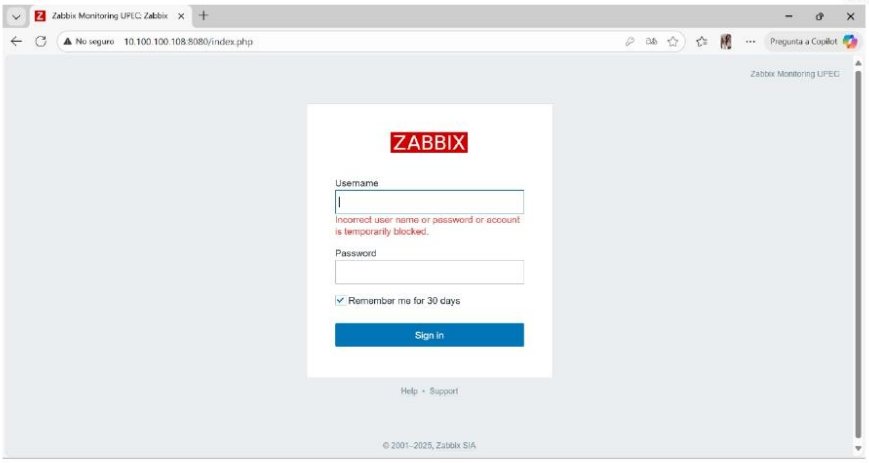
Acceder a la interfaz de Zabbix:

http://10.100.100.108:8080

Credenciales por defecto:

- **Usuario**:
- **Contraseña**:

Importante: Cambiar la contraseña del usuario inmediatamente después del primer inicio de sesión por seguridad.



Verificación Final

Para asegurar de que todo funciona correctamente:

1. **Verificar el estado del servidor Zabbix**:
2. systemctl status zabbix-server
3. **Revisar los logs en caso de problemas**:
4. tail -f /var/log/zabbix/zabbix_server.log
5. **Confirmar que PostgreSQL está funcionando**:
6. systemctl status postgresql

Conclusión

Se ha instalado exitosamente Zabbix 7.4 en tu servidor Debian 12. Ahora hay una plataforma de monitoreo completa lista para supervisar la infraestructura.

Referencias

- Documentación oficial de Zabbix
- Zabbix en GitHub
- Comunidad Zabbix

Conclusión del Manual

El presente Manual de Installacion de Zabbix Monitoring Universidad Politécnica Estatal del Carchi (UPEC) ha sido desarrollado con el propósito de guiar, capacitar y asistir al personal técnico y administrativo en el uso adecuado de la herramienta de monitoreo de red Zabbix.

La implementación de Zabbix en la UPEC representa un avance significativo en la gestión de la red universitaria, al ofrecer monitoreo en tiempo real, detección temprana de fallos y una administración eficiente de los recursos tecnológicos.

Gracias a su carácter open source, escalable y adaptable, Zabbix se consolida como una solución sostenible y de bajo costo para la supervisión de servicios críticos en entornos educativos.

Se recomienda mantener actualizado el sistema y las credenciales de acceso, así como documentar cualquier cambio en la infraestructura monitoreada, garantizando la continuidad y seguridad del servicio.

Finalmente, este manual busca convertirse en una herramienta de consulta y apoyo permanente para el Departamento de Tecnologías de la Información y Comunicación (TIC) de la UPEC, contribuyendo al fortalecimiento de la calidad del servicio de red y la optimización de los procesos tecnológicos institucionales.

Recomendaciones finales

- Realizar copias de seguridad periódicas de la base de datos de Zabbix.
- Mantener actualizado el software a la versión más reciente y estable.
- Revisar las políticas de notificación y autenticación cada semestre.
- Capacitar de forma continua al personal encargado del monitoreo.
- Documentar todos los cambios realizados en la configuración del sistema.

Créditos

Autora: Steffany Revelo

Tutor: Ing. Milton del Hierro Mosquera

Carrera: Ingeniería en Computación

Institución: Universidad Politécnica Estatal del Carchi (UPEC)

Año: 2025

Anexo 3. Manual de Usuario

UNIVERSIDAD POLITECNICA ESTATAL DEL CARCHI

FACULTAD DE INDUSTRIAS AGROPECUARIAS Y CIENCIAS AMBIENTALES

CARRERA DE COMPUTACION

MANUAL DE USUARIO ZABBIX

Zabbix es una herramienta de monitoreo de red que permite supervisar, en tiempo real, el funcionamiento de servidores, equipos y servicios dentro de una institución. Su propósito es detectar fallos o lentitud en la red antes de que afecten a los usuarios, ofreciendo una visión clara del rendimiento y del uso de los recursos tecnológicos.

A diferencia de otras soluciones comerciales, Zabbix es completamente open source, lo que significa que no requiere licencias y puede adaptarse a las necesidades de cada organización. Gracias a su interfaz web, los administradores pueden observar el estado general de la red, recibir alertas automáticas y tomar decisiones preventivas para mantener la estabilidad del sistema.

Según TechRadar (2025), Zabbix se destaca como una de las herramientas de monitoreo de red más completas y potentes del mercado, gracias a su carácter open source, su alta capacidad de personalización y su escalabilidad, lo que la convierte en una opción ideal para entornos institucionales y educativos donde se requiere control total sin costos de licencia.

1. Pantalla de inicio de sesión en Zabbix

La imagen muestra la interfaz de acceso al sistema **Zabbix Monitoring UPEC**, disponible a través del enlace **http://zabbix.upec.edu.ec:8080**. En esta página, los usuarios deben ingresar su **nombre de usuario (Username)** y **contraseña (Password)** para iniciar sesión de forma segura.

La opción **"Remember me for 30 days"** permite mantener la sesión activa durante treinta días, evitando repetir el ingreso frecuente de credenciales. Al hacer clic en **"Sign in"**, el sistema valida los datos y redirige al panel principal de monitoreo.

Nota: Se recomienda acceder únicamente desde una red segura y mantener actualizadas las credenciales asignadas.

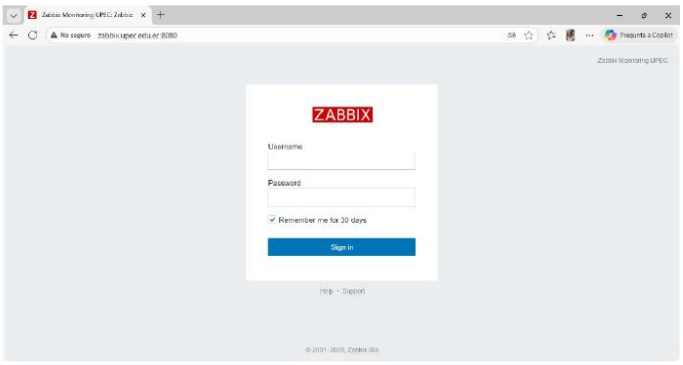


Figura 1. Pantalla de inicio de sesión en Zabbix Monitoring UPEC mediante la dirección *http://zabbix.upec.edu.ec:8080*

2. Panel principal de Zabbix (Global View)

Al ingresar correctamente al sistema mediante la dirección http://zabbix.upec.edu.ec:8080, se muestra el panel principal o vista global, donde el usuario puede observar el estado general de la red, los equipos monitoreados y los recursos del servidor. Esta vista ofrece información en tiempo real sobre el rendimiento y posibles alertas dentro del entorno de monitoreo.

2.1 Barra lateral de navegación

Dentro de la barra lateral izquierda, el apartado "Dashboards" permite acceder al panel principal donde se muestran los indicadores generales del sistema. En esta sección, el usuario puede visualizar de forma resumida el estado de los equipos monitoreados, el rendimiento del servidor y las alertas activas. Su propósito es ofrecer una visión global del funcionamiento de la red, facilitando la toma de decisiones rápidas ante cualquier eventualidad.

2.2 Filtros de visualización temporal

En la parte superior del panel se encuentra el filtro "From" y "To", que permite seleccionar el rango de tiempo para analizar los datos del monitoreo. Además, se incluyen accesos rápidos como "Last 2 days", "This week" o "Last 30 minutes" para ajustar la visualización sin necesidad de escribir manualmente las fechas.

2.3 Información del sistema

En el recuadro lateral derecho se muestran datos técnicos importantes, como:

Estado del servidor (Zabbix server is running).

Versión del servidor y de la interfaz web.

Número de hosts y plantillas activas.

Esta sección permite verificar que el sistema esté en funcionamiento correcto.

2.4 Utilización de recursos

En la parte inferior se visualizan indicadores sobre el uso de CPU, memoria, disponibilidad de hosts y problemas por severidad. Estos gráficos ofrecen una visión rápida del rendimiento general del sistema y ayudan a detectar sobrecargas o fallos.

2.5 Indicadores en tiempo real

El panel también muestra información en vivo, como la hora del sistema (zona horaria America/Guayaquil) y los valores por segundo, que reflejan la frecuencia de actualización de los datos monitoreados.

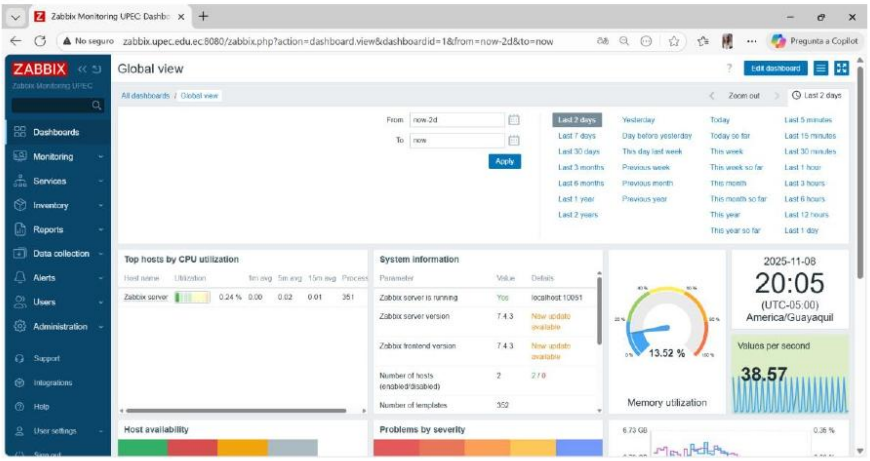


Figura 2. Vista global del panel principal de Zabbix Monitoring UPEC mediante la dirección http://zabbix.upec.edu.ec:8080

.

2.6 Disponibilidad de hosts

En este apartado se muestra el estado actual de los equipos o dispositivos conectados a la red. Los colores indican su nivel de disponibilidad: verde para los activos, rojo para

los no disponibles, y tonos intermedios que representan estados mixtos o desconocidos. Esta información permite identificar de forma inmediata si algún dispositivo presenta fallas o desconexiones dentro del sistema.

2.7 Problemas activos

La sección denominada “Current problems” presenta los incidentes que están ocurriendo en tiempo real dentro de la red. Cada fila muestra la hora, el tipo de dispositivo, la descripción del problema y la duración del evento. En la imagen se evidencian alertas en equipos Cisco IOS, con mensajes del tipo “Link down”, lo que indica una pérdida de enlace en las interfaces de red de áreas específicas como Tesorería, Bodega y Dirección de Infraestructura.
Esta función es esencial para el diagnóstico rápido, ya que permite conocer exactamente dónde se produce el fallo y cuánto tiempo lleva activo.

2.7 Recursos y ubicación del sistema

En la parte derecha del panel se presentan los gráficos de uso de memoria y valores por segundo, que reflejan la carga de procesamiento del servidor Zabbix. Junto a ellos, se muestra un mapa de ubicación que identifica de manera visual el sitio donde se encuentran los dispositivos monitoreados.
Ambos elementos ayudan al administrador a comprender el rendimiento general del sistema y localizar los puntos donde se generan las incidencias.

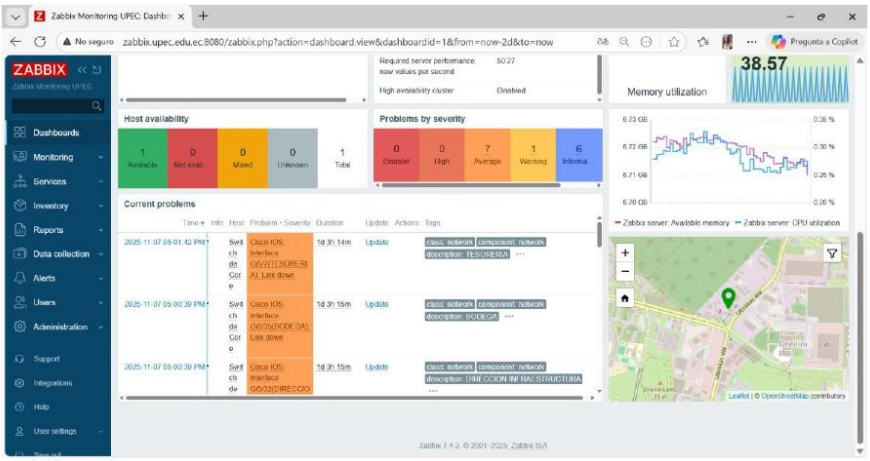


Figura 3. Panel principal con disponibilidad de hosts, problemas activos y recursos del sistema en *Zabbix Monitoring UPEC* mediante la dirección *http://zabbix.upec.edu.ec:8080*.

3. Monitoring

El módulo Monitoring de Zabbix tiene como función principal supervisar en tiempo real el estado y rendimiento de los equipos conectados a la red institucional. Desde este menú, el usuario puede acceder a diferentes vistas que muestran información sobre los problemas actuales, los hosts activos, los datos más recientes y los mapas de red.

3.1 Problems

La sección Problems muestra todos los incidentes detectados por el sistema, organizados según su tipo, severidad y dispositivo afectado. Es una de las vistas más utilizadas por los administradores, ya que permite detectar, filtrar y analizar fallos de forma precisa.

En la parte superior del panel se encuentra una barra de búsqueda avanzada, donde cada campo cumple una función específica:

- **Show:** selecciona qué tipo de registros mostrar: *Recent problems* (problemas recientes), *Problems* (todos los problemas activos) o *History* (historial completo de eventos solucionados).
- **Host groups / Hosts:** permiten elegir un grupo o equipo específico dentro de la red. En la imagen se muestra el host "Switch de Core", encargado de manejar el tráfico central.
- **Triggers:** define las condiciones que generan una alerta (por ejemplo, desconexión de un enlace o sobreuso de memoria).
- **Problem:** campo libre donde se puede escribir manualmente el tipo de problema que se desea localizar.
- **Severity:** clasifica los eventos según su nivel de importancia: *Not classified*, *Information*, *Warning*, *Average*, *High* o *Disaster*.
- **Tags:** filtra eventos según etiquetas específicas, combinando condiciones mediante *And/Or* para obtener búsquedas más precisas.
- **Host inventory:** permite vincular los problemas a los datos del inventario del dispositivo (modelo, ubicación, tipo, etc.).
- **Show tags y Tag name:** controlan la forma en que se muestran las etiquetas, pudiendo verse completas (*Full*), abreviadas (*Shortened*) o no mostrarse (*None*).
- **Show operational data:** añade información técnica adicional, como IP, interfaz o descripción del evento.

- **Compact view y Show details:** ajustan la vista general del panel; el primero simplifica la presentación de datos, mientras que el segundo muestra información más específica.
- **Show timeline:** activa una línea temporal que facilita identificar la evolución de los eventos.
- **Highlight whole row:** resalta la fila completa de cada evento para una mejor lectura visual.
- **Acknowledgement status:** muestra todos los eventos o filtra entre los que están *pendientes* (Unacknowledged) y los *revisados* (Acknowledged).

En la parte inferior se encuentran los botones de acción:

- **Apply:** ejecuta la búsqueda con los filtros seleccionados.
- **Reset:** borra los filtros aplicados para iniciar una nueva consulta.
- **Save as:** permite guardar configuraciones de búsqueda personalizadas.

Debajo de estos controles se muestra la **tabla de resultados**, donde se detallan los eventos detectados por el sistema:

- **Time:** fecha y hora en la que se generó el problema.
- **Severity:** nivel de criticidad (en este caso, *Average*).
- **Info / Host:** identifican el equipo afectado, como el *Switch de Core*.
- **Problem:** describe la causa del evento; por ejemplo, *"Cisco IOS: Interface Gi5/7 (TESORERÍA): Link down"*, lo cual significa que la conexión del puerto se ha perdido.
- **Duration:** indica cuánto tiempo lleva activo el problema.
- **Update:** permite editar el estado del evento o agregar observaciones.
- **Tags:** agrupa información sobre el tipo y descripción del problema (*class: network*, *component: network*, *description: TESORERÍA*).

Finalmente, en la parte superior derecha de la interfaz se encuentra la opción "Export to CSV", que permite descargar los resultados en un archivo para generar informes o respaldos.

En conjunto, esta vista facilita el control total de los eventos de red, ayudando al administrador a priorizar los más críticos y mantener la estabilidad de la infraestructura tecnológica.

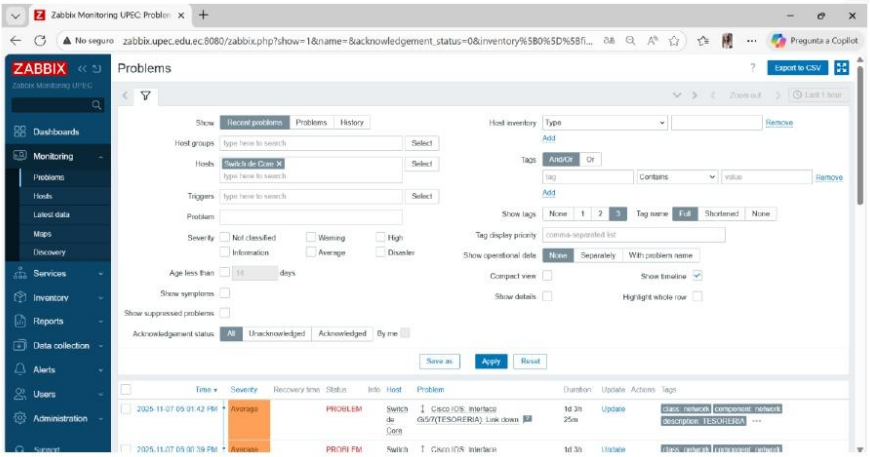


Figura 4. Vista completa del apartado *Problems* dentro del módulo *Monitoring* de Zabbix Monitoring UPEC mediante la dirección *http://zabbix.upec.edu.ec:8080*.

3.2 Hosts

La opción Hosts dentro del módulo *Monitoring* permite visualizar y administrar todos los dispositivos o equipos que están siendo monitoreados por el sistema Zabbix. Desde esta vista, el usuario puede comprobar la disponibilidad, el estado de conexión, los datos asociados y los problemas activos de cada host configurado.

En la parte superior se encuentra el panel de filtros, que permite realizar búsquedas específicas según distintos criterios:

- **Name:** sirve para buscar un dispositivo por su nombre asignado dentro del sistema.
- **Host groups:** permite filtrar los hosts pertenecientes a un grupo en particular.
- **IP / DNS / Port:** estos campos ayudan a localizar un host por su dirección IP, nombre de dominio o puerto de comunicación configurado.
- **Severity:** permite aplicar un filtro por nivel de severidad de los eventos registrados en ese host (por ejemplo: *Warning*, *Average* o *High*).
- **Status:** selecciona si se desean visualizar los hosts *habilitados (Enabled)*, *deshabilitados (Disabled)* o ambos (*Any*).
- **Tags:** posibilita buscar equipos por etiquetas asociadas, lo cual es útil cuando se manejan redes grandes o con diferentes categorías de dispositivos.
- **Show hosts in maintenance:** al activarse, muestra también los dispositivos que se encuentran en mantenimiento o con monitoreo temporalmente suspendido.

- **Show suppressed problems:** permite incluir o excluir hosts con alertas temporalmente ocultas.

Los botones Apply, Reset y Save as ofrecen acciones rápidas para ejecutar la búsqueda, restablecer filtros o guardar configuraciones personalizadas, respectivamente.

En la parte superior derecha se ubica el botón "Create host", que permite registrar un nuevo dispositivo para ser monitoreado.

Debajo del panel de filtros se presenta la tabla principal, donde se listan los hosts activos dentro del sistema. En la imagen se visualizan dos:

- **Switch de Core:** con dirección IP **172.20.1.1:161**, monitoreado mediante el protocolo **SNMP**. Está asociado a etiquetas como *class: network* y *target: cisco-ios*, lo que indica que pertenece a la infraestructura de red principal.
- **Zabbix server:** con dirección **127.0.0.1:10050**, monitoreado con el agente **ZBX**, que corresponde al propio servidor donde está instalada la plataforma.

La tabla también muestra información adicional:

- **Availability:** indica si el host responde correctamente a las consultas.
- **Latest data:** enlaza a los datos más recientes recopilados del host.
- **Problems:** muestra el número de incidentes detectados clasificados por severidad.
- **Graphs:** da acceso a las gráficas de rendimiento del equipo.
- **Dashboards:** enlaza con paneles personalizados relacionados con ese host.
- **Web:** disponible si el dispositivo tiene monitoreo web configurado.

Esta vista permite al administrador tener una panorámica general del estado de todos los equipos, verificar su comunicación con el servidor y acceder rápidamente a sus métricas o incidencias.

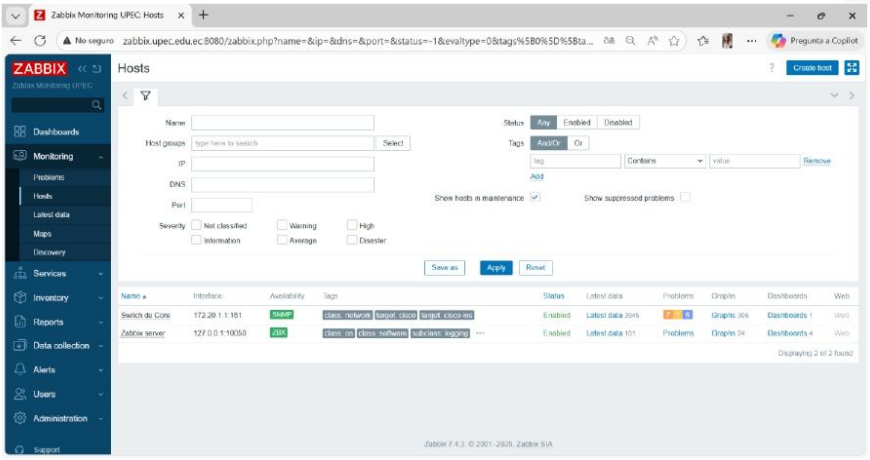


Figura 5. Vista del apartado *Hosts* dentro del módulo *Monitoring* de Zabbix Monitoring UPEC mediante la dirección *http://zabbix.upec.edu.ec:8080*.

3.3 Latest data

El apartado Latest data dentro del módulo *Monitoring* permite visualizar los valores más recientes obtenidos por el sistema en tiempo real de cada host o dispositivo monitoreado. Esta sección resulta fundamental para el análisis técnico, ya que muestra los datos actualizados de variables como temperatura, uso de CPU, estado de puertos y otros indicadores de rendimiento.

En la parte superior se encuentra el panel de filtros, que ofrece opciones para personalizar la consulta según distintos parámetros:

- **Host groups / Hosts:** permiten seleccionar grupos o dispositivos específicos. En la imagen se muestra el equipo Switch de Core, encargado de la conectividad principal de la red institucional.
- **Name:** sirve para buscar un parámetro concreto, como “CPU utilization” o “Temperature”.
- **Tags:** posibilita aplicar filtros según etiquetas o categorías, por ejemplo, component, interface o system.
- **Show tags y Tag name:** definen cómo se visualizan las etiquetas (completas, abreviadas o sin mostrar).
- **State:** permite elegir entre All (todos los datos), Normal (elementos en funcionamiento correcto) o Not supported (elementos que no están reportando información).
- **Show details:** al activarse, agrega información adicional en la tabla de resultados.

En la parte inferior de este panel aparecen tres botones funcionales:

- **Apply:** ejecuta la búsqueda con los filtros seleccionados.
- **Reset:** elimina los filtros aplicados para iniciar una nueva consulta.
- **Save as:** guarda configuraciones de búsqueda personalizadas para uso posterior.

Debajo del panel de control se presenta un resumen de los datos filtrados:

- **Hosts:** indica el número total de equipos incluidos en la búsqueda (en este caso, el Switch de Core).
- **Tags y Tag values:** muestran las etiquetas asociadas a cada componente, como cpu, memory, temperature o interface, seguidas de la cantidad de registros disponibles por cada categoría.

Más abajo, se despliega una tabla detallada con los resultados de los parámetros monitoreados. En ella se muestran columnas clave como:

- **Host:** nombre del dispositivo que reporta la información.
- **Name:** descripción del parámetro observado (por ejemplo, CPU utilization, air inlet: Temperature, air outlet: Temperature status).
- **Last check:** muestra el tiempo transcurrido desde la última actualización de datos (por ejemplo, 53 segundos o 3 minutos).
- **Last value:** presenta el valor más reciente obtenido, expresado en unidades como porcentaje (%), grados Celsius (°C) o estado (normal).
- **Change:** refleja la variación del valor respecto a la lectura anterior, ayudando a detectar incrementos o descensos abruptos.
- **Tags:** clasifica cada dato según su tipo o componente (component: cpu, component: temperature, etc.).
- **Info / Graph:** ofrece acceso directo a la gráfica de comportamiento del parámetro seleccionado, facilitando un análisis visual del rendimiento.

Esta vista proporciona un control en tiempo real de los valores críticos del sistema, permitiendo detectar desviaciones, sobrecalentamientos o picos de carga antes de que afecten el funcionamiento de la red. Gracias a su presentación clara y ordenada, el usuario puede identificar rápidamente los puntos que requieren atención y tomar decisiones preventivas.

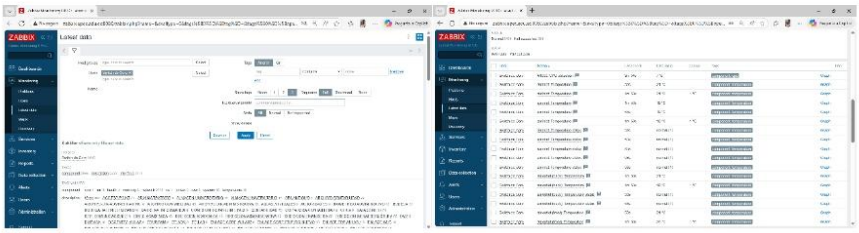


Figura 6. Vista del apartado Latest data dentro del módulo Monitoring de Zabbix Monitoring UPEC, mostrando la recopilación en tiempo real de los valores monitoreados mediante la dirección http://zabbix.upec.edu.ec:8080.

3.4 Maps

El apartado Maps dentro del módulo *Monitoring* permite crear y gestionar mapas de red personalizados que representan de forma visual la estructura de los dispositivos monitoreados. Esta herramienta facilita la comprensión gráfica de la infraestructura, mostrando cómo se interconectan los equipos y permitiendo detectar fallas o desconexiones de manera más intuitiva.

En la parte superior del panel se encuentra la barra de búsqueda, donde el campo Name permite localizar un mapa específico escribiendo su nombre. Los botones Apply y Reset sirven para aplicar el filtro o restaurar la vista original, respectivamente.

A la derecha de esta barra se ubican dos opciones importantes:

- **Create map:** permite generar un nuevo mapa de red, añadiendo manualmente los equipos o hosts que se deseen visualizar.
- **Import:** posibilita cargar mapas previamente creados en otros sistemas o respaldos de Zabbix.

Debajo, se muestra una tabla con los mapas existentes. En la imagen se visualiza uno llamado “Local network”, que representa la red interna de la institución. En la tabla se muestran los siguientes campos:

- **Name:** nombre asignado al mapa, que permite identificarlo dentro del sistema.
- **Width y Height:** indican las dimensiones del mapa en píxeles, en este caso **680 x 200**, lo que determina su tamaño dentro de la interfaz.
- **Actions:** contiene opciones para administrar el mapa.
- **Properties:** permite visualizar o modificar las características generales, como el título, tamaño o fondo.
- **Edit:** abre el editor gráfico donde se pueden añadir, mover o eliminar equipos y enlaces dentro del mapa.

En la parte inferior, el sistema también ofrece las opciones Export y Delete, las cuales se habilitan cuando se selecciona uno o varios mapas. Estas funciones permiten respaldar los mapas existentes o eliminarlos de forma permanente.

Gracias a esta vista, el usuario puede observar de manera centralizada y visual la topología de red, detectando rápidamente interrupciones o desconexiones entre los equipos. Además, los mapas resultan útiles para documentar la infraestructura tecnológica y optimizar la supervisión del sistema.

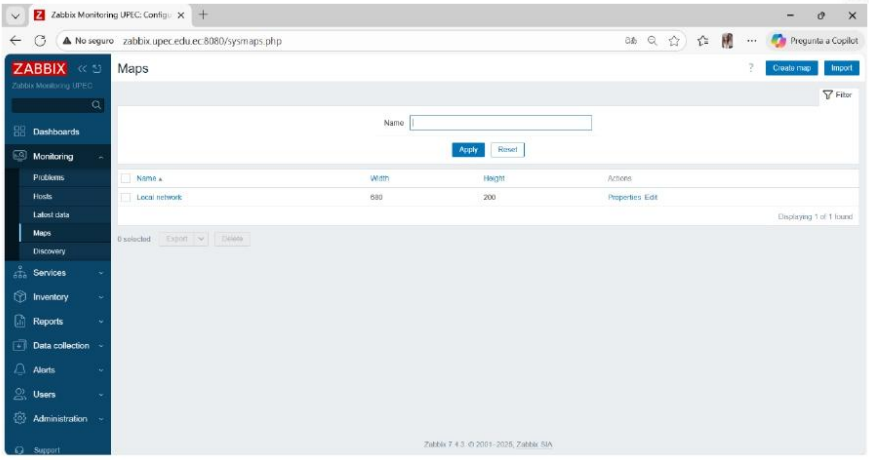


Figura 7. Vista del apartado *Maps* dentro del módulo *Monitoring* de Zabbix Monitoring UPEC mediante la dirección *http://zabbix.upec.edu.ec:8080*.

3.4.1 Opción "Properties"

Dentro del apartado Maps, al seleccionar la acción Properties, el sistema despliega una ventana con los parámetros generales del mapa seleccionado. Esta opción permite configurar la estructura, apariencia y comportamiento del mapa de red antes de ser visualizado o editado.

En esta vista se pueden observar los siguientes campos principales:

- **Owner:** indica el usuario responsable del mapa, en este caso Admin (Zabbix Administrator).
- **Name:** nombre asignado al mapa, que facilita su identificación (por ejemplo, Local network).
- **Width / Height:** definen el tamaño del mapa en píxeles, determinando el espacio de visualización disponible.
- **Background image:** permite agregar una imagen de fondo que sirva como base del mapa, útil para ubicar gráficamente edificios o áreas físicas de la red.
- **Background scale:** ajusta la proporción de esa imagen si se utiliza.
- **Automatic icon mapping:** ofrece la posibilidad de asignar íconos de manera automática a los diferentes dispositivos o servicios representados.
- **Icon highlight:** al activarse, resalta los íconos de los equipos cuando ocurre un evento o cambio de estado.
- **Mark elements on trigger status change:** marca de forma visual los dispositivos cuando cambian a un estado de alerta o falla.
- **Display problems:** define cómo se mostrarán los problemas detectados dentro del mapa (por ejemplo, expandiendo uno o mostrando todos).

- **Advanced labels y Map element label type:** permiten personalizar los textos que acompañan a cada elemento.
- **Show map element labels / Show link labels:** determinan si los nombres y enlaces entre equipos estarán siempre visibles o si se ocultarán automáticamente.
- **Minimum severity:** define el nivel mínimo de severidad de los eventos que se mostrarán en el mapa, desde Not classified hasta Disaster.
- **Show suppressed problems:** incluye o excluye los problemas que han sido temporalmente ocultados.

Estos parámetros permiten que el mapa sea visual, informativo y dinámico, ayudando al usuario a identificar rápidamente las zonas críticas dentro de la red.

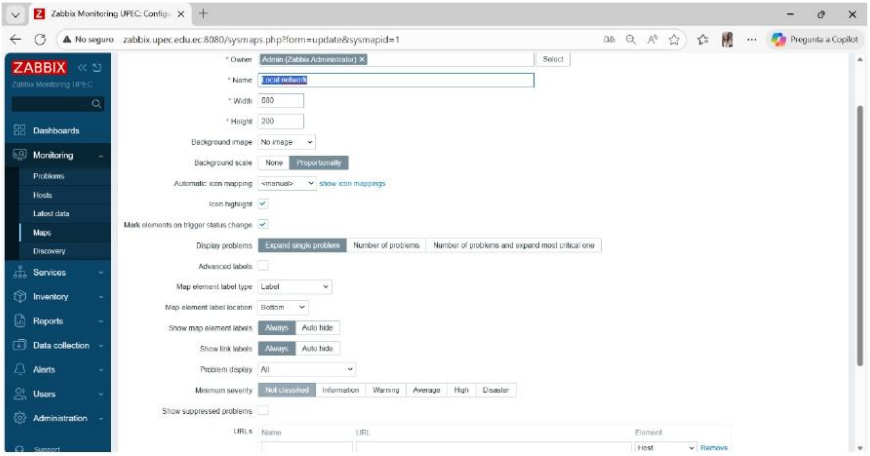


Figura 8. Configuración general del mapa de red en la opción Properties dentro del módulo Monitoring de Zabbix Monitoring UPEC, donde se establecen el tamaño, nombre, propietario y parámetros visuales del mapa mediante la dirección http://zabbix.upec.edu.ec:8080.

3.4.2 Opción "Sharing" dentro de Properties

En la pestaña Sharing, el sistema permite establecer los niveles de acceso y visibilidad del mapa. Existen dos tipos de configuración:

- **Private:** restringe el acceso únicamente al usuario propietario o a los grupos asignados manualmente.
- **Public:** permite que cualquier usuario con acceso a Zabbix pueda visualizar el mapa.

Además, se pueden agregar permisos específicos para:

- **User groups (grupos de usuarios):** se define qué grupos pueden ver o editar el mapa.
- **Users (usuarios individuales):** asigna permisos personalizados a cuentas específicas.

En la parte inferior, los botones Update, Clone, Delete y Cancel permiten guardar los cambios, crear una copia del mapa, eliminarlo o cancelar las modificaciones realizadas.

Esta opción es muy útil cuando el monitoreo se realiza en equipo, ya que garantiza que solo los usuarios autorizados puedan modificar o consultar la información representada.

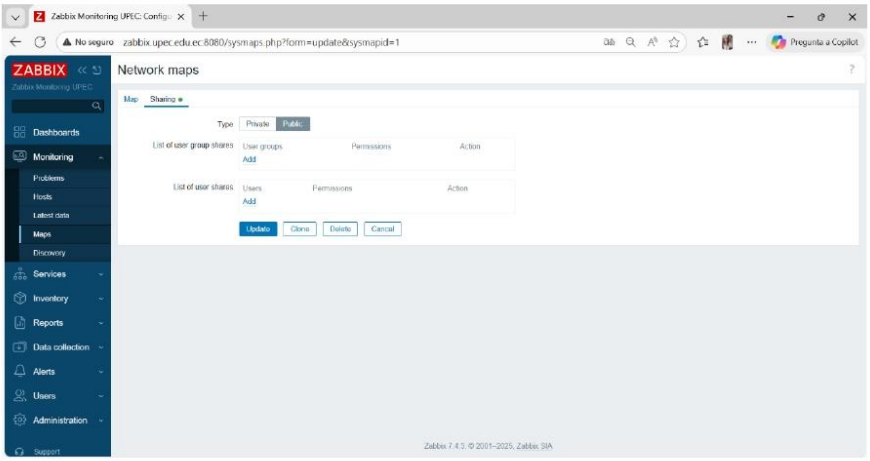


Figura 9. Configuración de permisos y visibilidad del mapa en la pestaña Sharing, donde se asignan accesos a usuarios o grupos específicos dentro del entorno de Zabbix Monitoring UPEC.

3.4.3 Opción "Edit"

La opción Edit permite acceder al editor gráfico del mapa de red, donde el usuario puede construir o modificar visualmente la topología de los dispositivos.

En la parte superior del editor se encuentran varias herramientas clave:

- **Map element (Add / Remove):** permite agregar o eliminar elementos del mapa, como servidores, switches o enlaces.
- **Link (Add / Remove):** crea conexiones entre los dispositivos para mostrar cómo están interconectados.
- **Expand macros:** permite ver información adicional o variables del sistema.
- **Grid (Shown / On):** activa una cuadrícula de referencia que facilita la alineación de los elementos.
- **Align map elements:** organiza automáticamente los equipos en el mapa para mantener un orden visual.
- **Update:** guarda los cambios realizados.

En el área central del mapa se observa el Zabbix server (127.0.0.1), representado mediante un ícono con el logotipo del sistema. Este componente simboliza el servidor principal encargado de recopilar la información de los equipos monitoreados.

Desde esta vista, el usuario puede añadir más elementos, moverlos libremente dentro del lienzo y establecer las conexiones correspondientes entre ellos, logrando una representación clara y estructurada de la red institucional.

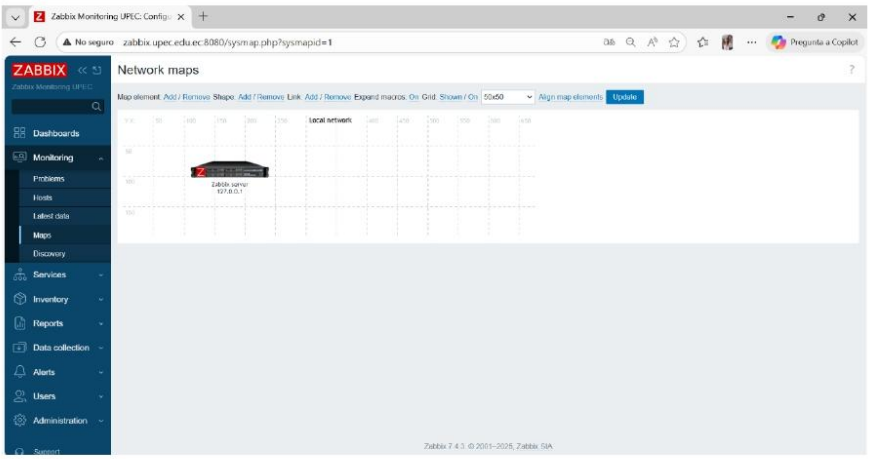


Figura 10. Vista del editor gráfico en la opción Edit, donde se añaden, conectan y organizan los elementos que conforman el mapa de red institucional en Zabbix Monitoring UPEC mediante la dirección http://zabbix.upec.edu.ec:8080.

3.5 Discovery

La opción Discovery, dentro del módulo Monitoring, tiene como finalidad detectar de manera automática los dispositivos y servicios activos dentro de la red institucional. Esta función simplifica el trabajo del administrador, ya que evita la necesidad de registrar manualmente cada equipo, permitiendo que el sistema identifique los nuevos dispositivos que se conectan a la red.

En la parte superior de la ventana se encuentra la barra de búsqueda y filtrado, donde el campo Discovery rule permite seleccionar o escribir la regla de descubrimiento que se desea aplicar. Las reglas determinan el rango de direcciones IP o segmentos de red que Zabbix explorará en busca de equipos disponibles.

A continuación, se encuentran los botones principales:

- **Apply:** ejecuta la búsqueda según la regla seleccionada, iniciando el proceso de detección automática.
- **Reset:** elimina los filtros o parámetros aplicados para volver a la vista inicial.

Debajo del panel de control, la interfaz muestra una tabla con los resultados del descubrimiento. Esta tabla presenta tres columnas principales:

- **Discovered device:** lista los dispositivos detectados dentro del rango especificado por la regla.
- **Monitored host:** indica si el dispositivo ya está siendo supervisado por el sistema Zabbix o si se trata de un nuevo hallazgo.
- **Uptime/Downtime:** muestra el tiempo de actividad o inactividad de cada dispositivo, útil para evaluar su disponibilidad.

En la imagen, la tabla aparece vacía con el mensaje "No data found", lo que significa que no se ha ejecutado aún ninguna regla de descubrimiento o que no se han encontrado dispositivos activos en el rango configurado.

Esta función es esencial en redes grandes o en crecimiento, ya que permite mantener un control actualizado de todos los equipos conectados, detectar nuevos dispositivos no registrados y fortalecer la seguridad mediante la supervisión continua del entorno tecnológico.

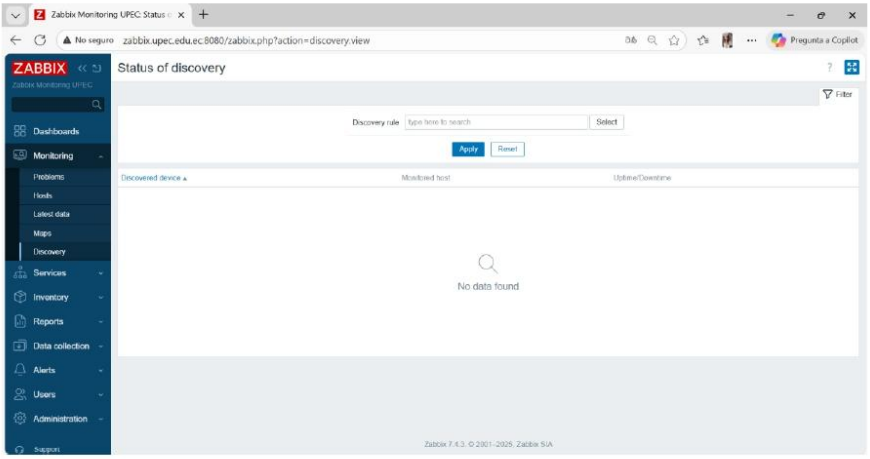


Figura 11. Vista del apartado Discovery dentro del módulo Monitoring de Zabbix Monitoring UPEC, donde se ejecutan reglas de detección automática de dispositivos mediante la dirección http://zabbix.upec.edu.ec:8080.

4. Services

El módulo Services de Zabbix permite gestionar y supervisar los servicios críticos de la infraestructura tecnológica, evaluando su disponibilidad y estado en tiempo real. A diferencia del monitoreo por hosts, este apartado se enfoca en la calidad y continuidad de los servicios ofrecidos, como correo institucional, red interna, plataformas educativas, entre otros.

4.1 Services

Dentro del módulo, la opción Services presenta una vista general donde se listan los servicios registrados y su estado operativo actual. Esta interfaz ayuda al administrador a identificar rápidamente si algún servicio se encuentra activo, en fallo o presenta advertencias.

En la parte superior del panel se ubica la barra de búsqueda y filtrado, la cual está compuesta por los siguientes campos:

- **Name:** permite buscar un servicio específico por su nombre dentro del sistema.
- **Status:** ofrece tres opciones para filtrar los resultados:
    - Any: muestra todos los servicios, sin importar su estado.
    - OK: filtra los servicios que están funcionando correctamente.
    - Problem: muestra únicamente los servicios que presentan fallas o interrupciones.
- **Tags:** posibilita aplicar filtros mediante etiquetas, combinando criterios con las opciones And/Or para búsquedas más precisas.
- **Apply:** ejecuta la búsqueda según los filtros definidos.
- **Reset:** limpia los campos para volver a la vista inicial.

En la parte inferior de la interfaz, se muestra la tabla principal de resultados, que incluye las siguientes columnas:

- **Name:** nombre del servicio configurado.
- **Status:** indica si el servicio está activo o presenta algún problema.
- **Root cause:** muestra la causa raíz del problema en caso de que exista una alerta asociada.
- **Created at:** detalla la fecha y hora de creación del servicio en Zabbix.
- **Tags:** visualiza las etiquetas asociadas al servicio para su clasificación o agrupación.

En la imagen mostrada, la tabla se encuentra vacía, lo que indica que aún no se han configurado servicios para monitoreo. Una vez añadidos, el sistema mostrará su estado en tiempo real, permitiendo supervisar su estabilidad y detectar interrupciones con rapidez.

Esta herramienta es esencial para las instituciones, ya que proporciona una visión centralizada del rendimiento de los servicios clave, ayudando a garantizar la calidad de la red y la continuidad de las operaciones.

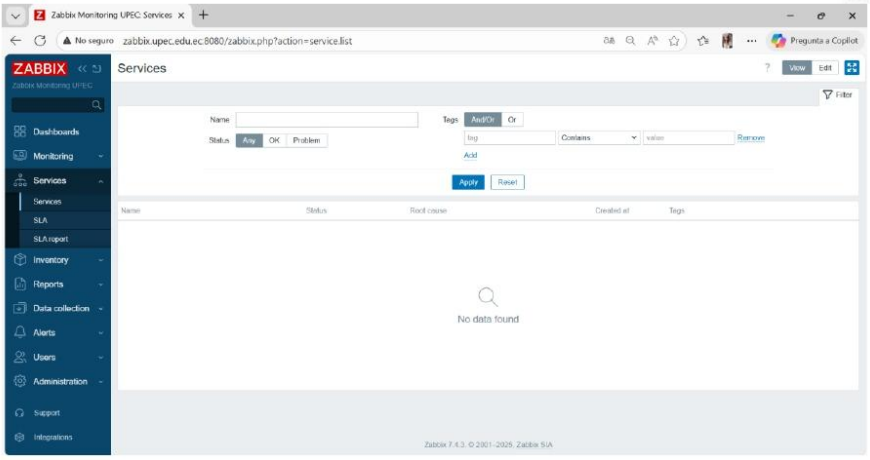


Figura 12. Vista general del apartado Services dentro del módulo Services de Zabbix Monitoring UPEC, donde se gestionan los servicios institucionales y su estado operativo mediante la dirección http://zabbix.upec.edu.ec:8080.

4.2 SLA

El apartado SLA (Service Level Agreement) dentro del módulo Services permite definir, medir y controlar los niveles de servicio que deben cumplirse dentro de una organización. A través de esta función, Zabbix ayuda a establecer indicadores de rendimiento y cumplimiento (conocidos como SLO – Service Level Objectives) que garantizan la calidad de los servicios ofrecidos por la infraestructura tecnológica.

En la parte superior de la interfaz se encuentra la barra de búsqueda y filtrado, compuesta por los siguientes elementos:

- **Name:** campo que permite buscar un Acuerdo de Nivel de Servicio específico dentro del sistema.
- **Status:** ofrece tres opciones para filtrar los registros:
    - Any: muestra todos los SLA creados, sin importar su estado.
    - Enabled: presenta solo los SLA activos.
    - Disabled: muestra los que han sido desactivados.
- **Service tags:** permite aplicar filtros por etiquetas, combinando criterios mediante las opciones And/Or.
- **Apply:** ejecuta la búsqueda según los filtros establecidos.
- **Reset:** elimina los filtros para volver a la vista inicial.

A la derecha del panel se encuentra el botón "Create SLA", que permite registrar un nuevo acuerdo de nivel de servicio, definiendo parámetros como su nombre, tiempo de evaluación y las métricas que serán supervisadas.

Debajo del panel de búsqueda se encuentra la tabla principal, donde se listan los SLA configurados en el sistema. Cada uno de ellos contiene la siguiente información:

- **Name:** nombre del acuerdo o indicador de nivel de servicio.
- **SLO:** valor porcentual que representa el nivel de cumplimiento esperado (por ejemplo, 99.5 % de disponibilidad).
- **Effective date:** fecha a partir de la cual el SLA entra en vigencia.
- **Reporting period:** periodo de evaluación, que puede ser diario, semanal o mensual.
- **Timezone:** zona horaria en la que se mide el cumplimiento del servicio.
- **Schedule:** muestra la programación asociada al acuerdo.
- **SLA report:** permite generar un informe detallado del cumplimiento del nivel de servicio.
- **Status:** indica si el SLA se encuentra activo o deshabilitado.

En la imagen presentada, no se muestran datos configurados, lo cual significa que aún no se ha creado ningún SLA en el sistema. Una vez establecidos, estos acuerdos permiten monitorear el rendimiento de los servicios clave, evaluar su estabilidad y garantizar que se cumplan los estándares de disponibilidad definidos por la institución.

La funcionalidad SLA en Zabbix es especialmente útil para instituciones educativas y departamentos de TI, ya que facilita el seguimiento del desempeño de la red, la planificación de mantenimientos y la mejora continua de los servicios tecnológicos.

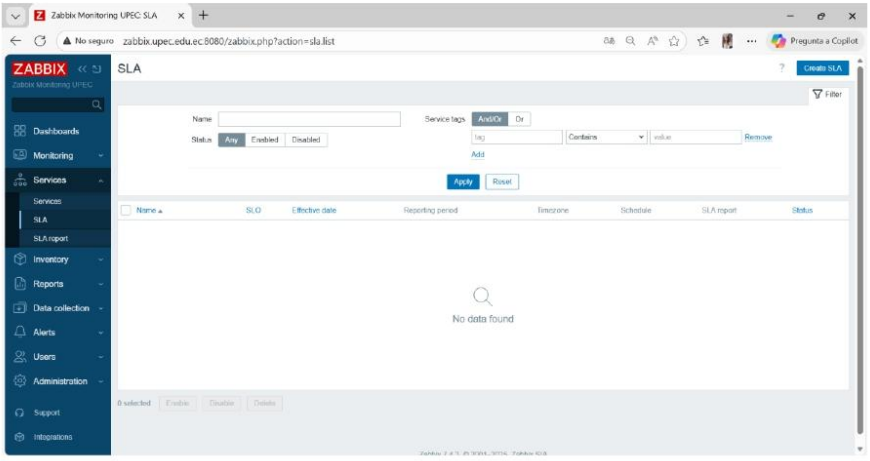


Figura 13. Vista del apartado SLA dentro del módulo Services de Zabbix Monitoring UPEC, donde se definen y gestionan los Acuerdos de Nivel de Servicio mediante la dirección http://zabbix.upec.edu.ec:8080.

4.3 SLA Report

El apartado SLA Report dentro del módulo Services de Zabbix permite generar informes detallados sobre el cumplimiento de los Acuerdos de Nivel de Servicio (SLA) definidos previamente en el sistema. Esta herramienta facilita el análisis de la calidad del servicio brindado, mostrando de manera clara si los objetivos establecidos se están cumpliendo dentro de los plazos y condiciones pactadas.

En la parte superior de la interfaz se encuentra la barra de filtros y parámetros de consulta, conformada por los siguientes elementos:

- **SLA:** permite seleccionar el acuerdo de nivel de servicio del cual se desea generar el informe.
- **Service:** posibilita elegir el servicio específico asociado al SLA, con el fin de obtener resultados precisos y segmentados.
- **From / To:** establecen el rango de fechas para el cual se desea visualizar la información del cumplimiento, utilizando el formato YYYY-MM-DD.
- **Apply:** ejecuta la búsqueda y genera el reporte según los parámetros definidos.
- **Reset:** elimina los filtros y restablece la vista inicial para realizar una nueva consulta.

Una vez aplicados los filtros, el sistema genera una tabla o gráfico que muestra los niveles de disponibilidad alcanzados, los tiempos de inactividad y el porcentaje de cumplimiento con respecto al objetivo establecido (SLO). En la parte inferior de la interfaz también puede visualizarse un mensaje indicativo cuando aún no existen datos registrados, como el que aparece en la imagen: “Select SLA to display SLA report.”

Esta función resulta fundamental para la evaluación del rendimiento institucional, ya que proporciona información cuantitativa sobre la calidad del servicio, permitiendo identificar desviaciones, planificar mejoras y garantizar el cumplimiento de los estándares acordados con los usuarios o departamentos internos.

En el contexto de la Universidad Politécnica Estatal del Carchi (UPEC), el uso de SLA Reports facilita a los administradores de red supervisar el desempeño de los servicios tecnológicos —como plataformas educativas, correo institucional o acceso a internet— y asegurar que funcionen de acuerdo con los niveles esperados de disponibilidad y estabilidad.

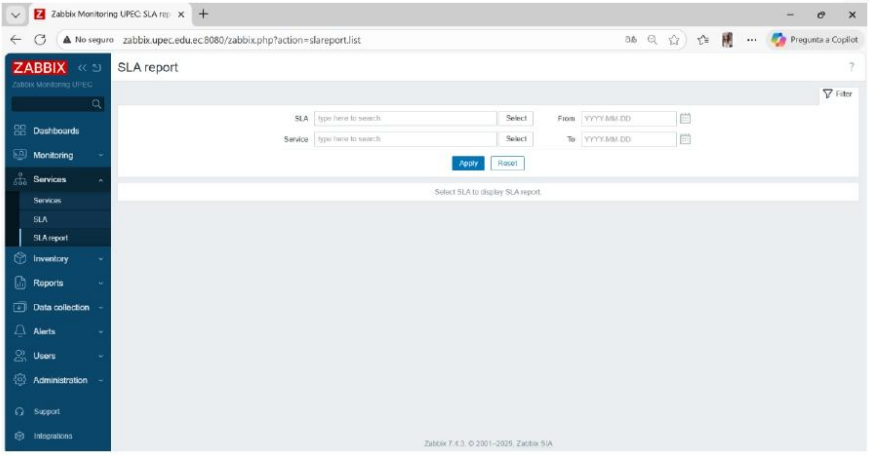


Figura 14. Vista del apartado SLA Report dentro del módulo Services de Zabbix Monitoring UPEC, donde se generan reportes de cumplimiento de los Acuerdos de Nivel de Servicio mediante la dirección http://zabbix.upec.edu.ec:8080.

5. Inventory

El módulo Inventory de Zabbix permite gestionar y registrar información detallada sobre los dispositivos o equipos (hosts) que forman parte de la infraestructura de red. Esta función ayuda a mantener un control ordenado y actualizado del inventario tecnológico de la institución, facilitando la identificación de equipos, su ubicación física, responsable, estado operativo y otros datos relevantes.

El uso del inventario es esencial en entornos institucionales, ya que permite una trazabilidad precisa de cada dispositivo monitoreado, lo que mejora la gestión de activos y agiliza la resolución de incidentes.

5.1 Overview

La opción Overview dentro del módulo *Inventory* muestra una visión general del inventario de hosts registrados en el sistema. Su objetivo principal es ofrecer al administrador un resumen rápido de los equipos activos, agrupados según diferentes criterios de clasificación.

En la parte superior de la interfaz se encuentran los principales filtros de búsqueda:

- **Host groups:** permite seleccionar el grupo de hosts o equipos que se desea visualizar. Esto es útil cuando los dispositivos están organizados por áreas o departamentos (por ejemplo: *Red Académica*, *Administración*, *Docencia*).

- **Grouping by:** ofrece la posibilidad de agrupar los resultados por categorías específicas, como tipo de dispositivo, ubicación o responsable.
- **Apply:** ejecuta la búsqueda y muestra los resultados del inventario según los filtros seleccionados.
- **Reset:** limpia los campos y restablece la vista original para realizar una nueva consulta.

En la parte inferior se visualiza una tabla con dos columnas principales:

- **Field:** indica el campo o categoría del inventario (como modelo, dirección IP o ubicación).
- **Host count:** muestra la cantidad de equipos que pertenecen a esa categoría.

En la imagen, el sistema presenta el mensaje "No data found", lo que indica que aún no se ha agregado ningún host al inventario o que no existen datos disponibles para los filtros seleccionados.

Cuando el inventario está activo y configurado, esta sección permite obtener una visión global de la infraestructura tecnológica, facilitando el control de los dispositivos monitoreados y su organización dentro del entorno institucional.

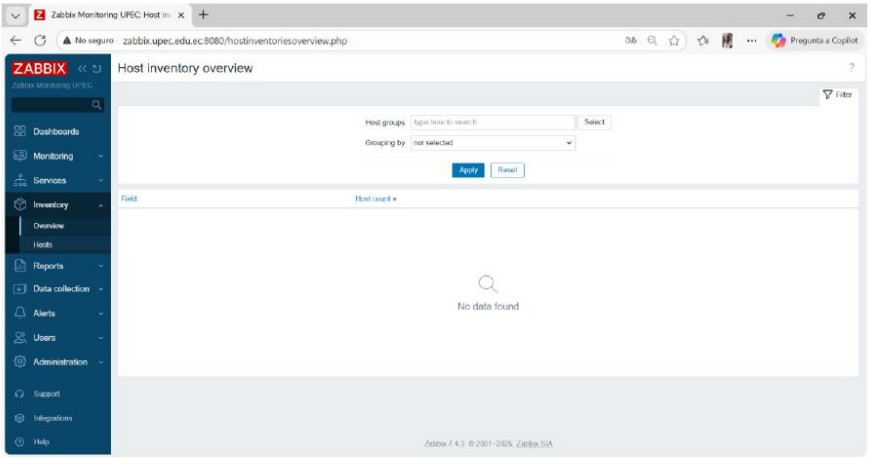


Figura 15. Vista general del apartado Overview dentro del módulo Inventory de Zabbix Monitoring UPEC, donde se muestran los equipos registrados y agrupados en el inventario mediante la dirección http://zabbix.upec.edu.ec:8080.

5.2 Hosts

El apartado Hosts dentro del módulo Inventory tiene como función mostrar el inventario detallado de los equipos que están siendo monitoreados por Zabbix. Desde esta vista, los

administradores pueden consultar información técnica y organizativa de cada dispositivo, facilitando la gestión del hardware y software dentro de la red institucional.

En la parte superior del panel se encuentran los filtros de búsqueda, que permiten personalizar la visualización de los equipos según distintos criterios:

- **Host groups:** selecciona los grupos de dispositivos que se desean visualizar. En este caso, se muestran los grupos UPEC NETWORK y Zabbix servers, que agrupan los equipos asociados al entorno de monitoreo de la Universidad Politécnica Estatal del Carchi (UPEC).
- **Field:** permite filtrar la búsqueda por campos específicos del inventario, como nombre, alias, dirección MAC o sistema operativo.
- **Apply:** ejecuta la búsqueda de los equipos según los parámetros seleccionados.
- **Reset:** elimina los filtros aplicados y devuelve la vista general del inventario.

En la parte inferior, se presenta la tabla principal del inventario, la cual resume la información técnica de los hosts registrados. Cada columna tiene un propósito específico:

- **Host:** muestra el nombre del dispositivo monitoreado, en este caso Zabbix server.
- **Group:** indica el grupo al que pertenece el equipo dentro del sistema de monitoreo (Zabbix servers).
- **Name:** representa el nombre asignado dentro del inventario (por ejemplo, zabbix).
- **Type:** especifica el tipo de host o dispositivo.
- **OS (Operating System):** muestra el sistema operativo instalado en el equipo. En la imagen, se detalla un sistema operativo **Linux versión 6.1.0-39-amd64**, con información técnica adicional sobre su kernel y compilador.
- **Serial number**, **Tag** y **MAC address:** aunque no están completadas en la vista actual, estas columnas permiten registrar información adicional como número de serie, etiquetas internas o direcciones físicas de red.

La interfaz refleja un registro activo correspondiente al servidor principal de Zabbix, lo que indica que el sistema está correctamente inventariado y operativo dentro de la red institucional.

Esta sección es de gran utilidad para el personal del área de Tecnologías de la Información y Comunicación (TIC), ya que permite mantener un inventario actualizado, preciso y automatizado, evitando la pérdida de información y garantizando un control efectivo sobre los recursos tecnológicos.

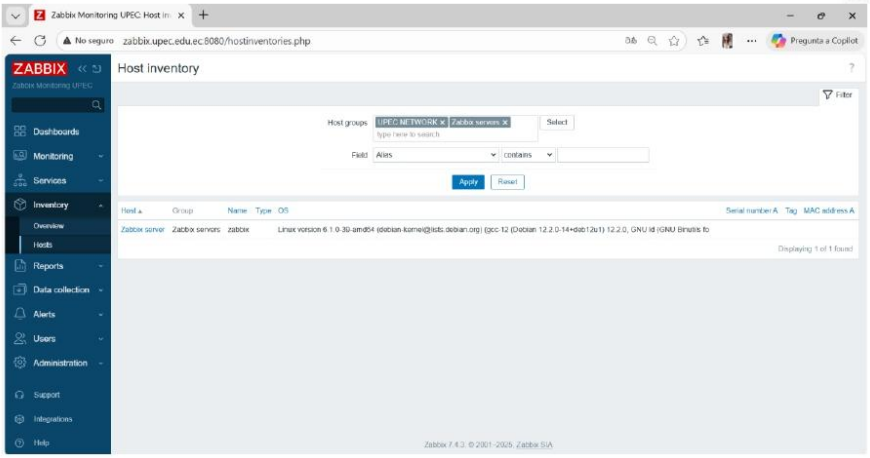


Figura 16. Vista del apartado Hosts dentro del módulo Inventory de Zabbix Monitoring UPEC, donde se detalla la información técnica de los equipos registrados en el inventario mediante la dirección http://zabbix.upec.edu.ec:8080.

6. Reports

El módulo Reports en Zabbix permite consultar, analizar y presentar información sobre el estado y rendimiento del sistema de monitoreo. A través de sus diferentes secciones, el administrador puede acceder a datos históricos, informes programados y registros de auditoría, lo que facilita la toma de decisiones basadas en evidencias.

Este módulo resulta fundamental para mantener un seguimiento técnico y administrativo del funcionamiento de la red, permitiendo evaluar el comportamiento de los dispositivos, los eventos generados y la eficiencia del servidor de monitoreo.

6.1 System Information

La opción System Information dentro del módulo *Reports* muestra un resumen general del estado actual del servidor Zabbix y de los recursos que administra. Esta vista es de gran utilidad para verificar si el sistema se encuentra operativo, cuántos equipos están siendo monitoreados y si existen actualizaciones pendientes.

La información se presenta en formato de tabla, organizada en tres columnas:

- **Parameter:** identifica los elementos o características que están siendo supervisados.
- **Value:** muestra el valor o estado actual de cada parámetro.

- **Details:** ofrece información complementaria o enlaces directos a las configuraciones correspondientes.

Entre los parámetros más importantes que se observan en la imagen, se destacan:

- **Zabbix server is running:** indica si el servidor de monitoreo está activo (Yes confirma su correcto funcionamiento).
- **Zabbix server version / frontend version:** muestran la versión instalada del servidor y la interfaz web. En este caso, ambas versiones son **7.4.3**, con la notificación de una nueva actualización disponible.
- **Software update last checked:** señala la última fecha en que se verificaron actualizaciones del sistema, en este caso el **9 de noviembre de 2025**.
- **Latest release:** muestra la versión más reciente disponible de Zabbix (7.4.5) junto con el enlace a las notas de la versión.
- **Number of hosts:** indica la cantidad total de equipos monitoreados, diferenciando entre habilitados (2) y deshabilitados (0).
- **Number of templates:** presenta el número total de plantillas disponibles para asociar a los hosts (352).
- **Number of items:** contabiliza los ítems de monitoreo activos, deshabilitados o no soportados, reflejando la amplitud del monitoreo.
- **Number of triggers:** muestra las condiciones configuradas para generar alertas automáticas, separadas por estado (habilitadas, deshabilitadas o en problema).
- **Number of users:** indica cuántos usuarios se encuentran actualmente conectados al sistema.
- **Required server performance:** refleja la capacidad del servidor para procesar nuevos valores por segundo (50.37 en este caso).
- **High availability cluster:** señala si la función de alta disponibilidad está habilitada; en esta configuración, se encuentra *Disabled*.

Esta vista permite al administrador obtener una instantánea del estado operativo del sistema de monitoreo, asegurando que todos los componentes funcionen correctamente y que el rendimiento sea óptimo.

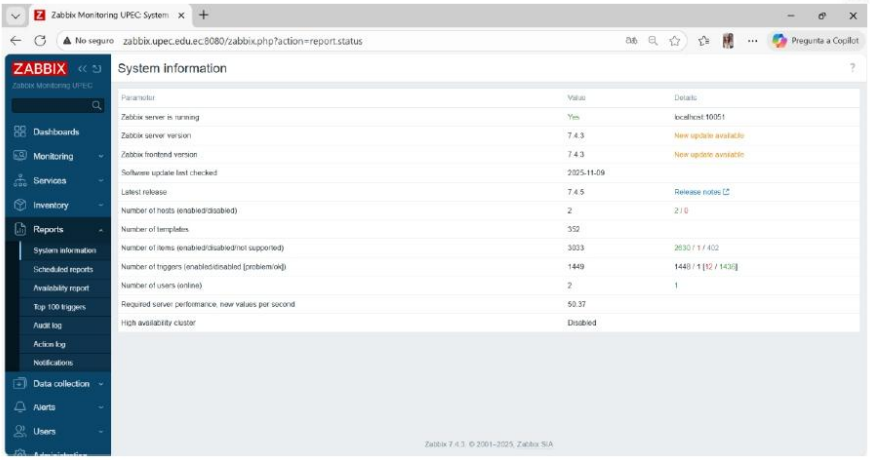


Figura 17. Vista del apartado *System Information* dentro del módulo *Reports* de Zabbix Monitoring UPEC, donde se presenta el estado general del servidor, las versiones activas y los recursos monitoreados mediante la dirección *http://zabbix.upec.edu.ec:8080*.

6.2 Scheduled Reports

La sección Scheduled Reports dentro del módulo Reports de Zabbix permite programar y automatizar la generación de informes del sistema, garantizando que la información sobre el estado de la red, los equipos o los servicios sea enviada de manera periódica y sin intervención manual. Esta funcionalidad es ideal para mantener una comunicación constante con el equipo técnico o con los responsables de infraestructura, asegurando la disponibilidad de datos actualizados.

En la parte superior de la interfaz se encuentran los filtros de búsqueda y control que permiten gestionar los informes ya creados:

- **Name:** permite buscar un informe programado por su nombre.
- **Show:** ofrece dos opciones de visualización:
    - All, para mostrar todos los informes registrados.
    - Created by me, para visualizar únicamente aquellos creados por el usuario actual.
- **Status:** filtra los reportes según su estado operativo, pudiendo elegir entre Any (todos), Enabled (activos), Disabled (deshabilitados) o Expired (caducados).
- **Apply:** ejecuta la búsqueda o actualización de la lista según los filtros seleccionados.
- **Reset:** borra los criterios de búsqueda y restablece la vista por defecto.

En el extremo derecho de la pantalla, el botón "Create report" permite crear un nuevo informe programado. Al hacerlo, el usuario puede definir los siguientes parámetros:

- El **tipo de informe** (por ejemplo, disponibilidad del sistema, rendimiento de equipos o alertas recientes).
- La **frecuencia de envío** (diaria, semanal o mensual).
- El **destinatario**, que puede ser un usuario o grupo dentro del sistema.
- El **formato de entrega**, que usualmente se envía como documento PDF al correo configurado.

En la parte inferior de la interfaz se encuentra la tabla principal, que muestra los informes configurados con las siguientes columnas:

- **Name:** nombre asignado al informe.
- **Owner:** usuario que lo creó.
- **Repeats:** frecuencia con la que el informe es generado.
- **Period:** rango de tiempo que abarca el informe.
- **Last sent:** fecha y hora del último envío.
- **Status:** estado actual del informe (activo, inactivo o caducado).
- **Info:** muestra detalles adicionales sobre su configuración.

En la imagen, la tabla se encuentra vacía con el mensaje "No data found", lo que indica que aún no se han creado reportes automáticos. Una vez configurados, esta sección se convierte en una herramienta fundamental para el seguimiento continuo del desempeño de la red y los servicios sin requerir generación manual de informes.

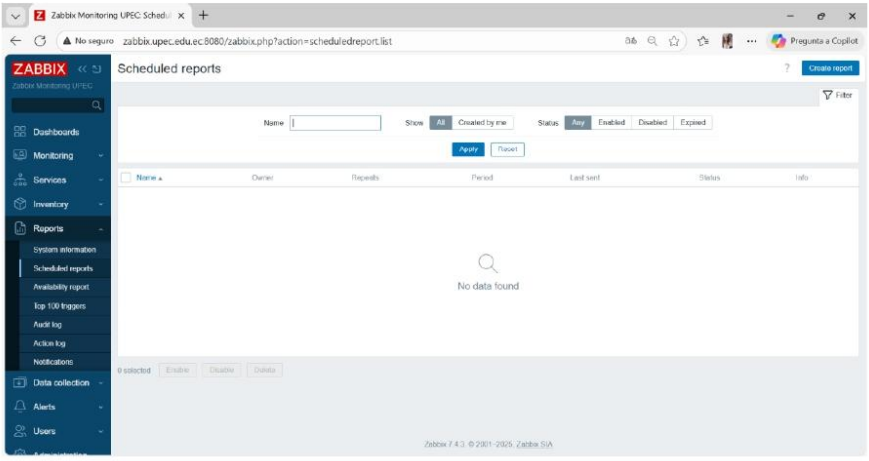


Figura 18. Vista del apartado Scheduled Reports dentro del módulo Reports de Zabbix Monitoring UPEC, donde se gestionan los informes programados y su estado mediante la dirección http://zabbix.upec.edu.ec:8080.

6.3 Availability Report

El apartado Availability Report del módulo Reports permite analizar la disponibilidad y el rendimiento de los equipos o servicios monitoreados dentro de la red institucional. Esta herramienta ofrece un registro visual del tiempo en que los dispositivos han permanecido operativos, detectando posibles interrupciones o fallos en su funcionamiento.

La interfaz está diseñada para proporcionar una vista rápida y detallada del nivel de disponibilidad de los hosts y sus componentes críticos.

En la parte superior del panel se encuentran los principales controles de filtrado:

- **From / To:** permiten establecer el rango de fechas o periodo de tiempo que se desea analizar. En este caso, se visualiza el intervalo comprendido entre **"now-1h" y "now"**, es decir, la última hora.
- **Apply:** ejecuta la búsqueda y actualiza el reporte de acuerdo con el periodo definido.
- A la derecha, se presentan accesos rápidos con rangos de tiempo predefinidos (últimos 5 minutos, 2 días, 1 semana, 1 mes, etc.), lo que facilita la comparación temporal del desempeño de la red.

En la parte superior derecha, también se incluye la opción Mode (By host), que permite elegir el modo de visualización, ya sea por host o por trigger (evento de alerta).

Debajo del panel de control, la tabla principal presenta los resultados obtenidos. Cada columna cumple una función específica:

- **Host:** muestra el nombre del equipo o dispositivo monitoreado (por ejemplo, Switch de Core).
- **Name:** detalla el evento o parámetro supervisado, como la utilización de CPU o la temperatura del dispositivo.
- **Problems:** indica si el sistema ha detectado fallos durante el periodo seleccionado.
- **Ok:** presenta el porcentaje de tiempo en el que el equipo ha permanecido operativo, representando su disponibilidad. En este caso, todos los equipos reportan un **100.0000 % de disponibilidad**, lo que refleja un funcionamiento estable y continuo.
- **Graph:** ofrece un enlace directo para visualizar el gráfico correspondiente al comportamiento del parámetro analizado.

En la imagen se observan diferentes métricas del dispositivo Switch de Core, entre ellas el uso de CPU y la temperatura de entrada y salida del aire. Estas variables son fundamentales para evaluar el estado térmico y la carga de trabajo del equipo, garantizando que opere dentro de los parámetros normales.

Gracias a este apartado, el administrador puede monitorear el tiempo de actividad (uptime) de cada dispositivo y anticiparse a posibles fallas, asegurando la continuidad del servicio en la red institucional.

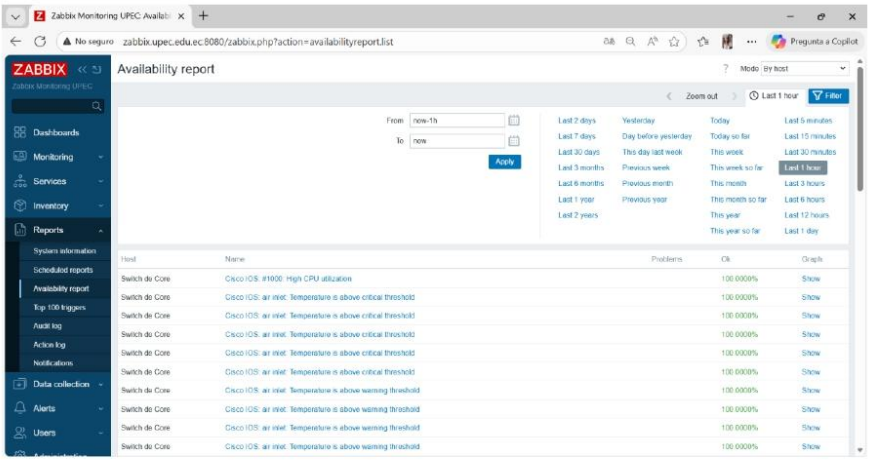


Figura 19. Vista del apartado Availability Report dentro del módulo Reports de Zabbix Monitoring UPEC, donde se muestran los porcentajes de disponibilidad de los equipos y parámetros monitoreados mediante la dirección http://zabbix.upec.edu.ec:8080.

6.4 Top 100 Triggers

El apartado Top 100 Triggers dentro del módulo Reports permite visualizar de manera rápida y jerarquizada los 100 eventos o alertas más relevantes generados por el sistema de monitoreo, según su nivel de severidad o recurrencia. Esta función es especialmente útil para identificar los equipos o servicios que presentan más incidencias dentro de la red, lo que ayuda a priorizar las acciones correctivas.

En la parte superior de la interfaz se encuentran los filtros de tiempo que permiten delimitar el rango de análisis:

- **From / To:** determinan el intervalo de tiempo de consulta; en este caso, se muestra el rango entre **"now-1h"** y **"now"**, correspondiente a la última hora.
- **Apply:** actualiza los resultados de acuerdo con el periodo definido.

- En la parte derecha se despliegan accesos rápidos a intervalos predefinidos como los últimos 5 minutos, 1 día, 1 semana, 1 mes o incluso 2 años, facilitando el análisis histórico.

Debajo del panel de filtros, se presenta una tabla con cuatro columnas principales:

- **Host:** muestra el nombre del equipo o dispositivo afectado.
- **Trigger:** indica la descripción del evento que originó la alerta o notificación, señalando el parámetro o condición que superó un umbral definido.
- **Severity:** clasifica el nivel de criticidad del evento, que puede ir desde Information hasta Disaster, dependiendo de su impacto en el sistema.
- **Number of problems:** especifica la cantidad de incidencias detectadas dentro del periodo seleccionado.

En la imagen se observa que el equipo Switch de Core presenta un evento con severidad "Warning", correspondiente al trigger "Cisco IOS: Interface Gi6/46 (INSIDE ASA): High bandwidth usage". Esto indica que una de las interfaces del switch ha registrado un uso elevado del ancho de banda, superando el umbral configurado por el administrador, aunque sin llegar a un nivel crítico.

Gracias a esta vista, el administrador puede detectar tendencias de saturación, sobreuso o errores recurrentes en los dispositivos monitoreados, lo que permite implementar acciones preventivas antes de que se produzcan interrupciones del servicio. Además, al concentrar los eventos más importantes en una sola lista, se optimiza la supervisión y se prioriza la atención de las alertas con mayor impacto en la red.

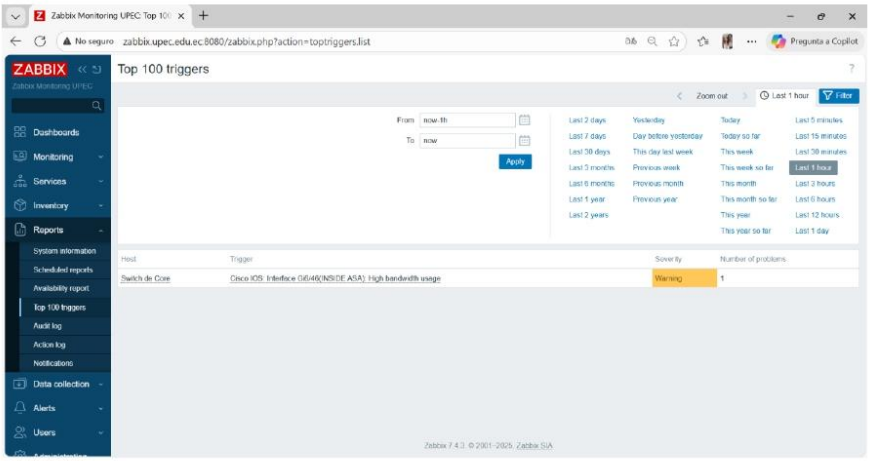


Figura 20. Vista del apartado Top 100 Triggers dentro del módulo Reports de Zabbix Monitoring UPEC, donde se observan los principales eventos generados por los dispositivos monitoreados en un intervalo de tiempo definido mediante la dirección http://zabbix.upec.edu.ec:8080.

6.5 Audit Log

El apartado Audit Log dentro del módulo Reports de Zabbix cumple una función esencial en la trazabilidad y control de las acciones realizadas dentro del sistema de monitoreo. Su objetivo es registrar cada cambio o actividad ejecutada por los usuarios, proporcionando una evidencia detallada de quién realizó una acción, cuándo y sobre qué elemento.

Este registro es de gran importancia en la gestión de redes institucionales, ya que permite mantener la integridad, transparencia y seguridad de la plataforma, asegurando que todas las configuraciones o modificaciones puedan ser auditadas en cualquier momento.

En la parte superior del panel se encuentran los filtros que permiten ajustar el intervalo de tiempo que se desea analizar:

- **From / To:** definen el rango temporal de los registros a visualizar; en este caso, se muestra el intervalo **"now-1h" a "now"**, correspondiente a la última hora.
- **Apply:** actualiza los datos mostrados de acuerdo con el rango seleccionado.
- En la parte derecha, se presentan accesos rápidos con intervalos predefinidos como Last 5 minutes, Last 7 days o Last 2 years, lo que facilita el análisis tanto en tiempo real como histórico.

La tabla inferior, una vez que se registran actividades en el sistema, muestra las siguientes columnas:

- **Time:** indica la fecha y hora exacta en que ocurrió la acción.
- **User:** identifica al usuario que ejecutó la operación.
- **IP:** muestra la dirección IP desde la cual se realizó el acceso o modificación.
- **Resource:** especifica el recurso afectado (por ejemplo, un host, plantilla o parámetro).
- **ID:** representa el identificador único del elemento modificado.
- **Action:** describe la operación efectuada, como la creación, edición o eliminación de un objeto.
- **Recordset ID:** detalla el registro o grupo de registros involucrados en la acción.
- **Details:** ofrece información complementaria sobre la operación, como los valores antes y después del cambio.

En la imagen presentada, la tabla muestra el mensaje "No data found", lo que indica que no se han realizado modificaciones o eventos dentro del periodo seleccionado. No obstante, cuando el sistema está en funcionamiento activo, esta vista se convierte en un recurso clave para supervisar el comportamiento de los usuarios y validar la correcta administración del entorno Zabbix.

El Audit Log es especialmente útil para los administradores responsables de mantener la estabilidad de la red, ya que permite detectar actividades no autorizadas, errores de configuración o acciones que puedan afectar el rendimiento general del sistema.

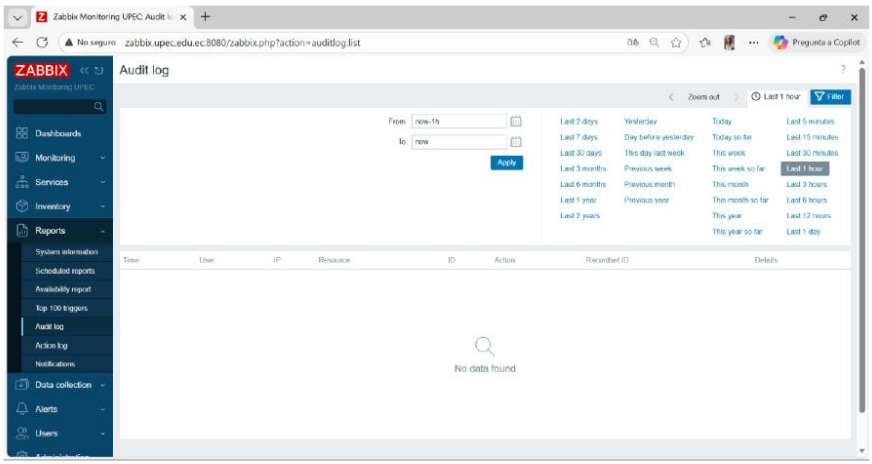


Figura 21. Vista del apartado Audit Log dentro del módulo Reports de Zabbix Monitoring UPEC, donde se registran las acciones ejecutadas por los usuarios y los cambios aplicados en la configuración, mediante la dirección http://zabbix.upec.edu.ec:8080.

6.6 Action Log

El apartado Action Log dentro del módulo Reports de Zabbix tiene como finalidad registrar y mostrar de manera detallada todas las acciones automáticas ejecutadas por el sistema en respuesta a eventos o condiciones previamente configuradas. En otras palabras, este módulo permite verificar qué acciones ha tomado Zabbix frente a un determinado evento de monitoreo, como el envío de notificaciones, la ejecución de scripts o la activación de alertas.

Este registro es esencial para auditar el comportamiento del sistema de alertas, asegurando que las políticas de notificación y respuesta ante incidentes funcionen correctamente.

En la parte superior de la interfaz se encuentran los controles de filtrado de tiempo:

- **From / To:** determinan el rango de fechas que se desea analizar; en este caso, se muestra el intervalo comprendido entre **"now-1h" y "now"**, correspondiente a la última hora.
- **Apply:** actualiza los datos visualizados según el rango seleccionado.

- A la derecha, los accesos rápidos permiten elegir periodos predefinidos como Last 5 minutes, Last 7 days o Last 2 years, facilitando la búsqueda y comparación de registros históricos.
- Además, en la parte superior derecha se encuentra la opción **Export to CSV**, que permite descargar los resultados en formato de hoja de cálculo para un análisis o respaldo posterior.

La tabla inferior muestra los detalles de cada acción registrada en el sistema, con las siguientes columnas:

- **Time:** indica la fecha y hora en que se ejecutó la acción.
- **Action:** especifica el nombre o tipo de acción ejecutada (por ejemplo, envío de correo, alerta SMS, ejecución remota, etc.).
- **Media type:** define el medio de comunicación empleado (correo electrónico, webhook, script, etc.).
- **Recipient:** muestra el usuario o grupo destinatario de la notificación.
- **Message:** contiene el texto o contenido del mensaje enviado.
- **Status:** refleja el resultado de la acción, mostrando si fue **exitosa (OK)** o si ocurrió algún **error** durante la ejecución.
- **Info:** ofrece detalles adicionales relacionados con el envío o el procesamiento de la acción.

En la imagen presentada, la tabla muestra el mensaje "No data found", lo que significa que, durante el periodo seleccionado, el sistema no ha ejecutado acciones automáticas. No obstante, en un entorno de monitoreo activo, este apartado se llena automáticamente con cada evento y su respuesta asociada, permitiendo verificar que las alertas se envían correctamente y que los mecanismos de respuesta funcionan conforme a la configuración definida.

El Action Log resulta especialmente valioso para los administradores, ya que proporciona una trazabilidad completa de las respuestas automáticas del sistema, contribuyendo a la mejora continua del proceso de monitoreo y gestión de incidentes dentro de la red institucional.

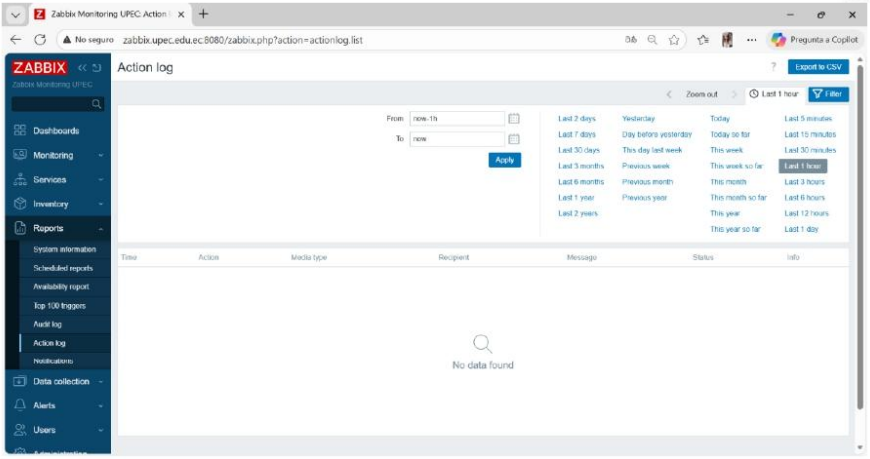


Figura 22. Vista del apartado Action Log dentro del módulo Reports de Zabbix Monitoring UPEC, donde se registran las acciones automáticas ejecutadas por el sistema ante eventos generados en la red, mediante la dirección http://zabbix.upec.edu.ec:8080.

6.7 Notifications

El apartado Notifications dentro del módulo Reports de Zabbix permite visualizar un resumen consolidado de las notificaciones emitidas por el sistema a los usuarios registrados, de acuerdo con los eventos ocurridos dentro de la infraestructura monitoreada. Esta sección facilita el seguimiento del flujo de alertas, permitiendo comprobar si los mensajes fueron enviados correctamente y hacia qué destinatarios, garantizando así la efectividad de la comunicación dentro del sistema de monitoreo.

En la parte superior de la interfaz se encuentran los filtros principales, que permiten personalizar la visualización de los datos:

- **Media type:** selecciona el tipo de medio empleado para el envío de las notificaciones (por ejemplo, correo electrónico, webhook, SMS o script).
- **Period:** define el intervalo de tiempo en el cual se agruparán los reportes. En este caso, se muestra el valor **"Weekly"**, lo que significa que las notificaciones se presentan de forma semanal.
- **Year:** permite seleccionar el año de referencia de los registros, aquí mostrado como **2025**, abarcando un periodo completo de revisión de alertas dentro del sistema.

La tabla principal muestra dos columnas temporales (From y Till) que indican el rango de fechas correspondientes a cada semana analizada. A la derecha, se incluyen los

usuarios involucrados en el sistema de monitoreo, como Admin (Zabbix Administrator) y guest, quienes pueden haber recibido notificaciones durante los periodos registrados.

Cada fila representa una semana del año, iniciando desde el 30 de diciembre de 2024 hasta el 7 de abril de 2025, lo que permite observar de manera cronológica la generación y distribución de notificaciones automáticas por parte del sistema.

Este apartado resulta especialmente útil para los administradores, ya que permite auditar la frecuencia y consistencia del envío de alertas, así como detectar posibles fallos en la entrega de mensajes. De este modo, se garantiza que los usuarios responsables sean informados oportunamente ante cualquier anomalía detectada en la red o en los equipos monitoreados.

El módulo Notifications complementa el funcionamiento del Action Log, ya que mientras este último detalla las acciones individuales realizadas, las notificaciones ofrecen una visión global y temporal del comportamiento del sistema de alertas dentro de Zabbix, contribuyendo así a la eficiencia y trazabilidad del monitoreo institucional.

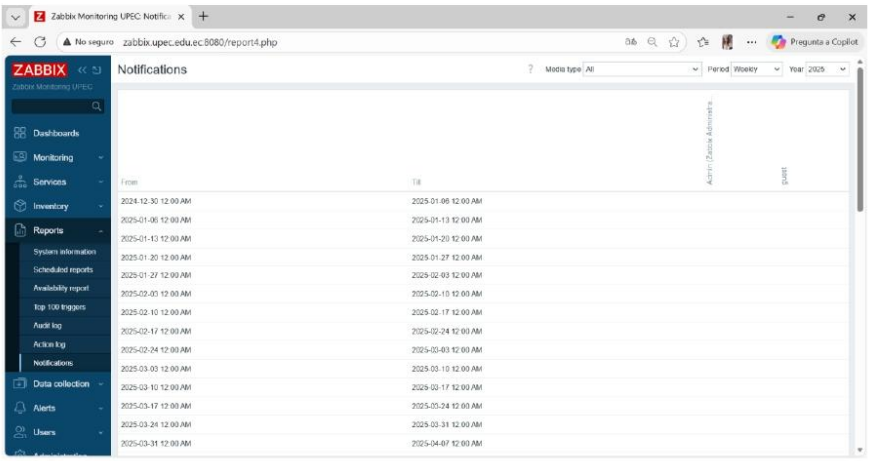


Figura 23. Vista del apartado Notifications dentro del módulo Reports de Zabbix Monitoring UPEC, donde se muestran las notificaciones enviadas semanalmente a los usuarios del sistema mediante la dirección http://zabbix.upec.edu.ec:8080.

7. Módulo Data Collection

El módulo Data Collection de Zabbix es el encargado de recolectar y gestionar toda la información proveniente de los dispositivos monitoreados dentro de la red. A través de este módulo, el sistema obtiene datos en tiempo real sobre el rendimiento, disponibilidad y estado de los equipos o servicios, permitiendo una supervisión continua y precisa.

Además, organiza los elementos de monitoreo mediante plantillas, grupos y reglas automáticas, facilitando la administración de grandes infraestructuras como la de la Universidad Politécnica Estatal del Carchi (UPEC).

7.1 Template Groups

El apartado Template Groups dentro del módulo Data Collection de Zabbix tiene como objetivo principal organizar las plantillas de monitoreo en grupos temáticos, lo que permite una administración más eficiente y estructurada de los diferentes tipos de dispositivos, servicios o aplicaciones que forman parte de la red institucional.

Las plantillas (o templates) son conjuntos predefinidos de elementos que incluyen ítems, gráficos, disparadores y macros, los cuales permiten automatizar la configuración del monitoreo para diferentes sistemas sin necesidad de crear parámetros manualmente. Gracias a los grupos de plantillas, los administradores pueden clasificar los objetos de monitoreo según su tipo o función, facilitando la búsqueda, el mantenimiento y la escalabilidad del sistema.

En la parte superior de la interfaz se encuentra la barra de filtrado que permite buscar un grupo específico ingresando su nombre en el campo Name, acompañado de los botones:

- **Apply:** ejecuta el filtro para mostrar los resultados coincidentes.
- **Reset:** limpia los filtros y restaura la vista general.

En la sección central se listan los principales grupos de plantillas disponibles, junto con el número de plantillas incluidas dentro de cada uno. Entre los más relevantes se encuentran:

- **Templates/Applications:** contiene 99 plantillas destinadas al monitoreo de aplicaciones, servidores web, entornos de desarrollo y sistemas distribuidos. Incluye, por ejemplo, plantillas para **Apache, Docker, Kubernetes, GitLab, VMware** y **HTTP**, entre otros.
- **Templates/Cloud:** agrupa 42 plantillas orientadas a la supervisión de servicios en la nube como **AWS, Azure y Google Cloud**, permitiendo controlar el rendimiento de instancias, bases de datos o balanceadores de carga.
- **Templates/Databases:** con 27 plantillas, abarca sistemas de gestión de bases de datos como **MySQL, PostgreSQL, Oracle y MSSQL**, ofreciendo métricas detalladas sobre disponibilidad, consultas y rendimiento general.

Estos grupos reflejan la gran capacidad de Zabbix para adaptarse a diferentes entornos tecnológicos, desde infraestructuras locales hasta plataformas híbridas o en la nube. Además, el botón Create template group, ubicado en la esquina superior derecha, permite crear nuevos grupos personalizados según las necesidades del administrador, manteniendo la coherencia y el orden en el monitoreo de red.

En resumen, el apartado Template Groups constituye la base de la reutilización y estandarización del monitoreo en Zabbix, asegurando que los parámetros de observación sean consistentes, escalables y fácilmente replicables entre diferentes dispositivos o servicios.

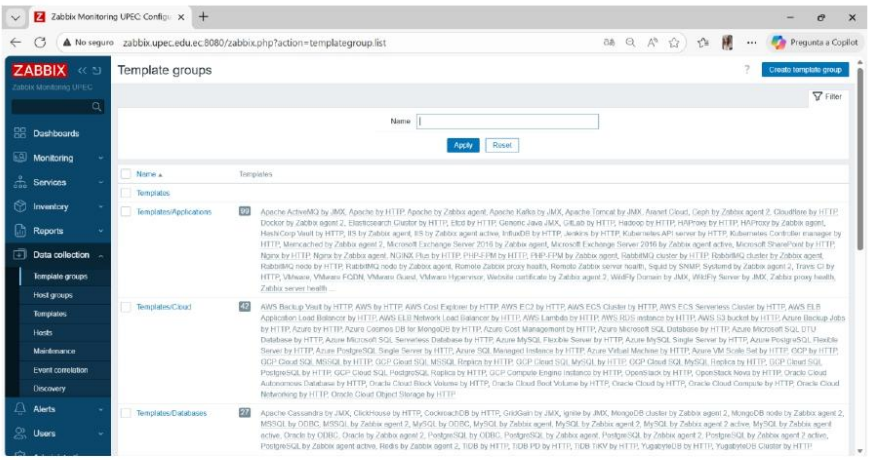


Figura 24. Vista del apartado Template Groups dentro del módulo Data Collection de Zabbix Monitoring UPEC, donde se agrupan las plantillas de monitoreo según su tipo o función, mediante la dirección http://zabbix.upec.edu.ec:8080.

7.2 Host Groups

El apartado Host Groups dentro del módulo Data Collection permite organizar los equipos o dispositivos monitoreados (hosts) en grupos lógicos, facilitando su administración y supervisión dentro del entorno de Zabbix.
Esta función es esencial para instituciones como la Universidad Politécnica Estatal del Carchi (UPEC), donde se manejan múltiples dispositivos de red y servidores distribuidos en distintas áreas o departamentos.

En la parte superior de la interfaz se encuentra una barra de búsqueda que permite filtrar los grupos existentes escribiendo el nombre en el campo Name. Los botones Apply y Reset sirven, respectivamente, para aplicar el filtro o restablecer la vista general. En la esquina superior derecha, el botón Create host group ofrece la posibilidad de crear nuevos grupos personalizados, según las necesidades del administrador de red.

En la sección central se muestra una lista con los grupos configurados dentro del sistema, donde cada uno agrupa a uno o varios hosts asociados. Entre los grupos visibles destacan:

- **Applications:** para equipos o servicios dedicados a la ejecución de aplicaciones específicas.
- **Databases:** orientado al monitoreo de bases de datos institucionales.

- **Discovered hosts:** agrupa los dispositivos detectados automáticamente por las reglas de descubrimiento de Zabbix.
- **Hypervisors y Virtual machines:** permiten monitorear entornos virtualizados.
- **Linux servers:** agrupa servidores que operan bajo sistemas GNU/Linux.
- **UPEC NETWORK:** contiene los dispositivos principales de la red universitaria, como el Switch de Core, encargado de la conectividad troncal.
- **Zabbix servers:** agrupa los servidores que ejecutan el propio sistema de monitoreo, como el Zabbix server localizado en la dirección 127.0.0.1.

Esta organización estructurada permite segmentar los dispositivos según su función o ubicación, mejorando la visibilidad del estado de la infraestructura y simplificando la aplicación de políticas de monitoreo o mantenimiento. Además, contribuye a una gestión jerárquica más ordenada, donde cada grupo puede tener asignadas plantillas y alertas específicas según las necesidades operativas.

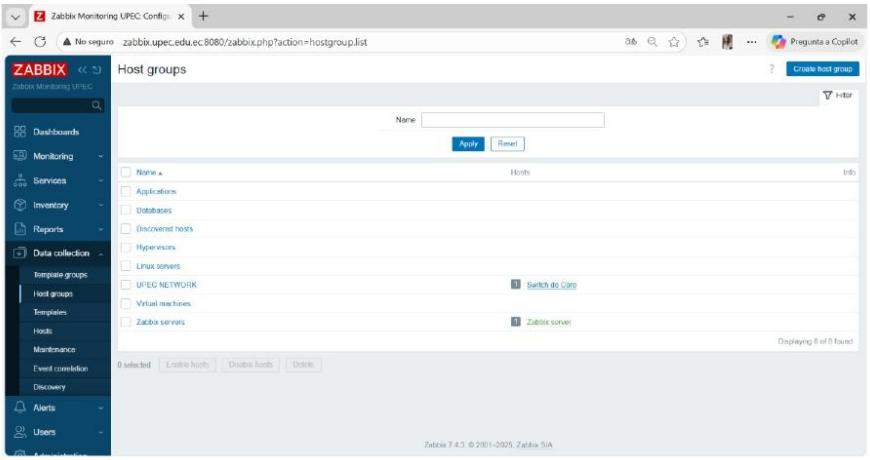


Figura 25. Vista del apartado Host Groups en el módulo Data Collection de Zabbix Monitoring UPEC, donde se muestran los grupos de equipos organizados por función y categoría, accesible mediante la dirección http://zabbix.upec.edu.ec:8080.

7.3 Templates

El apartado Templates dentro del módulo Data Collection permite gestionar las plantillas de monitoreo que Zabbix utiliza para estandarizar la recolección de datos de múltiples dispositivos o servicios.
Una plantilla define de manera centralizada los ítems, gráficas, triggers (disparadores), dashboards y reglas de descubrimiento que se aplicarán automáticamente a los hosts

asociados, evitando configuraciones manuales repetitivas y asegurando una supervisión uniforme en toda la red.

En la parte superior de la interfaz se encuentran los campos de filtrado, que permiten **buscar plantillas específicas** según distintos criterios:

- **Template groups:** para seleccionar el grupo de plantillas al que pertenece.
- **Linked templates:** muestra las plantillas asociadas entre sí.
- **Name, Vendor y Version:** facilitan la localización precisa de una plantilla según su nombre, fabricante o versión.
  También se dispone de las opciones **Apply** y **Reset** para aplicar o limpiar los filtros.

En la parte superior derecha, los botones Create template e Import permiten, respectivamente, crear una nueva plantilla personalizada o importar una existente desde otro sistema o repositorio de Zabbix.

La lista principal muestra las plantillas disponibles dentro del servidor de monitoreo, junto con detalles relevantes como:

- **Hosts e Items:** indican la cantidad de dispositivos y métricas vinculadas.
- **Triggers y Graphs:** muestran los eventos configurados y las gráficas asociadas.
- **Dashboards y Discovery:** facilitan la visualización de datos y detección automática de componentes.
- **Vendor y Version:** identifican el origen y versión de la plantilla.
- **Tags:** describen el propósito o la tecnología asociada (por ejemplo, class: software, target: apache, subclass: webserver).

En la figura se observan varias plantillas predeterminadas del sistema, como Apache by HTTP, Acronis Cyber Protect Cloud by HTTP o Alcatel Timetra TiMOS by SNMP, las cuales permiten supervisar aplicaciones, servidores web o dispositivos de red específicos.

Estas plantillas son esenciales para la automatización del monitoreo, ya que garantizan que todos los hosts asociados utilicen los mismos parámetros, asegurando consistencia en la recolección de métricas y reducción de errores humanos.
En el caso de la UPEC, estas configuraciones optimizan el monitoreo de la infraestructura institucional, integrando servicios web, bases de datos y equipos de red dentro de un entorno estandarizado y centralizado.

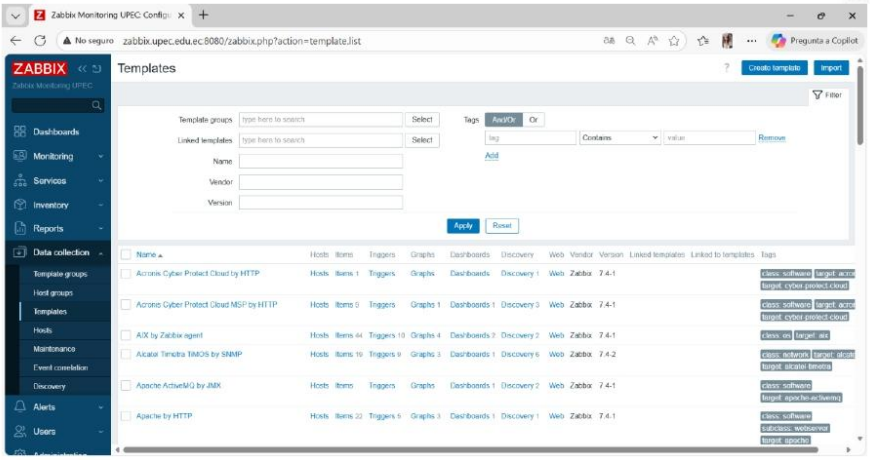


Figura 26. Vista del apartado Templates del módulo Data Collection en Zabbix Monitoring UPEC, donde se gestionan las plantillas utilizadas para la recolección automática de datos y monitoreo estandarizado.

7.4 Hosts

El apartado Hosts dentro del módulo Data Collection representa el núcleo del monitoreo en Zabbix, ya que en esta sección se configuran y administran los dispositivos, servidores o equipos de red que serán observados de manera continua. Cada host corresponde a un elemento físico o virtual dentro de la infraestructura tecnológica de la Universidad Politécnica Estatal del Carchi (UPEC), y su correcta configuración garantiza la recolección de datos en tiempo real sobre el estado y desempeño de la red.

En la parte superior del panel se encuentran los filtros de búsqueda que permiten localizar un host específico mediante distintos parámetros como:

- **Host groups:** grupo al que pertenece el equipo monitoreado.
- **Templates:** plantilla de monitoreo asociada.
- **Name, DNS, IP y Port:** identificadores básicos para búsqueda directa.
- **Status:** permite seleccionar hosts habilitados (Enabled), deshabilitados (Disabled) o todos (Any).
- **Monitored by:** define si el host es controlado directamente por el servidor o por un proxy.

Además, se incluye una sección de etiquetas (Tags) que facilita el filtrado de hosts mediante metadatos o condiciones personalizadas. Los botones Apply y Reset permiten aplicar los filtros o restablecer la vista general.

En la parte superior derecha destacan tres funciones importantes:

- **Host Wizard:** asistente de configuración rápida.
- **Create host:** permite agregar un nuevo dispositivo a la plataforma.
- **Import:** posibilita cargar hosts previamente configurados desde un archivo externo.

En la vista principal se observa el listado de equipos actualmente monitoreados. En este caso, se encuentran configurados los siguientes:

- **Switch de Core:** con dirección IP **172.20.1.1:161**, monitoreado mediante el protocolo **SNMP**, utilizando la plantilla Cisco IOS by SNMP. Este dispositivo corresponde al núcleo de la red institucional de la UPEC, responsable del enrutamiento principal del tráfico.
- **Zabbix server:** con dirección **127.0.0.1:10050**, supervisado mediante el **Zabbix Agent**, encargado de recopilar información sobre el rendimiento y estado del propio servidor de monitoreo.

Ambos hosts se encuentran con el estado Enabled, lo que indica que el sistema está recibiendo métricas activas. En las columnas adicionales se detallan las cantidades de Items, Triggers, Graphs y Discoveries, que representan los elementos asociados a cada host para medir variables, generar alertas, visualizar gráficas y detectar componentes automáticamente.

Este apartado es esencial para la gestión del monitoreo, ya que permite añadir, editar o eliminar hosts, vincularlos con las plantillas adecuadas y verificar su disponibilidad mediante los protocolos SNMP, Zabbix Agent o ICMP. De esta forma, el administrador TIC puede mantener una visión global del funcionamiento de la red institucional y responder oportunamente ante cualquier eventualidad.

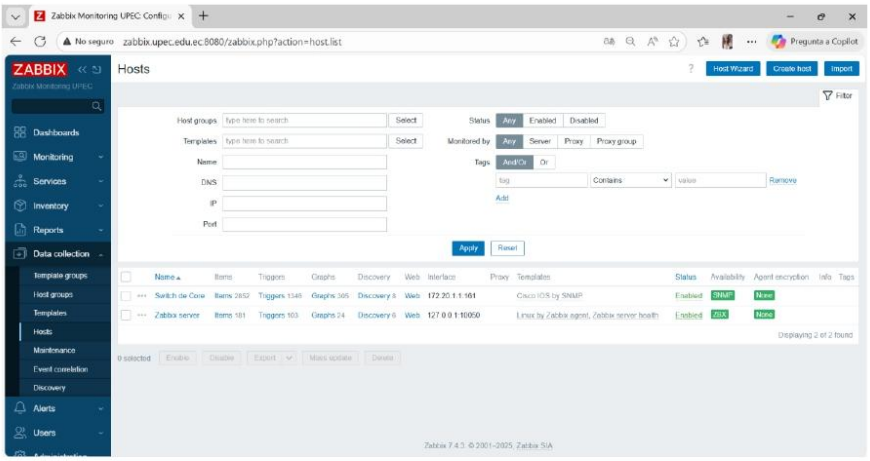


Figura 27. Vista del apartado Hosts del módulo Data Collection en Zabbix Monitoring UPEC, donde se visualizan los dispositivos monitoreados como el Switch de Core y el Zabbix server, con sus respectivos parámetros de configuración y estado operativo.

7.5 Maintenance

El apartado Maintenance dentro del módulo Data Collection permite definir y gestionar los periodos de mantenimiento en los que determinados hosts o grupos de equipos quedan temporalmente excluidos del monitoreo activo. Esta función es esencial para evitar falsas alarmas o alertas innecesarias durante tareas planificadas de actualización, configuración o pruebas dentro de la red institucional.

En la parte superior de la interfaz se encuentra el panel de búsqueda y filtrado, que facilita la localización de periodos de mantenimiento ya creados. Los campos disponibles permiten realizar búsquedas por:

- **Host groups:** agrupa los dispositivos afectados por el mantenimiento.
- **Name:** identifica el nombre asignado al periodo.
- **State:** permite filtrar por estado, pudiendo elegir entre Active (activo), Approaching (próximo), Expired (finalizado) o Any (todos los estados).

Los botones Apply y Reset permiten aplicar los filtros establecidos o restaurar la vista general del panel.

En la esquina superior derecha se ubica el botón Create maintenance period, mediante el cual el administrador puede crear un nuevo periodo de mantenimiento especificando su duración, descripción, tipo de mantenimiento y los equipos implicados.

La tabla central presenta una lista de los periodos existentes, con columnas que indican el nombre del mantenimiento, su tipo, el rango de tiempo activo (Active since / Active till), su estado actual y una descripción adicional. En este caso, aún no se han definido periodos, por lo que el sistema muestra el mensaje No data found.

Esta funcionalidad es de gran utilidad en entornos como el de la Universidad Politécnica Estatal del Carchi (UPEC), ya que permite realizar labores técnicas —como la actualización de firmware en routers o la instalación de parches de seguridad en servidores— sin que se generen alertas que podrían confundir al personal de monitoreo. Además, su uso contribuye a mantener la precisión de los reportes y estadísticas, diferenciando claramente entre incidentes reales y mantenimientos programados.

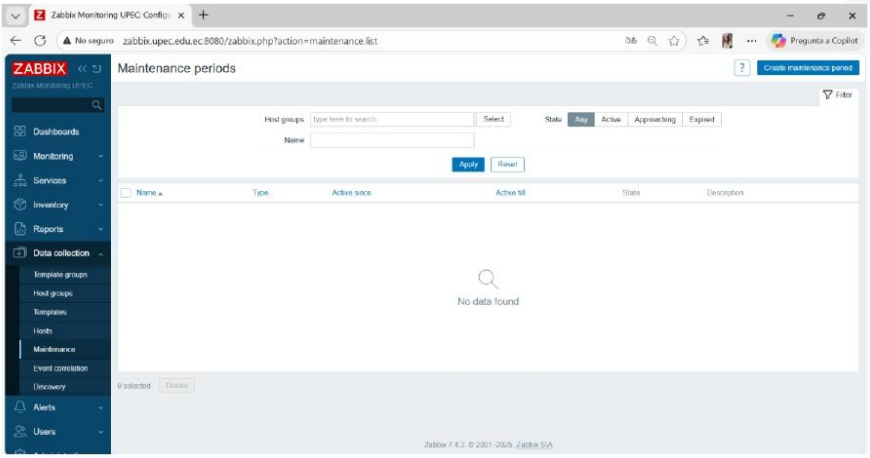


Figura 28. Vista del apartado Maintenance del módulo Data Collection en Zabbix Monitoring UPEC, donde se gestionan los periodos de mantenimiento de los equipos para evitar alertas durante intervenciones planificadas.

7.6 Event Correlation

El apartado Event Correlation dentro del módulo Data Collection permite configurar reglas de correlación de eventos, una funcionalidad avanzada que ayuda a reducir el ruido de alertas y mejorar la eficiencia en la gestión de incidencias dentro del sistema de monitoreo.

En entornos complejos como el de la Universidad Politécnica Estatal del Carchi (UPEC), es común que un único fallo en la red genere múltiples alertas simultáneas provenientes de distintos dispositivos o servicios relacionados. La correlación de eventos permite agrupar, suprimir o relacionar estas alertas, mostrando solo la información realmente relevante para los administradores de red.

En la parte superior del panel se dispone de herramientas de búsqueda que facilitan la gestión de las reglas creadas.
Los campos más relevantes son:

- **Name:** permite buscar una correlación específica por su nombre.
- **Status:** filtra las reglas activas (Enabled), inactivas (Disabled) o todas (Any). Los botones **Apply** y **Reset** permiten aplicar los filtros o limpiar los criterios de búsqueda.

En la esquina superior derecha se encuentra el botón Create event correlation, que permite crear nuevas reglas de correlación definiendo condiciones y operaciones específicas. Cada regla puede configurarse para que Zabbix detecte relaciones entre eventos, como

dependencias, repeticiones o cierres automáticos, evitando alertas duplicadas o innecesarias.

La tabla inferior, que actualmente muestra el mensaje No data found, está destinada a listar las correlaciones activas en el sistema, junto con detalles como:

- **Name:** nombre asignado a la regla.
- **Conditions:** criterios definidos para correlacionar eventos.
- **Operations:** acciones automáticas que se ejecutan una vez que las condiciones se cumplen (por ejemplo, cerrar eventos duplicados o ignorar alertas secundarias).
- **Status:** estado actual de la correlación.

Gracias a esta funcionalidad, Zabbix logra optimizar la detección y el tratamiento de incidencias, priorizando los eventos críticos y reduciendo la sobrecarga de información que podría afectar la respuesta del equipo técnico.
En el contexto institucional, esto permite que el personal TIC de la UPEC se concentre en los problemas reales de conectividad o rendimiento, manteniendo una red universitaria más estable y eficiente.

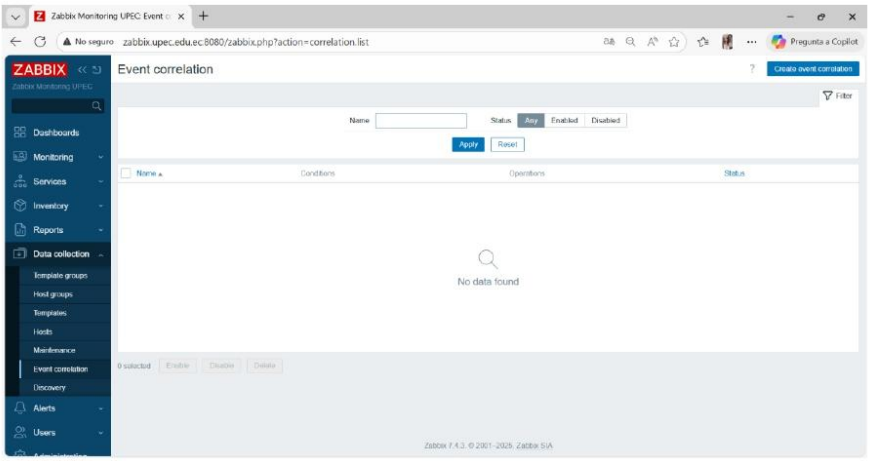


Figura 29. Vista del apartado Event Correlation del módulo Data Collection en Zabbix Monitoring UPEC, donde se configuran las reglas de correlación que optimizan la gestión de eventos y reducen alertas innecesarias.

7.7 Discovery

El apartado Discovery del módulo Data Collection permite a Zabbix realizar la detección automática de dispositivos en la red, facilitando la incorporación de nuevos equipos al

sistema de monitoreo sin necesidad de añadirlos manualmente. Esta funcionalidad resulta especialmente útil en entornos como la Universidad Politécnica Estatal del Carchi (UPEC), donde la red institucional está conformada por una amplia variedad de dispositivos —como switches, routers, servidores y puntos de acceso— que requieren una vigilancia constante para mantener la calidad del servicio.

En la parte superior del panel se encuentran los campos de búsqueda que permiten filtrar las reglas de descubrimiento existentes mediante los parámetros:

- **Name:** nombre asignado a la regla.
- **Status:** filtra entre reglas habilitadas (Enabled), deshabilitadas (Disabled) o todas (Any).

El botón Apply ejecuta los filtros configurados, mientras que Reset restablece la vista inicial.

En la esquina superior derecha se dispone del botón Create discovery rule, que permite crear nuevas reglas de descubrimiento. Estas reglas definen los rangos de direcciones IP que serán escaneadas, el método de comprobación que se empleará (por ejemplo, Zabbix Agent, ICMP Ping o SNMP), el intervalo de tiempo entre cada exploración y las acciones que deben ejecutarse cuando se detecta un nuevo dispositivo.

En la tabla principal se muestra la lista de reglas activas. En este caso, se observa la regla denominada Local network, que realiza un escaneo dentro del rango de direcciones 192.168.0.1–254, con un intervalo de 1 hora y utilizando el método de comprobación Zabbix Agent.
El estado de esta regla se encuentra actualmente en Disabled, lo que indica que el descubrimiento está desactivado temporalmente, pero puede habilitarse en cualquier momento según las necesidades del administrador de red.

Mediante esta herramienta, el sistema Zabbix puede detectar automáticamente nuevos hosts, servidores o dispositivos de red conectados, asignándoles plantillas predefinidas y comenzando su monitoreo de manera inmediata.
Esto optimiza significativamente el proceso de administración de la red y contribuye a mantener un inventario actualizado de los equipos, reduciendo errores humanos y tiempos de configuración manual.

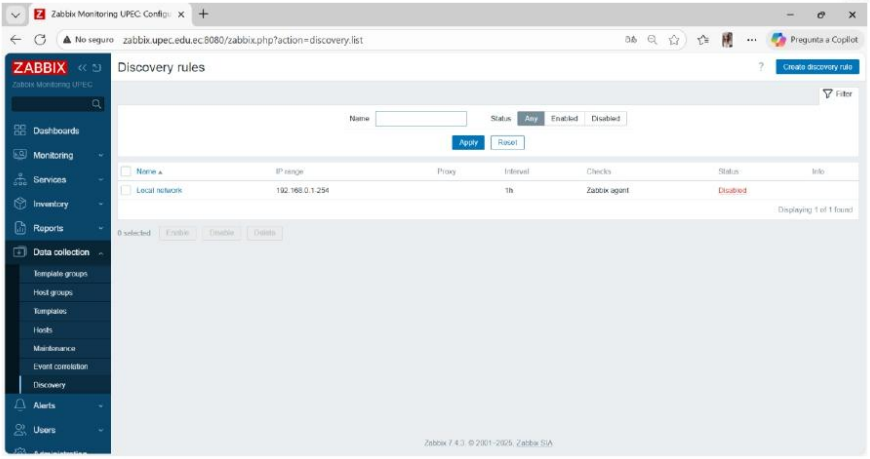


Figura 30. Vista del apartado Discovery del módulo Data Collection en Zabbix Monitoring UPEC, donde se muestra la regla de descubrimiento Local network configurada para detectar equipos dentro del rango IP 192.168.0.1–254 mediante el método Zabbix Agent.

8. Módulo Alerts

El módulo Alerts de Zabbix cumple una función esencial dentro del sistema de monitoreo, ya que permite gestionar las notificaciones y respuestas automáticas ante eventos detectados en la red.
Su objetivo principal es garantizar que los administradores sean informados oportunamente de cualquier incidencia, anomalía o cambio relevante dentro de la infraestructura monitoreada.

Gracias a este módulo, Zabbix no solo detecta problemas, sino que también ejecuta acciones automatizadas como el envío de correos electrónicos, mensajes instantáneos, o la ejecución de scripts específicos que contribuyen a una respuesta rápida ante fallos. Esto lo convierte en una herramienta indispensable para mantener la continuidad operativa y la calidad del servicio (QoS) en entornos complejos como el de la Universidad Politécnica Estatal del Carchi (UPEC).

El módulo Alerts está compuesto principalmente por tres secciones:

- **Actions:** donde se configuran las reglas que definen cómo y cuándo deben generarse las alertas.
- **Media types:** que gestiona los medios de comunicación utilizados (correo electrónico, SMS, webhook, etc.).

- **Scripts:** que permite ejecutar tareas automatizadas personalizadas ante determinados eventos.

8.1 Actions

El apartado Actions es el núcleo operativo del sistema de alertas en Zabbix. Aquí se definen reglas automatizadas que determinan qué debe suceder cuando ocurre un evento específico en la red.
Cada acción puede incluir condiciones (para definir cuándo se activa), operaciones (qué hacer cuando se activa) y destinatarios (quién recibe la notificación).

En el panel izquierdo, dentro de Actions, se encuentran varias categorías especializadas según el tipo de evento que se desea gestionar. A continuación se describen los subapartados principales:

8.1.1 Trigger Actions

El subapartado Trigger Actions permite crear acciones que se ejecutan automáticamente cuando se activa un trigger o disparador dentro del sistema.
Los triggers son condiciones definidas previamente en los hosts o plantillas, que se activan al detectar valores fuera de rango o fallas de conectividad.

Por ejemplo, si el uso de CPU de un servidor sobrepasa el 90 %, Zabbix puede generar un evento y enviar una alerta al equipo técnico.
Desde esta sección se configuran los parámetros de notificación (quién recibe el aviso, a través de qué medio y con qué mensaje), así como acciones correctivas, como la ejecución de un script para reiniciar un servicio automáticamente.

Esta capacidad permite que el monitoreo sea proactivo y automatizado, reduciendo tiempos de respuesta y mejorando la estabilidad de la red universitaria.

8.1.2 Service Actions

El subapartado Service Actions está orientado a la gestión de alertas relacionadas con servicios definidos en el módulo Services de Zabbix.
Permite crear acciones que se ejecutan cuando un servicio —por ejemplo, el correo institucional, Moodle o un servidor web— cambia de estado (de “OK” a “Problem” o viceversa).

En esta sección, los administradores pueden definir qué notificaciones deben enviarse, a qué grupos de usuarios, y qué medios deben utilizarse.
Esto garantiza una comunicación clara y oportuna ante cualquier problema que afecte a los servicios esenciales de la institución.

8.1.3 Discovery Actions

El subapartado Discovery Actions gestiona las acciones automáticas que se ejecutan cuando Zabbix descubre nuevos dispositivos dentro de la red mediante las reglas configuradas en el módulo Data Collection.

Por ejemplo, si se detecta un nuevo switch dentro del rango IP definido, el sistema puede añadirlo automáticamente al monitoreo, asignarle una plantilla y enviar una notificación al administrador de red.

Esta automatización permite mantener actualizado el inventario de equipos sin intervención manual, reduciendo la carga operativa y asegurando una cobertura total del monitoreo institucional.

8.1.4 Autoregistration Actions

La sección Autoregistration Actions está destinada a definir reglas para la autoregistración de agentes Zabbix.
Cuando un agente se instala en un nuevo dispositivo y se comunica con el servidor, puede registrarse automáticamente y comenzar a enviar datos de monitoreo sin requerir configuración manual.

Estas acciones son ideales en entornos con múltiples estaciones o servidores distribuidos, como los laboratorios o aulas de la UPEC, donde los equipos se integran de manera automática al sistema central.

Las reglas de autoregistro permiten, además, asignar plantillas, grupos de hosts y etiquetas específicas, asegurando una configuración coherente y estandarizada.

8.1.5 Internal Actions

Finalmente, el subapartado Internal Actions gestiona las acciones internas del sistema Zabbix, es decir, aquellas que se ejecutan ante eventos del propio software de monitoreo y no necesariamente por fallos en la red.

En la interfaz se muestran tres acciones predeterminadas:

- **Report not supported items:** informa cuando un ítem deja de ser soportado.
- **Report not supported low level discovery rules:** alerta sobre errores en las reglas de descubrimiento de bajo nivel.
- **Report unknown triggers:** notifica cuando un trigger cambia a un estado “unknown”.

Estas acciones están orientadas a mantener la integridad del sistema de monitoreo, garantizando que las métricas y procesos internos funcionen correctamente. En este caso, todas las acciones se encuentran deshabilitadas (Disabled), pero pueden activarse o personalizarse según las políticas de administración de la red.

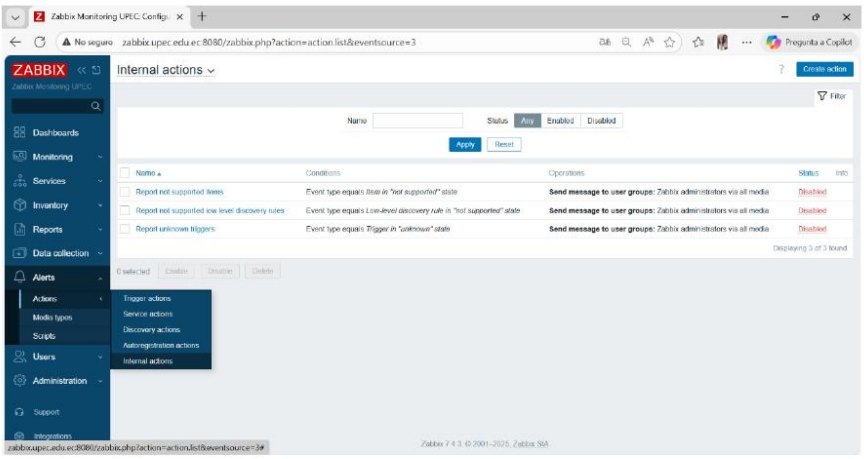


Figura 31. Vista del apartado Internal Actions del módulo Alerts en Zabbix Monitoring UPEC, donde se configuran las acciones internas que permiten mantener el correcto funcionamiento del sistema y la notificación de errores del propio monitoreo.

8.2 Media Types

El apartado Media Types dentro del módulo Alerts de Zabbix define los canales de comunicación que el sistema utiliza para enviar notificaciones automáticas ante eventos o incidencias detectadas.
A través de este componente, los administradores pueden determinar cómo se entregarán las alertas, ya sea por correo electrónico, mensajería instantánea, webhooks o integraciones con plataformas externas.

Esta funcionalidad es fundamental para garantizar una respuesta oportuna ante fallos en la red o servicios, permitiendo que el personal técnico de la Universidad Politécnica Estatal del Carchi (UPEC) reciba notificaciones inmediatas en los medios que utilice habitualmente, sin necesidad de estar revisando constantemente la interfaz de Zabbix.

En la parte superior del panel, se encuentran los campos de búsqueda y filtros principales:

- **Name:** permite localizar un tipo de medio específico.
- **Status:** filtra entre medios habilitados (Enabled), deshabilitados (Disabled) o todos (Any).

- **Display actions:** posibilita mostrar solo los medios disponibles o aquellos asignados a acciones específicas.

Los botones Apply y Reset sirven para aplicar los filtros o restaurar la vista inicial respectivamente.

En la esquina superior derecha, el botón Create media type permite crear nuevos medios de comunicación, configurando parámetros técnicos como el tipo (por ejemplo, Email, Webhook, SMS, Script, etc.), los servidores de salida, credenciales o tokens de autenticación, y los mensajes de prueba antes de su implementación.

En la tabla principal se listan los diferentes medios disponibles en el sistema. Entre los tipos visibles se encuentran Email, Webhook y sus respectivas integraciones con plataformas externas, como Discord, GitHub, Gmail o GLPI. Cada uno incluye la siguiente información:

- **Name:** nombre asignado al tipo de medio.
- **Type:** protocolo o canal utilizado (por ejemplo, Email o Webhook).
- **Status:** indica si el medio está activo o no.
- **Used in actions:** muestra las acciones en las que el medio está configurado.
- **Details:** ofrece información técnica relevante (por ejemplo, el servidor SMTP o la URL del webhook).

En la captura se puede observar que la mayoría de los medios, incluyendo Email, Discord, GitHub y Gmail, se encuentran en estado Disabled, lo que significa que aún no están habilitados para el envío de notificaciones. Sin embargo, estos pueden activarse fácilmente según las políticas internas del área de redes o los canales preferidos de comunicación institucional.

La posibilidad de integrar múltiples medios convierte a Zabbix en una herramienta altamente flexible y adaptable. En el contexto de la UPEC, esto facilita la coordinación inmediata entre los técnicos responsables de infraestructura, reduciendo los tiempos de reacción y contribuyendo al mantenimiento de la calidad del servicio (QoS) en la red universitaria.

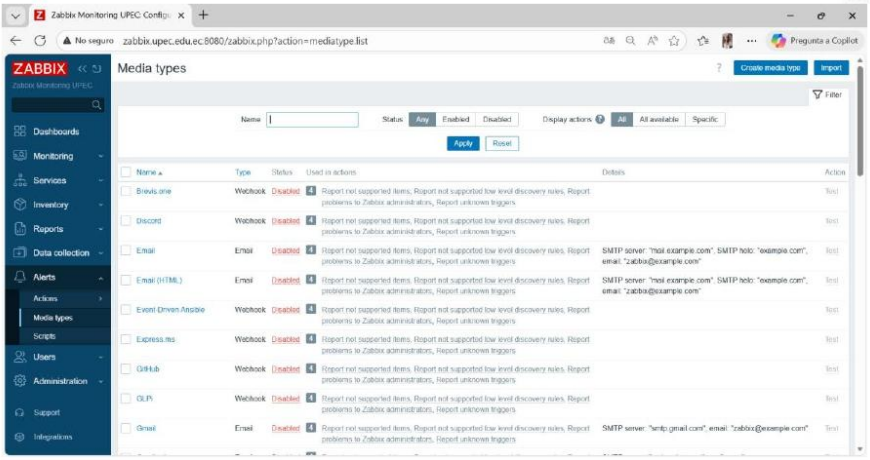


Figura 32. Vista del apartado Media Types del módulo Alerts en Zabbix Monitoring UPEC, donde se configuran los canales de comunicación (correo electrónico, webhooks, entre otros) utilizados para el envío automatizado de notificaciones ante incidencias detectadas.

8.3 Scripts

El apartado Scripts dentro del módulo Alerts permite configurar comandos o acciones automáticas que el sistema ejecuta en respuesta a eventos específicos o de forma manual sobre los hosts.
Esta característica dota a Zabbix de una gran capacidad de automatización, ya que facilita la ejecución directa de scripts en el servidor o en los proxies, sin necesidad de ingresar manualmente a cada dispositivo.

En el contexto de la Universidad Politécnica Estatal del Carchi (UPEC), esta funcionalidad resulta de suma utilidad para tareas de diagnóstico rápido, mantenimiento remoto o pruebas de conectividad entre los distintos equipos de la red institucional.

En la parte superior del panel se presentan los principales filtros de búsqueda:

- **Name:** permite localizar un script específico.
- **Scope:** determina el alcance del script, pudiendo ser una Action operation, una Manual host action o una Manual event action.
- Los botones **Apply** y **Reset** sirven para aplicar los filtros o restablecer la vista por defecto.

En la esquina superior derecha, el botón Create script posibilita crear nuevos scripts personalizados. Durante su creación, el administrador puede definir el comando que se

ejecutará, el tipo de entorno (Server, Proxy, o Agent), los permisos de ejecución, el grupo de usuarios autorizado y el tipo de acción (manual o automatizada).

En la tabla principal del panel se listan los scripts preconfigurados, que incluyen:

- **Detect operating system:** ejecuta un comando nmap sobre la dirección IP del host para identificar el sistema operativo del dispositivo.
- **Ping:** realiza una prueba de conectividad mediante el comando ping hacia el host, verificando la disponibilidad del dispositivo.
- **Traceroute:** efectúa un rastreo de la ruta de red (traceroute) hasta el host, útil para diagnosticar problemas de latencia o saltos intermedios en la comunicación.

Cada uno de estos scripts se clasifica como una Manual host action, lo que significa que pueden ser ejecutados de forma manual desde la interfaz de Zabbix por un usuario autorizado.
En la columna Execute on, se observa que todos se ejecutan desde el Server (proxy), garantizando que las operaciones se realicen de manera centralizada desde el servidor principal de monitoreo.

Asimismo, en la columna Commands se muestran los comandos exactos que utiliza cada script. Por ejemplo:

- Para Ping: ping -c 3 {HOST.CONN}
- Para Traceroute: /usr/bin/traceroute {HOST.CONN}
- Para Detect operating system: sudo /usr/bin/nmap -O {HOST.CONN}

El uso de variables como {HOST.CONN} permite que los comandos sean dinámicos y se apliquen al host seleccionado, haciendo que las pruebas sean adaptables y escalables.

Gracias a esta capacidad, los administradores de la UPEC pueden realizar acciones rápidas de diagnóstico o recuperación, sin necesidad de salir del entorno de Zabbix, optimizando la eficiencia operativa y reduciendo significativamente los tiempos de respuesta ante incidentes de red.

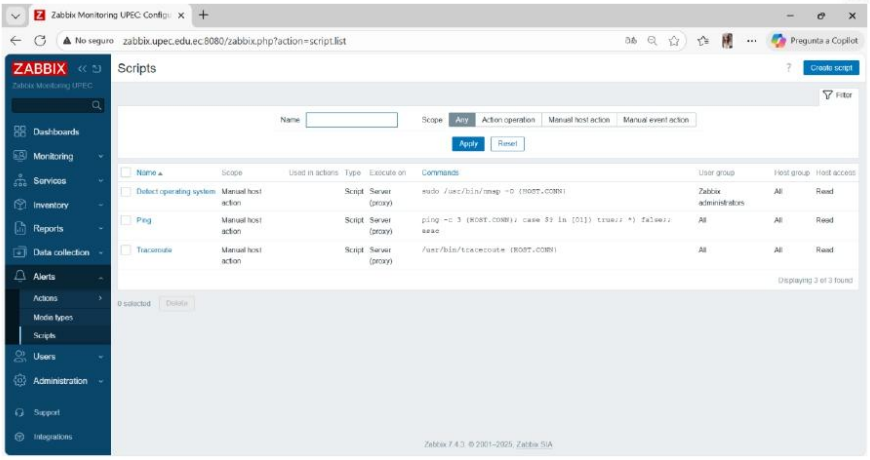


Figura 33. Vista del apartado Scripts del módulo Alerts en Zabbix Monitoring UPEC, donde se muestran los scripts disponibles para ejecución manual o automática, utilizados para pruebas de conectividad, detección de sistemas operativos y trazado de rutas de red.

9. Módulo Users

El módulo Users de Zabbix permite administrar de forma integral los usuarios, roles y permisos del sistema de monitoreo. Gracias a esta función, es posible establecer niveles de acceso diferenciados para cada integrante del equipo técnico o grupo de trabajo, garantizando la seguridad y la trazabilidad de las acciones realizadas dentro del entorno de monitoreo.

En el contexto de la Universidad Politécnica Estatal del Carchi (UPEC), este módulo resulta fundamental para mantener un control adecuado sobre quién puede visualizar, modificar o administrar los diferentes elementos del sistema, como hosts, dashboards, alertas o configuraciones de red.

9.1 User Groups

El subapartado User Groups agrupa a los usuarios según su nivel de responsabilidad, función o área de trabajo dentro del sistema de monitoreo. Cada grupo puede tener diferentes permisos sobre los elementos monitoreados y sobre las acciones que pueden ejecutar en la plataforma.

Esto permite implementar una administración jerárquica y segura, en la cual los administradores tienen acceso total al sistema, mientras que los usuarios invitados o de tipo “guest” poseen únicamente permisos de visualización.

En la parte superior del panel se encuentran los filtros de búsqueda por nombre y estado (Enabled o Disabled), junto con los botones Apply y Reset, que permiten aplicar los filtros o restaurar la vista original.

En la parte superior derecha se ubica el botón Create user group, que sirve para crear nuevos grupos personalizados. Al hacerlo, el administrador puede definir:

- Los usuarios que integrarán el grupo.
- Los permisos de acceso al frontend (interfaz principal de Zabbix).
- El modo de depuración (Debug mode), si se requiere monitoreo técnico del grupo.
- Las restricciones sobre los hosts o plantillas que podrán visualizar o editar.

Existen varios grupos predefinidos por el sistema.
El grupo Zabbix administrators posee control total sobre la plataforma, mientras que el grupo Guests está destinado a usuarios con acceso limitado o solo de lectura.
El grupo Internal agrupa usuarios técnicos y administrativos con permisos intermedios, facilitando la organización de tareas dentro del entorno de monitoreo.

Esta clasificación es esencial para asegurar que cada usuario tenga acceso únicamente a la información y funciones que necesita, preservando la seguridad y estabilidad del sistema.

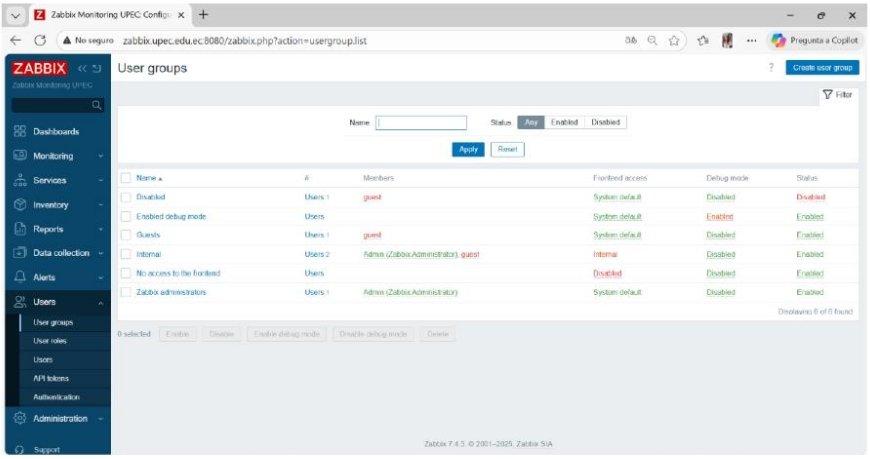


Figura 34. Vista del apartado User Groups del módulo Users en Zabbix Monitoring UPEC, donde se administran los grupos de usuarios y sus respectivos permisos, garantizando un control seguro y estructurado de los niveles de acceso al sistema.

9.2 User Roles

El subapartado User Roles dentro del módulo Users de Zabbix permite definir los roles y privilegios específicos que posee cada usuario dentro del sistema de monitoreo. Mientras que los User Groups agrupan usuarios por funciones o áreas, los User Roles determinan qué tipo de acciones o configuraciones puede ejecutar cada usuario, brindando un control preciso sobre la administración del entorno.

Esta estructura jerárquica garantiza una gestión segura y ordenada de los permisos, evitando que usuarios con menos experiencia o con funciones limitadas modifiquen parámetros críticos de la red o del sistema de monitoreo.

En la parte superior del panel se encuentra un campo de búsqueda por nombre y los botones Apply y Reset, los cuales permiten filtrar roles existentes o restaurar la vista general.
Asimismo, el botón Create user role, ubicado en la parte superior derecha, permite al administrador crear nuevos roles personalizados, definiendo qué elementos pueden visualizar, editar o gestionar dentro de la interfaz de Zabbix.

En la tabla principal se presentan los roles disponibles por defecto en el sistema, entre ellos:

Nombre del Rol	Usuarios Asociados	Descripción General
Admin role	Usuarios administrativos	Posee permisos avanzados para modificar configuraciones, agregar hosts, gestionar plantillas y acceder a la mayoría de las funciones del sistema.
Guest role	guest	Tiene permisos mínimos, limitados únicamente a la visualización de ciertos paneles o reportes; ideal para visitantes o usuarios en capacitación.
Super admin role	Admin (Zabbix Administrator)	Es el rol con el máximo nivel de privilegios. Permite acceder a todas las secciones del sistema, modificar configuraciones globales, gestionar usuarios, grupos, alertas y plantillas.
User role	Usuarios estándar	Tiene permisos intermedios, generalmente para visualizar el rendimiento de hosts, analizar alertas y generar reportes, pero sin posibilidad de editar configuraciones críticas.

Cada rol define de manera explícita el nivel de interacción con la plataforma, asegurando que las operaciones realizadas sean acordes con la responsabilidad asignada a cada usuario.
Por ejemplo, un Administrador de red puede tener el rol Admin role, mientras que un

técnico de soporte puede operar bajo el User role, limitando su acceso a tareas de monitoreo sin comprometer la configuración del sistema.

La presencia del Super admin role garantiza que siempre exista al menos un usuario con control total sobre la plataforma, lo cual es esencial para la seguridad, mantenimiento y gestión global del sistema Zabbix implementado en la Universidad Politécnica Estatal del Carchi (UPEC).

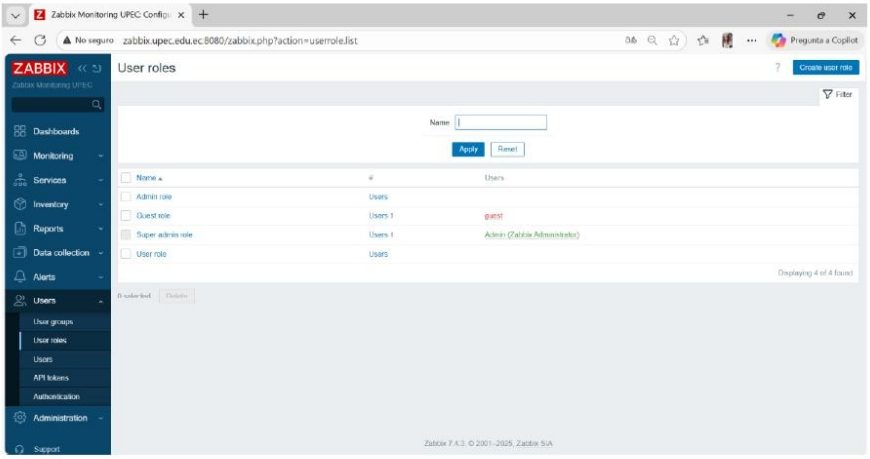


Figura 35. Vista del apartado User Roles del módulo Users en Zabbix Monitoring UPEC, donde se definen los distintos roles de usuario y sus permisos específicos dentro del sistema de monitoreo.

9.3 Users

El subapartado Users constituye el núcleo del módulo Users, ya que desde este espacio se gestionan los perfiles individuales de todas las personas con acceso al sistema de monitoreo Zabbix.
Aquí se definen las credenciales, roles, grupos, permisos y configuraciones de autenticación que permiten garantizar un acceso seguro, controlado y jerárquico al entorno de supervisión de red de la Universidad Politécnica Estatal del Carchi (UPEC).

En la parte superior del panel se encuentran los campos de búsqueda por Username, Name y Last name, así como filtros por User roles y User groups. Los botones Apply y Reset permiten aplicar o limpiar los filtros de manera rápida.
En la esquina superior derecha se dispone del botón Create user, que permite crear nuevos usuarios dentro del sistema.

Al crear un usuario, el administrador puede definir parámetros esenciales como:

- **Nombre de usuario (Username)** y **contraseña de acceso.**

- **Nombre completo (Name y Last name).**
- **Rol asignado (User role)**, el cual determina su nivel de permisos dentro del sistema.
- **Grupos de pertenencia (User groups)**, que permiten organizar a los usuarios según su área o responsabilidad.
- **Estado de la cuenta**, que puede estar habilitada (Enabled) o deshabilitada (Disabled).
- **Acceso a la interfaz (Frontend access)**, que regula si puede ingresar a la interfaz web de Zabbix.
- **Acceso a la API (API access)**, útil para integraciones automáticas con otros sistemas o aplicaciones.

Elusuario Admin es el principal administrador del sistema, con privilegios totales sobre la plataforma. Este usuario posee el rol Super admin role, lo que le permite realizar cualquier configuración, monitorear todos los hosts y administrar usuarios, grupos, alertas y plantillas.
Por otro lado, el usuario guest representa un perfil de acceso restringido, destinado a la visualización limitada de información o al acceso temporal durante procesos de prueba o auditoría.

Los indicadores Is online?, Login, y Frontend access muestran información relevante sobre la conexión y actividad reciente de cada usuario. En el caso del usuario Admin, se puede verificar el estado “Online” y el acceso correcto a la interfaz (Frontend access: Internal).

Este sistema de gestión de usuarios ofrece trazabilidad y seguridad, ya que cada acción realizada dentro de Zabbix puede asociarse a un usuario específico, lo que resulta esencial para la auditoría de actividades dentro del sistema de monitoreo de red institucional.

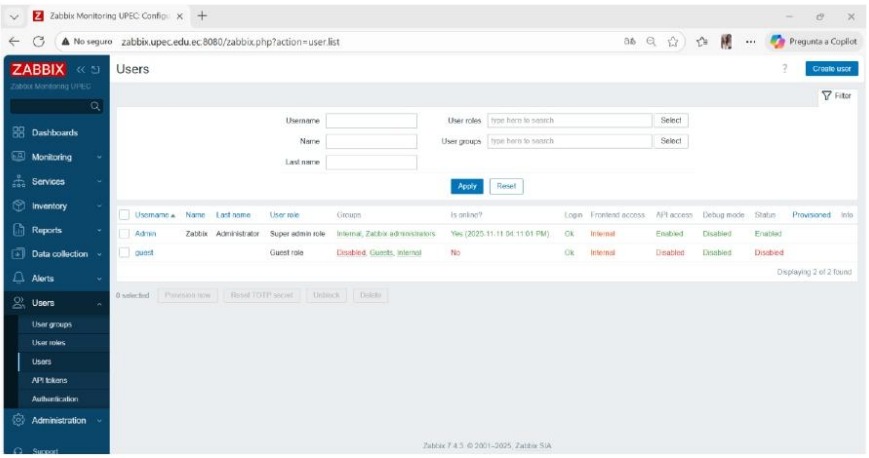


Figura 36. Vista del subapartado Users del módulo Users en Zabbix Monitoring UPEC, donde se administran los perfiles de usuario, roles, grupos y permisos, garantizando un acceso seguro y controlado al sistema.

9.4 API Tokens

El subapartado API Tokens dentro del módulo Users permite gestionar las claves de acceso programático que posibilitan la interacción segura entre Zabbix y otras aplicaciones externas.
Estas claves, conocidas como tokens, son esenciales para la automatización de procesos y la integración de sistemas, ya que permiten realizar operaciones dentro del entorno de monitoreo sin requerir el inicio de sesión manual de un usuario.

En el contexto de la Universidad Politécnica Estatal del Carchi (UPEC), esta funcionalidad ofrece la posibilidad de conectar Zabbix con otros sistemas institucionales —como plataformas de reportes, servicios de red o herramientas de análisis—, garantizando una comunicación segura y controlada.

El panel principal de este apartado muestra una interfaz sencilla que permite visualizar, crear y administrar los tokens disponibles. En la parte superior, se encuentran los filtros para búsqueda por nombre del token (Name), usuario asociado (User) y estado (Status), junto con los botones Apply y Reset que permiten aplicar o limpiar los filtros.

El botón Create API token, ubicado en la esquina superior derecha, se utiliza para generar una nueva clave. Durante este proceso, el administrador puede definir:

- **Nombre del token**, que sirve para identificar su propósito.
- **Usuario asociado**, responsable del token.
- **Fecha de expiración (Expires at)**, que establece un límite temporal de validez, incrementando la seguridad del sistema.
- **Estado**, que puede ser Enabled o Disabled según su disponibilidad de uso.

En la tabla inferior se muestran los tokens creados, junto con información relevante como:

- El usuario creador y fecha de creación.
- El último acceso registrado (Last accessed at).
- El estado actual del token (Status).

En la captura mostrada, no existen tokens activos registrados, lo que significa que no hay conexiones automatizadas habilitadas en ese momento. Esto es común en entornos donde el monitoreo se realiza de forma local o sin integraciones externas activas.

La correcta gestión de los API Tokens es fundamental para mantener la integridad, trazabilidad y confidencialidad de la información intercambiada entre Zabbix y otros

sistemas. Su uso permite aprovechar el potencial del monitoreo automatizado, pero siempre bajo una política de seguridad y control definida por los administradores del sistema.

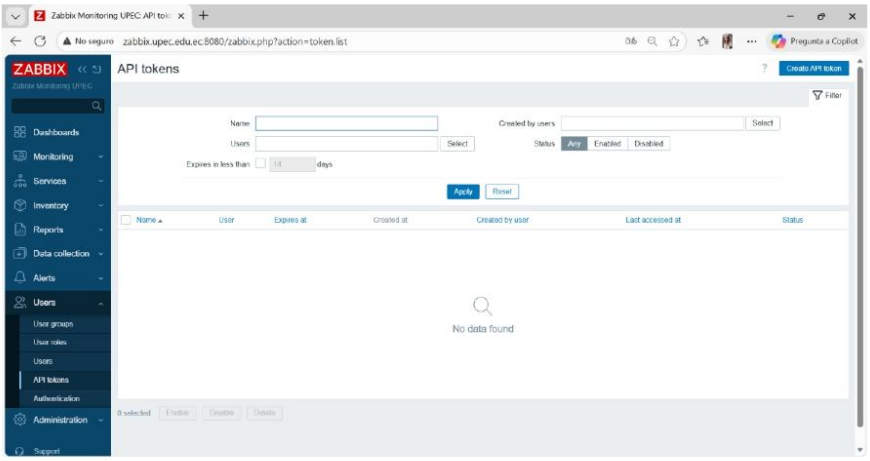


Figura 37. Vista del subapartado API Tokens del módulo Users en Zabbix Monitoring UPEC, donde se administran las claves de acceso programático para integraciones seguras y controladas con otros sistemas.

9.5 Authentication

El subapartado Authentication dentro del módulo Users de Zabbix es uno de los componentes más importantes en materia de seguridad y control de acceso. Desde esta sección se configuran los métodos de autenticación que determinan cómo los usuarios pueden acceder al sistema, así como las políticas de contraseñas y validación aplicadas para resguardar la integridad del entorno de monitoreo de red.

La correcta configuración de este apartado garantiza que únicamente usuarios autorizados puedan acceder al panel de control de Zabbix, lo cual es esencial en entornos institucionales como el de la Universidad Politécnica Estatal del Carchi (UPEC), donde se manejan datos técnicos de la infraestructura de red.

9.5.1 Authentication

En este subpunto se configuran los parámetros generales de autenticación interna, es decir, los que dependen del propio sistema Zabbix sin requerir servidores externos.

Entre las opciones más relevantes se encuentran:

- Default authentication: permite seleccionar el método principal de autenticación (Internal o LDAP).
- Password policy: define las políticas de seguridad de las contraseñas, tales como:
    - Longitud mínima (Minimum password length), que por defecto se establece en 8 caracteres.
    - Requisitos de complejidad, como incluir letras mayúsculas, minúsculas, dígitos o caracteres especiales.
    - Opción Avoid easy-to-guess passwords, que evita el uso de contraseñas predecibles.

Una vez configurados estos parámetros, el botón Update guarda los cambios y aplica las políticas de seguridad establecidas.

Esta configuración es clave para mantener un acceso controlado y robusto, reduciendo el riesgo de intrusiones o accesos no autorizados.

9.5.2 HTTP Settings

El subpunto HTTP Settings permite configurar la autenticación a través del protocolo HTTP, generalmente utilizada cuando se integra Zabbix con otros servicios web o servidores que utilizan cabeceras HTTP para validar usuarios.

A través de esta configuración, el sistema puede aceptar las credenciales enviadas por un servidor web intermedio, lo que resulta útil en entornos donde ya existen sistemas de autenticación centralizada.
Entre los parámetros configurables se incluyen el método de autenticación, los encabezados de usuario, y el control de dominio.

Esta opción facilita la integración de Zabbix en entornos corporativos o educativos que ya cuentan con políticas de acceso unificadas a través de la web institucional.

9.5.3 LDAP Settings

El subpunto LDAP Settings permite conectar Zabbix con un servidor LDAP (Lightweight Directory Access Protocol), una herramienta común en organizaciones que utilizan directorios centralizados, como Active Directory.

Mediante esta opción, los usuarios pueden iniciar sesión en Zabbix utilizando las mismas credenciales institucionales, evitando la duplicación de cuentas y fortaleciendo la gestión de identidades.

Los parámetros configurables incluyen:

- **Servidor LDAP:** dirección del servidor y puerto de conexión.

- **Base DN y Bind DN:** rutas y credenciales utilizadas para la búsqueda de usuarios.
- **Attribute mapping:** relación entre los atributos LDAP y los campos de Zabbix (por ejemplo, nombre de usuario o correo).

En la UPEC, esta función permitiría vincular Zabbix con el sistema institucional de autenticación, facilitando el acceso a los administradores y técnicos del área de redes mediante una gestión centralizada de usuarios.

9.5.4 SAML Settings

El subpunto SAML Settings introduce la posibilidad de configurar la autenticación mediante SAML (Security Assertion Markup Language), un protocolo utilizado en entornos empresariales y académicos para implementar autenticación única (Single Sign-On, SSO).

Este método permite que los usuarios accedan a Zabbix sin necesidad de ingresar sus credenciales directamente, siempre que ya estén autenticados en el sistema central (por ejemplo, en una intranet o plataforma educativa).

La configuración de SAML incluye parámetros como:

- Entity ID y SSO URL del proveedor de identidad.
- Certificados digitales para validar las comunicaciones entre el proveedor y Zabbix.

La implementación de este método aumenta significativamente la seguridad y eficiencia del acceso, al reducir los puntos de ingreso de credenciales y mejorar la experiencia del usuario.

9.5.5 MFA Settings

Finalmente, el subpunto MFA Settings (Multi-Factor Authentication) agrega una capa adicional de seguridad, exigiendo un segundo factor de verificación además de la contraseña.

Esto puede incluir el uso de códigos temporales (TOTP), aplicaciones de autenticación móvil o dispositivos físicos.
El objetivo de este método es prevenir accesos indebidos, incluso si las credenciales del usuario son comprometidas.

Su activación se recomienda especialmente para cuentas con permisos administrativos o acceso a configuraciones críticas del sistema.

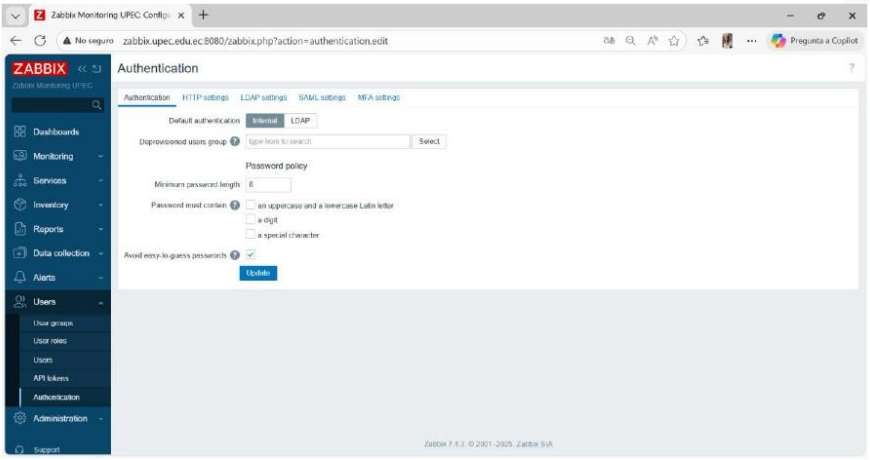


Figura 38. Vista del subapartado Authentication del módulo Users en Zabbix Monitoring UPEC, donde se configuran los métodos de autenticación y las políticas de seguridad para el acceso de usuarios al sistema.

10. Administration

El módulo Administration en Zabbix constituye el conjunto de herramientas que permiten la configuración avanzada y el mantenimiento del sistema de monitoreo. Desde este módulo, los administradores pueden definir parámetros globales que afectan al funcionamiento general de la plataforma, garantizando así la estabilidad, personalización y eficiencia operativa del entorno de supervisión de red.

En el caso del entorno de monitoreo de la Universidad Politécnica Estatal del Carchi (UPEC), este módulo es esencial para adaptar la interfaz, los registros, las políticas de limpieza, la gestión de proxies y los recursos del sistema de acuerdo con las necesidades de la infraestructura institucional.

Dentro de este módulo, uno de los apartados más importantes es General, el cual agrupa diversas configuraciones globales que afectan tanto a la experiencia visual de los usuarios como al comportamiento del sistema.

10.1 General

El apartado General dentro del módulo Administration centraliza las configuraciones básicas del sistema Zabbix, proporcionando control sobre el idioma, la zona horaria, los límites de datos mostrados, la apariencia de la interfaz gráfica y otros parámetros esenciales.

Esta sección garantiza que el entorno se mantenga coherente, optimizado y adaptado a las preferencias del equipo técnico que utiliza la plataforma.

En la barra lateral izquierda, bajo Administration → General, se despliegan varios subpuntos que organizan las configuraciones por categoría. El primero de ellos es GUI, descrito a continuación.

10.1.1 GUI

El subpunto GUI (Graphical User Interface) permite ajustar todos los aspectos relacionados con la interfaz visual y el entorno de trabajo del sistema Zabbix. Desde aquí, los administradores pueden definir la forma en que los usuarios interactúan con la plataforma y personalizar la presentación general de los datos.

Entre las principales configuraciones disponibles se encuentran:

- **Default language:** permite seleccionar el idioma predeterminado de la interfaz. En el caso de la implementación de la UPEC, el idioma seleccionado es *English (en_US)*.
- **Default time zone:** define la zona horaria del sistema. Se utiliza *(UTC-05:00) America/Guayaquil*, correspondiente a la ubicación geográfica de la institución.
- **Default theme:** ajusta el tema visual de la interfaz; en este caso, se emplea el tema *Blue*, caracterizado por su diseño claro y profesional.
- **Limit for search and filter results:** establece el número máximo de resultados que pueden visualizarse en búsquedas o filtros (por defecto, 1000).
- **Max number of columns and rows in overview tables:** determina el límite de columnas y filas en las tablas de resumen, asegurando una presentación ordenada de los datos (valor por defecto: 50).
- **Show warning if Zabbix server is down:** opción habilitada que muestra una advertencia en caso de que el servidor deje de responder, lo cual es crucial para mantener una **vigilancia continua del sistema**.
- **Working time:** define el horario laboral o de monitoreo principal; en este caso, de lunes a viernes de 09:00 a 18:00.
- **Show technical errors:** cuando se activa, permite visualizar errores técnicos en la interfaz, útil para tareas de diagnóstico.
- **Max history display period y Time filter default period:** determinan la duración máxima de los periodos mostrados en los gráficos históricos y filtros temporales.

El botón Update aplica los cambios configurados, mientras que Reset defaults restaura los valores originales del sistema.

Estas configuraciones son fundamentales para garantizar una interfaz eficiente, clara y adaptada al entorno institucional, facilitando la gestión visual del sistema de monitoreo por parte de los técnicos de redes y administradores del área de TIC.

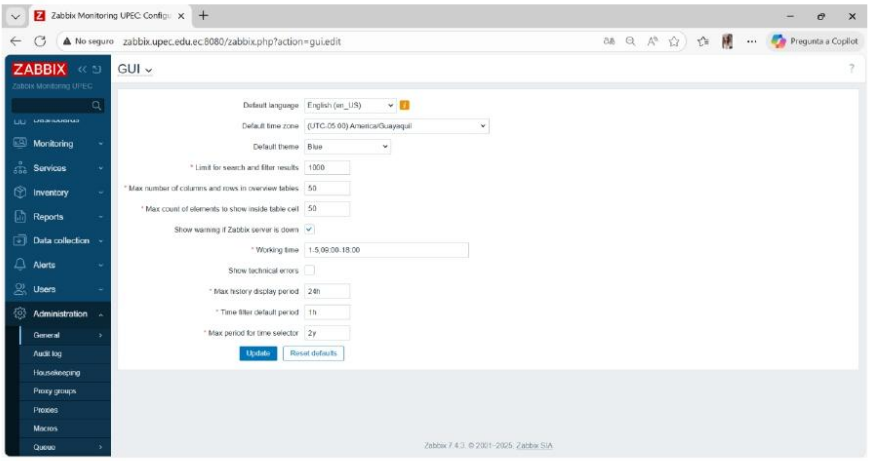


Figura 39. Vista del subapartado GUI del módulo Administration → General en Zabbix Monitoring UPEC, donde se configuran parámetros globales de idioma, zona horaria, tema visual y límites de visualización de datos.

10.1.2 Autoregistration

El subapartado Autoregistration dentro de Administration → General permite configurar los parámetros relacionados con la autoregistración de agentes Zabbix. Esta función resulta sumamente útil en entornos donde se incorporan nuevos equipos o servidores a la red, ya que facilita su detección y registro automático dentro del sistema de monitoreo sin necesidad de intervención manual por parte del administrador.

En el contexto del monitoreo implementado en la Universidad Politécnica Estatal del Carchi (UPEC), esta característica agiliza el proceso de incorporación de nuevos hosts o dispositivos a la infraestructura supervisada, optimizando la administración del sistema y garantizando una actualización constante del inventario de red.

La interfaz del subapartado muestra opciones específicas relacionadas con el nivel de cifrado de la comunicación entre el agente y el servidor Zabbix, siendo estos parámetros fundamentales para garantizar la seguridad y autenticidad de las conexiones.

Entre las principales configuraciones se encuentran:

- **Encryption level (Nivel de cifrado):** permite definir el tipo de seguridad empleado durante el proceso de autoregistro.

- *No encryption:* la comunicación entre el agente y el servidor no está cifrada, por lo tanto, se utiliza en entornos de prueba o redes internas seguras.
- *PSK (Pre-Shared Key):* habilita el uso de claves precompartidas para autenticar y cifrar la comunicación, brindando un nivel adicional de protección frente a accesos no autorizados.

- **Update:** una vez seleccionada la configuración deseada, este botón guarda los cambios y los aplica de forma inmediata en el sistema.

En la configuración observada en la imagen, la opción No encryption se encuentra habilitada, lo que indica que los agentes pueden registrarse en el servidor sin aplicar cifrado. Esto suele ser adecuado en entornos controlados y de acceso restringido, como el laboratorio o red interna de la UPEC, aunque para entornos productivos o expuestos a internet se recomienda activar la autenticación mediante PSK para reforzar la seguridad.

El uso correcto de la autoregistración permite automatizar la incorporación de nuevos equipos a la red, mantener un control continuo del inventario y reducir la carga operativa de los administradores del sistema, asegurando así una gestión eficiente, segura y escalable del monitoreo institucional.

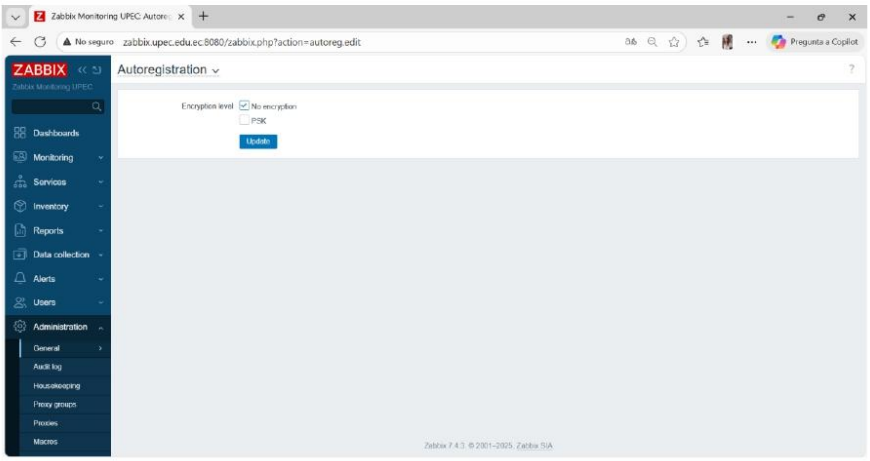


Figura 40. Vista del subapartado Autoregistration del módulo Administration → General en Zabbix Monitoring UPEC, donde se definen los niveles de cifrado y políticas de autoregistro de agentes en el sistema de monitoreo.

10.1.3 Timeouts

El subapartado Timeouts dentro de Administration → General permite configurar los tiempos de espera (timeout) aplicados a los distintos procesos de monitoreo y comunicación del sistema Zabbix.
Estos valores determinan cuánto tiempo esperará el servidor antes de considerar que una operación ha fallado por falta de respuesta.

La correcta configuración de los timeouts resulta esencial para garantizar que el sistema mantenga un equilibrio entre rendimiento, precisión y disponibilidad, evitando falsas alarmas y sobrecargas innecesarias.

En la interfaz se observa un conjunto de parámetros que definen los tiempos de espera para diferentes tipos de ítems y comprobaciones de red, expresados generalmente en segundos.

Timeouts for item types

En esta primera sección se definen los tiempos de espera asociados a los distintos tipos de elementos (items) que Zabbix utiliza para recolectar información. Entre los principales se encuentran:

- **Zabbix agent:** determina el tiempo máximo que el servidor esperará una respuesta del agente Zabbix instalado en el host. Por defecto, el valor es de 3 segundos.
- **Simple check:** establece el tiempo de espera para verificaciones básicas, como ping o disponibilidad de puertos.
- **SNMP agent:** define el tiempo límite para recibir respuesta de dispositivos que utilizan el protocolo SNMP, comúnmente aplicado a switches, routers o impresoras.
- **External check y Database monitor:** regulan las consultas externas y las verificaciones de bases de datos, respectivamente.
- **HTTP agent, SSH agent y TELNET agent:** especifican los tiempos máximos de espera en comunicaciones realizadas mediante estos protocolos.
- **Script:** tiempo permitido para la ejecución de scripts personalizados dentro del monitoreo.
- **Browser:** en este caso, con un valor de 60 segundos, se emplea en pruebas que requieren interacción con navegadores o simulaciones web.

Estos valores predeterminados garantizan una respuesta ágil y estable del sistema, especialmente en entornos donde los dispositivos pueden presentar ligeras demoras debido a la carga de red o latencia.

Network timeouts for UI

La segunda parte del panel permite establecer los tiempos de espera de red asociados a la interfaz de usuario (UI) y otras funciones relacionadas con las pruebas y ejecución de comandos.
Entre los parámetros configurables se incluyen:

- **Communication:** tiempo de espera general para la comunicación entre el frontend y el servidor Zabbix.
- **Connection:** límite de espera para la conexión inicial con un servicio remoto.
- **Media type test:** define el tiempo máximo para la prueba de medios de comunicación (como correo o webhook).
- **Script execution e Item test:** regulan el tiempo máximo de ejecución de scripts o pruebas de ítems personalizados.

Cada parámetro puede ajustarse en función del rendimiento del sistema y las condiciones de la red institucional. En el caso de la implementación en la Universidad Politécnica Estatal del Carchi (UPEC), se mantienen los valores por defecto, lo cual es adecuado para una red de tamaño medio con respuesta eficiente en los equipos supervisados.

El botón Update permite guardar los cambios realizados, mientras que el sistema aplica los nuevos valores de forma inmediata a los procesos de recolección y comunicación. Una configuración equilibrada en este apartado garantiza un monitoreo fluido, confiable y libre de retrasos excesivos, asegurando así la continuidad del servicio y la detección oportuna de fallas en la red institucional.

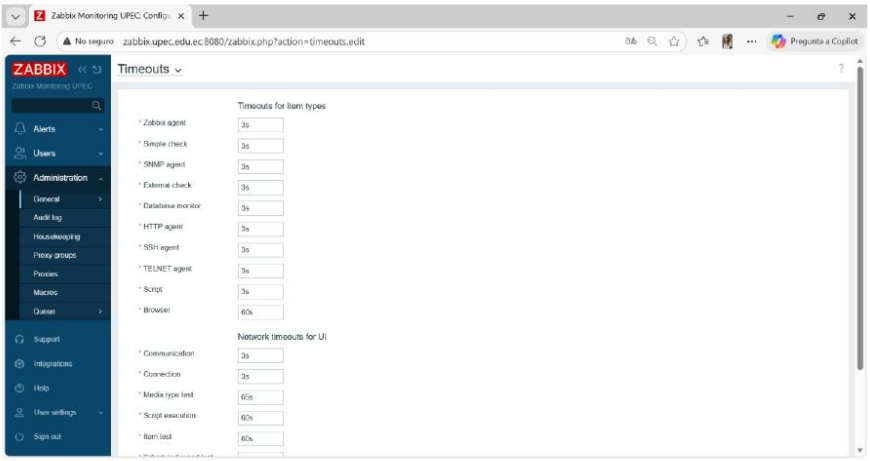


Figura 41. Vista del subapartado Timeouts del módulo Administration → General en Zabbix Monitoring UPEC, donde se configuran los tiempos de espera aplicados a los distintos tipos de comprobaciones y procesos de comunicación del sistema.

10.1.4 Images

El subapartado Images dentro de Administration → General permite gestionar los iconos e imágenes que utiliza Zabbix para representar visualmente los distintos dispositivos, servicios y componentes dentro del sistema de monitoreo.
Estas imágenes se emplean principalmente en la creación de mapas de red, dashboards y plantillas gráficas, facilitando una interpretación visual rápida y efectiva del estado de los equipos supervisados.

En el contexto de la implementación en la Universidad Politécnica Estatal del Carchi (UPEC), este apartado cumple un papel importante en la personalización y presentación visual del entorno de monitoreo, ayudando a los administradores de red a identificar con mayor claridad los distintos dispositivos y su condición operativa.

La interfaz del subapartado muestra una galería organizada de íconos clasificados por tipo y tamaño, como se aprecia en la figura. Entre los más representativos se incluyen:

- **Cloud:** ícono utilizado para representar servicios o recursos alojados en la nube, tales como almacenamiento remoto o aplicaciones web institucionales.
- **Crypto-router:** símbolo que representa routers o dispositivos de red con funciones de cifrado o seguridad.
- **Disk array:** ícono empleado para ilustrar servidores de almacenamiento o matrices de discos.

Cada imagen se encuentra disponible en distintos tamaños —desde 24x24 píxeles hasta 128x128 píxeles—, permitiendo adaptarlas al diseño de mapas o diagramas según la necesidad del usuario.

Asimismo, Zabbix permite incorporar nuevas imágenes personalizadas mediante la opción “Create icon”, lo que resulta útil para entornos institucionales que deseen incluir logotipos, símbolos propios o representaciones específicas de su infraestructura.

Esta flexibilidad gráfica contribuye a que los mapas de red elaborados dentro de Zabbix no solo sean funcionales, sino también claros y visualmente profesionales, fortaleciendo la gestión visual del monitoreo en la UPEC.

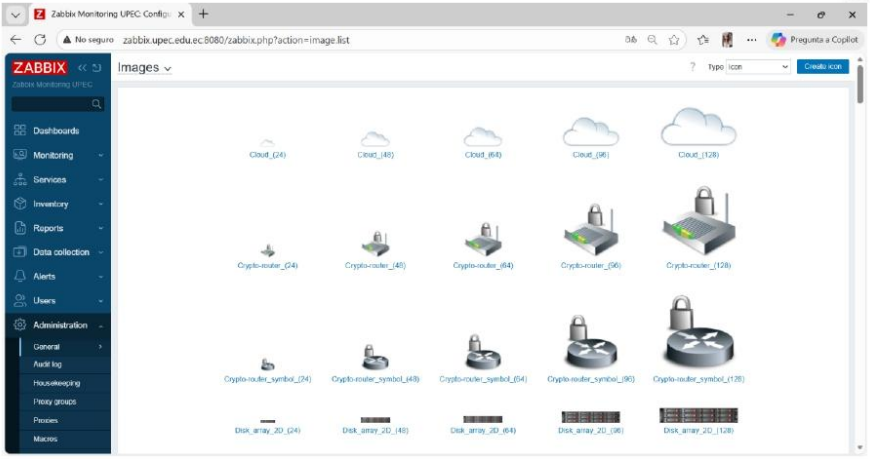


Figura 42. Vista del subapartado Images del módulo Administration → General en Zabbix Monitoring UPEC, donde se administran los íconos utilizados para representar visualmente los diferentes dispositivos y recursos en los mapas de red.

10.1.5 Icon Mapping

El subapartado Icon Mapping dentro de Administration → General permite establecer la asociación automática de íconos con distintos tipos de dispositivos o elementos de la red, en función de los valores registrados en el inventario de Zabbix. Esta funcionalidad resulta especialmente útil para personalizar mapas de red o representaciones gráficas, ya que permite asignar de manera dinámica un ícono específico según las características del host o equipo monitoreado.

En el contexto de la implementación realizada en la Universidad Politécnica Estatal del Carchi (UPEC), esta opción mejora la claridad visual y la organización del entorno de monitoreo, facilitando la rápida identificación de los diferentes equipos conectados a la red institucional (por ejemplo, routers, servidores o dispositivos de almacenamiento).

Configuración de Mapeo de Íconos

La interfaz de este apartado, como se muestra en la figura, permite definir distintos parámetros que determinan cómo se asignan los íconos:

- **Name:** campo donde se especifica el nombre del conjunto de mapeo o la política visual que se está configurando.
- **Mappings:** sección donde se definen las reglas que asocian un campo de inventario con un ícono determinado.

- **Inventory field:** permite seleccionar el campo del inventario que servirá como base para la asignación, por ejemplo, Type, Model o Location.
- **Expression:** se emplea para definir una condición o texto que debe coincidir con el valor del campo seleccionado.
- **Icon:** aquí se elige el ícono que se mostrará automáticamente cuando la condición especificada se cumpla.

Además, el sistema permite agregar múltiples reglas de mapeo mediante la opción "Add", lo que posibilita una gestión visual más flexible y adaptada a diferentes tipos de dispositivos.

En el ejemplo mostrado, se observa una configuración en la que el campo Type del inventario se asocia al ícono Cloud (24), lo que indica que cada host cuyo tipo corresponda a un servicio o recurso en la nube será representado automáticamente con dicho ícono en los mapas de red.

El uso del Icon Mapping mejora notablemente la eficiencia y estética de los mapas generados en Zabbix, permitiendo una presentación más intuitiva del entorno de monitoreo. Esto no solo facilita la labor del personal técnico, sino que también contribuye a una mayor comprensión visual del estado de la red institucional, especialmente en reportes o presentaciones internas de la UPEC.

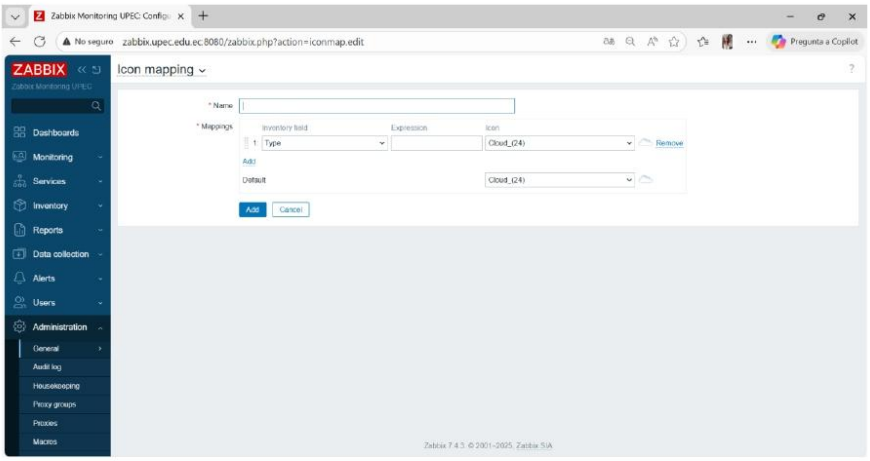


Figura 43. Vista del subapartado Icon Mapping del módulo Administration → General en Zabbix Monitoring UPEC, donde se definen las reglas de asociación entre los campos del inventario y los íconos empleados en los mapas de red.

10.1.6 Regular Expressions

El subapartado Regular Expressions dentro del módulo Administration → General en Zabbix, cumple una función avanzada destinada a la definición y gestión de expresiones regulares que permiten realizar filtrados, validaciones o exclusiones automáticas dentro de procesos de descubrimiento y monitoreo.
Estas expresiones se utilizan ampliamente en las reglas de descubrimiento (Discovery Rules), en las plantillas SNMP y en otros módulos que requieren analizar información mediante patrones de texto.

En el contexto de la Universidad Politécnica Estatal del Carchi (UPEC), este apartado tiene una relevancia técnica considerable, ya que posibilita refinar la detección automática de dispositivos y servicios dentro de la red institucional. De esta manera, se logra una administración más precisa, evitando registrar elementos innecesarios o duplicados durante los procesos de escaneo.

Configuración y estructura

En la interfaz del subapartado Regular Expressions, mostrada en la figura, se despliega una lista de expresiones predefinidas, entre las que se incluyen:

- **File systems for discovery:** permite filtrar los sistemas de archivos que serán considerados durante el proceso de descubrimiento, utilizando patrones como btrfs, ext4, xfs, entre otros.
- **Network interfaces for discovery:** define qué interfaces de red deben incluirse o excluirse durante la detección, mediante expresiones como Software Loopback o NULL, que evitan incluir interfaces virtuales o no activas.
- **Storage devices for SNMP discovery:** filtra los dispositivos de almacenamiento basados en memoria física o buffers de intercambio, optimizando la información recolectada por el protocolo SNMP.
- **Windows service names for discovery:** regula los servicios del sistema operativo Windows que serán analizados o ignorados en el monitoreo, contribuyendo a un control más selectivo de los procesos.
- **Windows service startup states for discovery:** determina qué servicios se considerarán activos, usando expresiones como automatic o automatic delayed, que definen estados válidos de inicio automático.

Cada expresión regular se compone de un patrón de coincidencia (pattern) y un resultado lógico (TRUE o FALSE), que especifica si el elemento detectado cumple con el criterio establecido.

Aplicación práctica en la UPEC

Durante la configuración de Zabbix para el monitoreo de la red institucional de la UPEC, el uso de expresiones regulares permite automatizar la detección y clasificación de dispositivos, reduciendo la carga de trabajo del administrador y garantizando la precisión de los datos recolectados.
Por ejemplo, mediante la exclusión de interfaces de tipo Loopback, se evita que el sistema interprete conexiones locales como elementos de red activos, lo que contribuye a un reporte más exacto del tráfico y rendimiento real.

Esta funcionalidad, aunque técnica, refuerza el enfoque de eficiencia y control automatizado que caracteriza la arquitectura de monitoreo implementada, asegurando una gestión más limpia y coherente de los recursos tecnológicos institucionales.

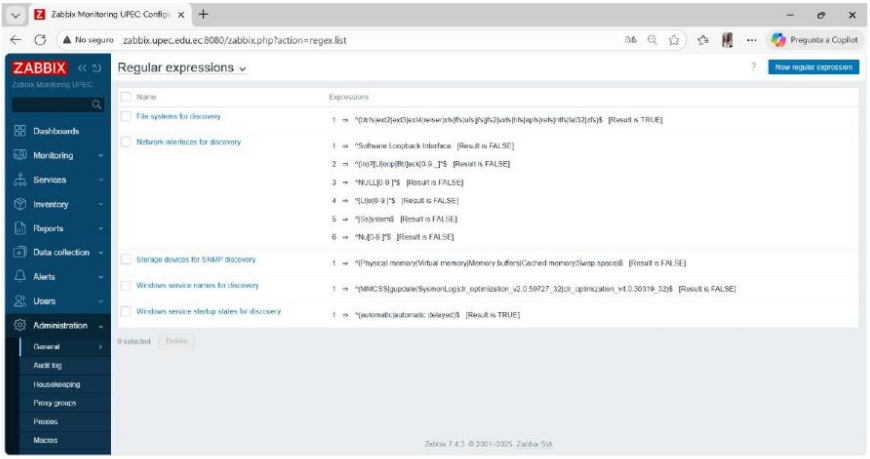


Figura 44. Vista del subapartado Regular Expressions del módulo Administration → General en Zabbix Monitoring UPEC, donde se definen patrones que permiten filtrar y controlar los elementos detectados en los procesos de descubrimiento de red.

10.1.7 Trigger Displaying Options

El subapartado Trigger Displaying Options, ubicado dentro del módulo Administration → General, permite configurar la forma en que se visualizan los eventos y alertas dentro de la interfaz de Zabbix. Esta sección es fundamental para personalizar la representación visual de los distintos niveles de severidad de los problemas detectados, facilitando la interpretación rápida y efectiva del estado de la red y los servicios monitoreados.

A través de estas opciones, el administrador puede definir cómo se muestran los eventos de tipo Problem (problema) y Resolved (resuelto), tanto si han sido reconocidos (acknowledged) como si aún no lo han sido, además de ajustar los parámetros de color, parpadeo y duración de visualización.

Configuraciones principales

En la interfaz del apartado, representada en la figura, se destacan los siguientes parámetros configurables:

- **Use custom event status colors:** permite habilitar el uso de colores personalizados para identificar los diferentes estados de los eventos.
- **Unacknowledged / Acknowledged PROBLEM events:** definen el comportamiento visual de los problemas detectados, ya sean nuevos o ya reconocidos por un operador; por defecto, se pueden mantener en modo "blinking" para captar rápidamente la atención.
- **Unacknowledged / Acknowledged RESOLVED events:** establecen cómo se mostrarán los eventos ya solucionados, pudiendo optar por mantener o eliminar el parpadeo.
- **Display OK triggers for:** determina el tiempo durante el cual se muestra un evento en estado "OK" antes de desaparecer del panel visual.
- **On status change triggers blink for:** especifica la duración del parpadeo cuando un evento cambia de estado (por ejemplo, de Problem a Resolved).

Asimismo, se incluyen las categorías de severidad, cada una asociada con un color distintivo que mejora la identificación visual de la gravedad del evento:

Nivel de severidad	Descripción	Color asociado
Not classified	Evento sin clasificación	Gris
Information	Información general	Azul
Warning	Advertencia o anomalía leve	Amarillo
Average	Problema moderado	Naranja
High	Problema crítico	Rojo oscuro
Disaster	Fallo grave o interrupción total	Rojo intenso

Importancia para el monitoreo en la UPEC

Durante la implementación del sistema de monitoreo en la Universidad Politécnica Estatal del Carchi (UPEC), esta configuración resulta clave para el seguimiento visual del estado de la red.
La correcta asignación de colores y efectos visuales (como el parpadeo de los eventos activos) permite que el personal técnico del Departamento de TIC identifique con rapidez los eventos más urgentes, mejorando la capacidad de respuesta ante incidentes.

Gracias a la personalización de los niveles de severidad y su visualización en tiempo real, Zabbix se convierte en una herramienta más intuitiva y eficaz para el control continuo de la calidad del servicio (QoS) en la infraestructura institucional.

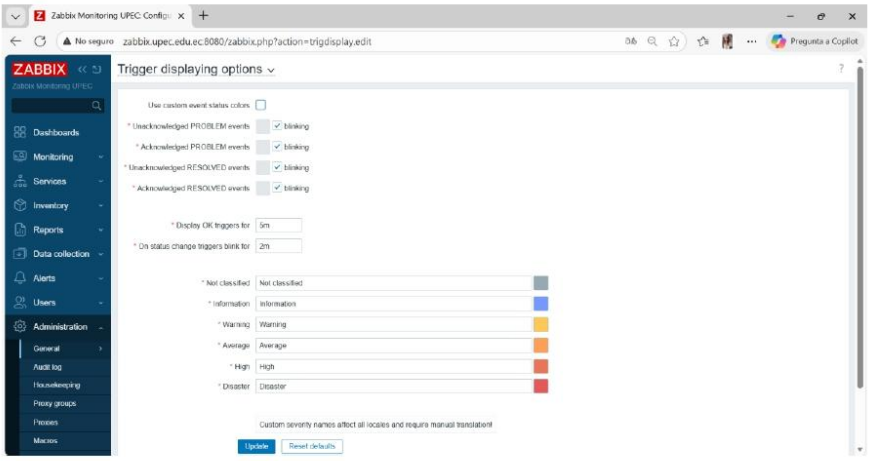


Figura 45. Vista del subapartado Trigger Displaying Options del módulo Administration → General en Zabbix Monitoring UPEC, donde se definen los parámetros de visualización y colores de los distintos niveles de severidad en los eventos del sistema.

10.1.8 Geographical Maps

El subapartado Geographical Maps dentro del módulo Administration → General permite configurar la integración de mapas geográficos dentro de la interfaz de Zabbix. Esta funcionalidad resulta especialmente útil para visualizar la ubicación física de los dispositivos o sedes monitoreadas, proporcionando una representación espacial de la infraestructura tecnológica bajo supervisión.

A través de este apartado, el administrador puede definir el proveedor de mapas, la URL base para la carga de teselas (tiles) y el nivel máximo de zoom permitido, ajustando el nivel de detalle visual de acuerdo con las necesidades de monitoreo de la institución.

Parámetros principales

En la interfaz del subapartado, mostrada en la figura, se pueden configurar los siguientes elementos:

- **Tile provider:** especifica el proveedor de mapas utilizado para renderizar la vista geográfica. En este caso, Zabbix emplea **OpenStreetMap Mapnik**, un servicio de código abierto ampliamente reconocido por su precisión y cobertura global.

- **Tile URL:** define la dirección de las teselas que conforman el mapa. La URL predeterminada (https://{s}.tile.openstreetmap.org/{z}/{x}/{y}.png) permite que Zabbix obtenga las imágenes cartográficas en función del nivel de zoom y la ubicación seleccionada.
- **Max zoom level:** establece el nivel máximo de acercamiento del mapa, determinado en 19 por defecto, lo que proporciona un equilibrio entre detalle y rendimiento del sistema.

Aplicación práctica en la UPEC

Durante la implementación del sistema de monitoreo en la Universidad Politécnica Estatal del Carchi (UPEC), la integración de mapas geográficos permite asociar visualmente los diferentes nodos de red o sedes institucionales dentro de un entorno geográfico real.
Por ejemplo, los distintos edificios del campus pueden representarse sobre un mapa de OpenStreetMap, facilitando la localización de servidores, switches o puntos de acceso, así como la identificación inmediata de zonas donde se registran fallos o interrupciones.

Esta funcionalidad no solo mejora la usabilidad y la comprensión del estado global de la red, sino que también optimiza la capacidad de respuesta ante incidentes, ya que los técnicos pueden ubicar físicamente el origen del problema mediante una representación visual directa.

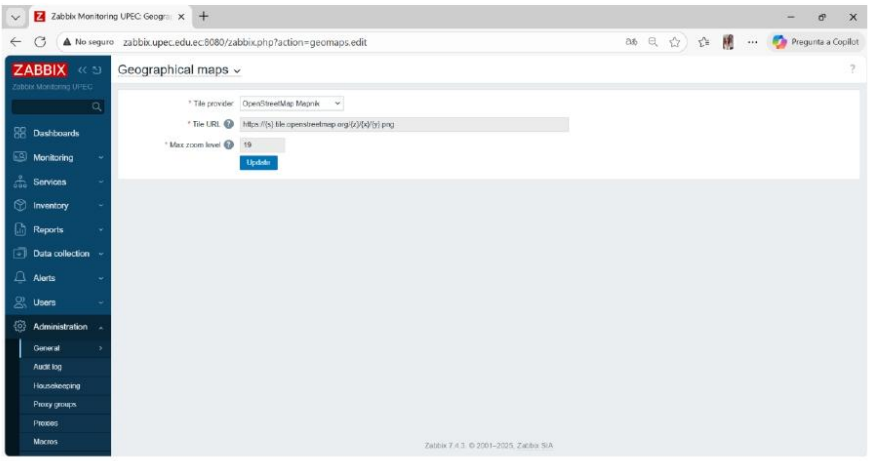


Figura 46. Vista del subapartado Geographical Maps del módulo Administration → General en Zabbix Monitoring UPEC, donde se configura el proveedor de mapas, la URL base y el nivel de zoom máximo para la visualización geográfica de los dispositivos monitoreados.

10.1.9 Modules

El subapartado Modules dentro del módulo Administration → General permite la gestión y supervisión de los módulos complementarios que amplían las funcionalidades del sistema Zabbix. Estos módulos proporcionan extensiones o complementos integrados directamente en la interfaz, que mejoran la visualización, el control y la administración de los diferentes componentes monitoreados en la red institucional.

Cada módulo cumple una función específica dentro del entorno de monitoreo, y puede activarse o desactivarse según los requerimientos del administrador. Esta modularidad permite personalizar la experiencia de uso, optimizando el rendimiento del sistema y adaptando la plataforma a las necesidades concretas de cada organización.

Descripción general de la interfaz

En la figura correspondiente se observa la lista de módulos disponibles, acompañados de información clave como:

- **Name:** nombre del módulo instalado o incorporado al sistema.
- **Version:** versión actual del módulo, lo que facilita la compatibilidad con la versión del servidor Zabbix.
- **Author:** autor o entidad desarrolladora del módulo; en este caso, todos los módulos son desarrollados por Zabbix SIA.
- **Description:** breve descripción de la función principal del módulo.
- **Status:** indica si el módulo está Enabled (habilitado) o Disabled (deshabilitado).

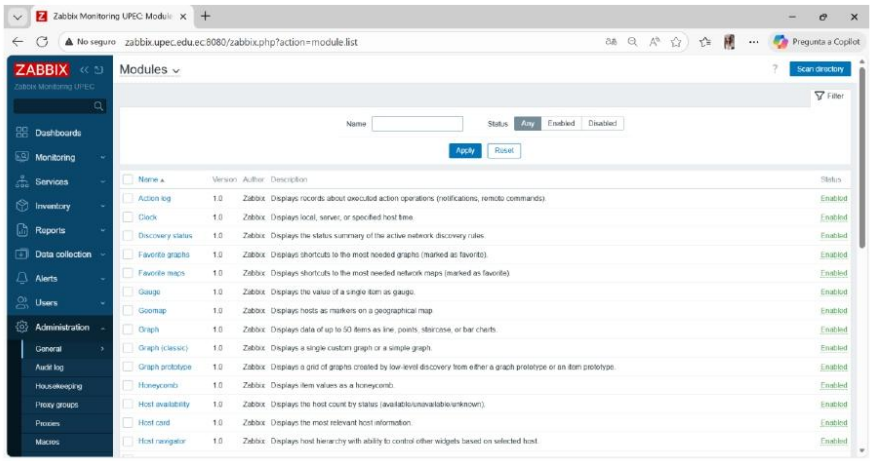


Figura 47. Vista del subapartado Modules dentro del módulo Administration → General en Zabbix Monitoring UPEC, donde se muestran los módulos habilitados, sus versiones, descripciones y estado actual de activación.

10.1.10 Connectors

El subapartado Connectors dentro del módulo Administration → General permite la creación y gestión de conectores de datos, los cuales son mecanismos que facilitan la integración de Zabbix con sistemas externos. Estos conectores permiten el intercambio de información entre la plataforma de monitoreo y otros servicios, como herramientas de análisis, sistemas de mensajería, o plataformas de gestión de infraestructura.

Mediante esta funcionalidad, Zabbix puede enviar o recibir datos en tiempo real utilizando protocolos estandarizados, como el Zabbix Streaming Protocol (ZSP) v1.0, garantizando una comunicación eficiente y segura entre diferentes entornos tecnológicos.

Descripción de la interfaz

En la figura se muestra la ventana de creación de un nuevo conector (New connector), donde se configuran los parámetros principales:

- **Name:** campo destinado al nombre identificativo del conector, lo cual facilita su administración en entornos con múltiples integraciones.
- **Protocol:** define el protocolo utilizado para la transferencia de datos. En este caso, Zabbix emplea el Zabbix Streaming Protocol v1.0, diseñado para optimizar la comunicación de métricas y eventos.
- **Data type:** especifica el tipo de información a transmitir, ya sea Item values (valores de ítems) o Events (eventos generados en el sistema).
- **URL:** dirección del destino o endpoint donde se enviarán los datos.
- **Tag filter:** permite aplicar filtros según etiquetas (tags) asociadas a los ítems o eventos, limitando el envío solo a aquellos que cumplen determinadas condiciones.
- **Type of information:** determina los tipos de datos que serán transmitidos, como numéricos, de texto, logs o caracteres.
- **HTTP authentication:** habilita la autenticación para conexiones seguras, protegiendo los datos durante la transferencia.
- **Advanced configuration:** apartado opcional para describir o documentar la funcionalidad específica del conector.

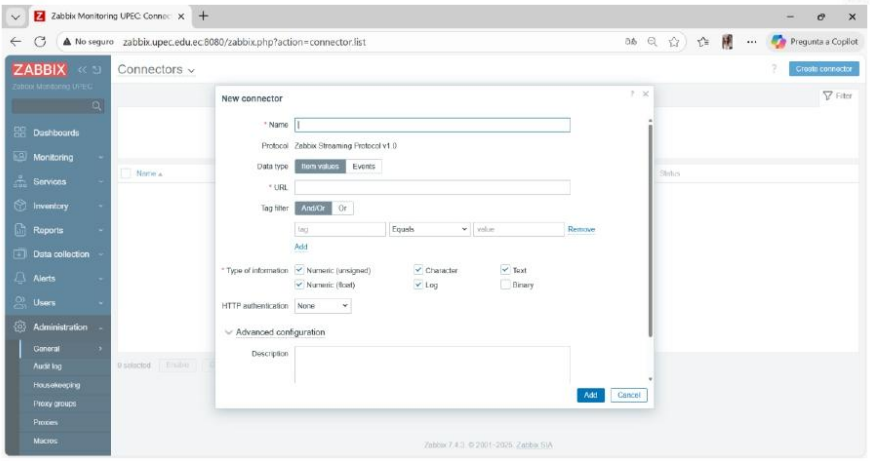


Figura 48. Vista del subapartado Connectors del módulo Administration → General en Zabbix Monitoring UPEC, donde se muestra la creación de un nuevo conector utilizando el protocolo Zabbix Streaming Protocol v1.0 para el intercambio de datos con sistemas externos.

10.1.11 Other Configuration Parameters

El subapartado Other Configuration Parameters dentro del módulo Administration → General agrupa una serie de ajustes avanzados que permiten personalizar y optimizar el comportamiento general del sistema Zabbix. Estos parámetros abarcan configuraciones relacionadas con la autenticación de usuarios, manejo de seguridad, almacenamiento de credenciales y comportamiento de descubrimiento automático de hosts, lo que contribuye a una gestión más segura y adaptada del entorno de monitoreo.

Descripción general de la interfaz

En la figura correspondiente se observa la ventana de configuración de este subapartado, donde se detallan los siguientes componentes principales:

- **Frontend URL:** define la dirección base del entorno gráfico de Zabbix (interfaz web). Este campo puede ser configurado para permitir accesos directos o integraciones con otras plataformas internas.
- **Group for discovered hosts:** asigna un grupo predeterminado a los dispositivos detectados mediante el descubrimiento automático (auto discovery).
- **Default host inventory mode:** determina el modo de inventario de los hosts, que puede ser Disabled, Manual o Automatic, dependiendo del nivel de

automatización requerido para registrar la información de los equipos monitoreados.

- **User group for database down message:** permite designar el grupo de usuarios que recibirá notificaciones cuando se detecten problemas en la base de datos de Zabbix. En este caso, se asigna a Zabbix administrators.
- **Log unmatched SNMP traps:** habilita la opción de registrar en los logs aquellos traps SNMP que no correspondan a reglas definidas, facilitando el análisis de eventos no categorizados.

Sección de Authorization

Esta sección define los parámetros de seguridad de acceso al sistema:

- **Login attempts:** establece el número máximo de intentos de inicio de sesión permitidos antes de activar un bloqueo temporal.
- **Login blocking interval:** define el intervalo de tiempo (en segundos) durante el cual se bloquea el acceso después de superar el número de intentos fallidos. Estos ajustes previenen ataques de fuerza bruta y refuerzan la seguridad de la autenticación de usuarios.

Sección de Storage of Secrets

Zabbix ofrece compatibilidad con sistemas externos de gestión de secretos, como:

- **HashiCorp Vault**
- **CyberArk Vault**

Estas herramientas permiten **almacenar de forma segura credenciales sensibles** (por ejemplo, contraseñas, claves o tokens API), evitando su exposición directa en los archivos de configuración del sistema.
Asimismo, el parámetro **Resolve secret vault macros by** define si la resolución de macros protegidas se realiza desde el Zabbix server o también a través de los proxies.

Sección de Security

Finalmente, la sección de seguridad incluye configuraciones relacionadas con la validación de URLs y políticas de acceso web:

- **Validate URI schemes:** define los esquemas de URI permitidos, tales como http, https, ftp, file, mailto, tel y ssh.

- **Use X-Frame-Options HTTP header:** protege contra ataques de clickjacking al limitar el modo en que la interfaz puede ser embebida en otros sitios web. En este caso, el valor SAMEORIGIN permite la visualización únicamente desde el mismo dominio.
- **Use iframe sandboxing:** añade una capa adicional de seguridad al restringir el contenido embebido mediante iframes.

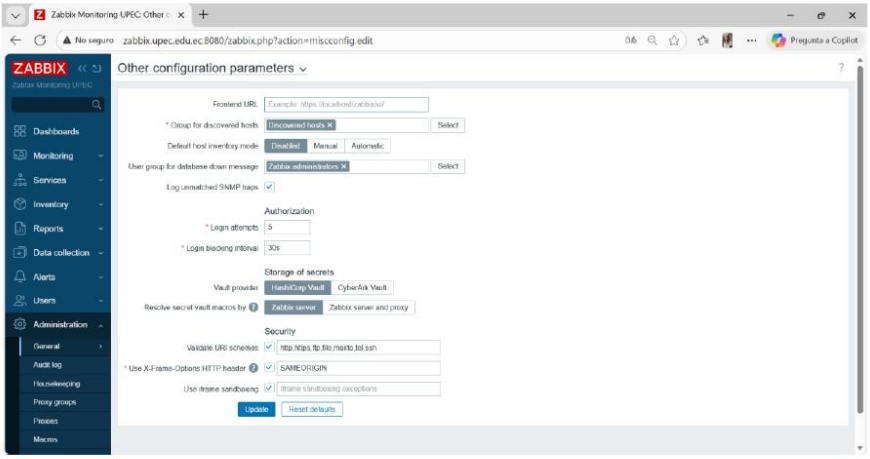


Figura 49. Vista del subapartado Other Configuration Parameters del módulo Administration → General en Zabbix Monitoring UPEC, donde se muestran los parámetros avanzados de seguridad, autenticación y almacenamiento de secretos.

10.2 Audit Log

El submódulo Audit Log dentro del apartado Administration de Zabbix tiene como finalidad registrar y supervisar todas las acciones realizadas por los usuarios dentro del sistema, permitiendo mantener un historial detallado de las configuraciones, accesos y modificaciones ejecutadas en la plataforma.
Este registro cumple un rol fundamental en la seguridad, trazabilidad y control administrativo, garantizando que cualquier cambio dentro del entorno de monitoreo pueda ser verificado y auditado en caso de incidentes o inconsistencias operativas.

Descripción de la interfaz

En la figura se presenta la vista del submódulo Audit Log, donde se observan las principales opciones de configuración relacionadas con el registro de auditoría del sistema:

- **Enable audit logging:** activa el registro de auditoría, permitiendo a Zabbix registrar las acciones de los usuarios en el sistema.
- **Log system actions:** habilita la opción para registrar también las acciones automáticas o internas que ejecuta el propio sistema, como la creación de elementos o los ajustes en los procesos de descubrimiento.
- **Enable internal housekeeping:** permite que el propio sistema gestione de forma automática la limpieza y optimización del registro de auditoría, evitando la acumulación excesiva de datos históricos.
- **Data storage period:** define el tiempo que se conservarán los registros en la base de datos antes de ser eliminados. En este caso, se establece un periodo de **31 días**, lo cual proporciona un equilibrio entre disponibilidad de información histórica y eficiencia del almacenamiento.

Importancia del registro de auditoría

El Audit Log resulta indispensable para garantizar la transparencia y responsabilidad dentro del entorno de monitoreo. Gracias a esta herramienta, los administradores pueden:

- Rastrear quién realizó una determinada acción (por ejemplo, agregar un host o modificar una alerta).
- Determinar cuándo y desde qué sesión se ejecutó un cambio.
- Detectar actividades inusuales o no autorizadas.
- Cumplir con políticas de seguridad institucionales y auditorías internas.

Además, la función de internal housekeeping asegura que el sistema mantenga un rendimiento estable al eliminar automáticamente los registros que ya no son necesarios, lo cual optimiza el uso de la base de datos de Zabbix.

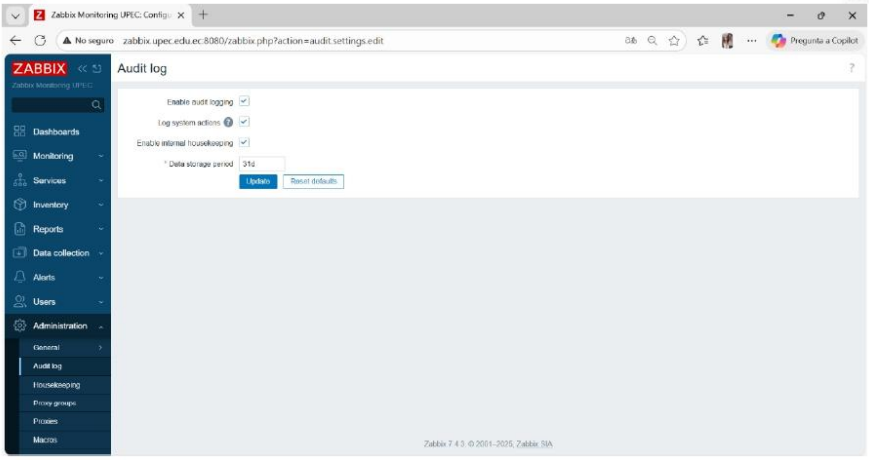


Figura 50. Vista del submódulo Audit Log dentro del módulo Administration en Zabbix Monitoring UPEC, donde se muestra la configuración del registro de auditoría y su periodo de almacenamiento de datos.

10.3 Housekeeping

El submódulo Housekeeping dentro del apartado Administration cumple una función esencial en el mantenimiento del sistema Zabbix, ya que se encarga de gestionar automáticamente la limpieza y optimización de la base de datos. Gracias a este proceso, se eliminan de forma periódica los registros antiguos o innecesarios, lo que contribuye a mantener el sistema ágil, ordenado y con un rendimiento óptimo.

En la figura se muestran las diferentes secciones que permiten configurar los periodos de retención de datos para los distintos componentes del sistema:

- **Events and alerts:** define cuánto tiempo se conservarán los registros relacionados con alertas, disparadores (triggers), servicios, descubrimientos de red y procesos de autorregistro.
- **Services:** gestiona la eliminación de datos asociados a los servicios monitoreados una vez cumplido el tiempo establecido.
- **User sessions:** determina el periodo durante el cual se almacenan las sesiones de los usuarios antes de ser eliminadas.
- **History:** establece la duración del almacenamiento de los datos históricos de monitoreo, garantizando que la base de datos no se sature con información antigua.

En resumen, este módulo permite que Zabbix mantenga su base de datos ligera y organizada sin intervención manual, favoreciendo la eficiencia, estabilidad y continuidad del monitoreo dentro de la red institucional.

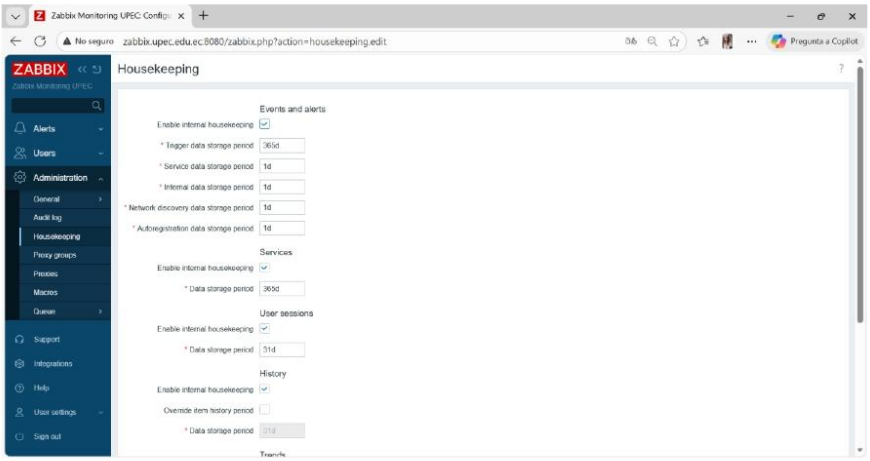


Figura 51. Vista del submódulo Housekeeping dentro del módulo Administration en Zabbix Monitoring UPEC, donde se configuran los periodos de retención de datos para eventos, servicios, sesiones e historial.

10.4 Proxy Groups

El submódulo Proxy Groups dentro del apartado Administration permite organizar y administrar los diferentes proxies configurados en Zabbix, agrupándolos de acuerdo con su función, ubicación o tipo de servicio que supervisan. Esta característica resulta útil especialmente en entornos distribuidos, donde varios proxies recopilan información desde distintas redes o sedes institucionales.

En la figura se muestra la ventana de creación de un nuevo grupo de proxy, donde el sistema solicita parámetros como el nombre del grupo, el tiempo de conmutación (Failover period) y el número mínimo de proxies activos necesarios para garantizar la disponibilidad del monitoreo. Además, se incluye un campo opcional de descripción, que facilita identificar el propósito o ámbito de aplicación del grupo creado.

Esta configuración contribuye a mantener un control estructurado y eficiente de los proxies, asegurando una comunicación constante entre los agentes de monitoreo y el servidor principal. Gracias a esta función, Zabbix puede distribuir la carga de monitoreo y garantizar la continuidad del servicio incluso ante posibles fallos en alguno de los proxies.

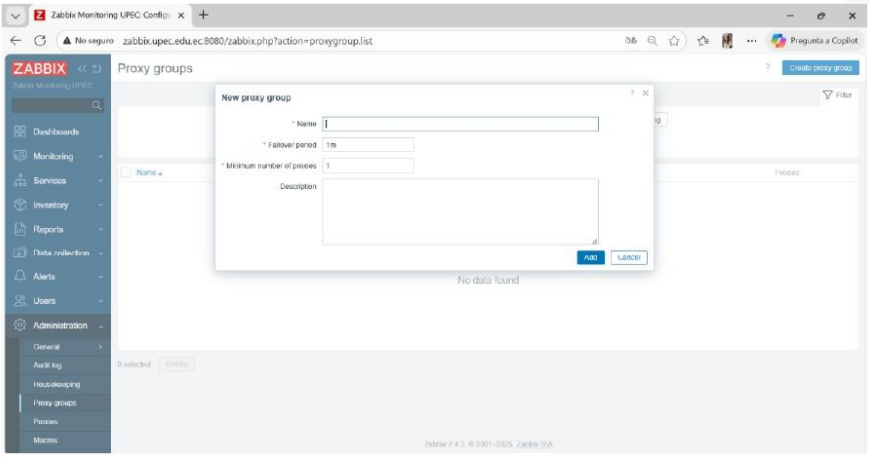


Figura 52. Ventana del submódulo Proxy Groups dentro del módulo Administration en Zabbix Monitoring UPEC, donde se configuran los parámetros para la creación de nuevos grupos de proxies.

10.5 Proxies

El submódulo Proxies dentro del apartado Administration de Zabbix permite gestionar los servidores proxy utilizados para recolectar y transmitir datos de monitoreo al servidor principal. Los proxies son componentes intermedios que actúan como agentes distribuidores, especialmente útiles cuando se supervisan redes remotas o sedes institucionales con conexiones limitadas o segmentadas.

En la figura se muestra la interfaz del submódulo, donde es posible crear, configurar y supervisar los proxies activos del sistema. La plataforma permite definir el modo de operación —activo o pasivo—, establecer parámetros de encriptación, conocer el estado de conexión, la versión instalada, el número de elementos supervisados y los hosts asociados a cada proxy.

Aunque en este entorno de monitoreo no se muestran proxies configurados, esta funcionalidad resulta esencial para ampliar la capacidad del sistema y garantizar la continuidad del monitoreo en infraestructuras distribuidas, reduciendo la carga sobre el servidor principal. En contextos como el de la Universidad Politécnica Estatal del Carchi (UPEC), la implementación de proxies sería especialmente útil para monitorear redes o edificios ubicados en diferentes campus o laboratorios sin comprometer el rendimiento del sistema central.

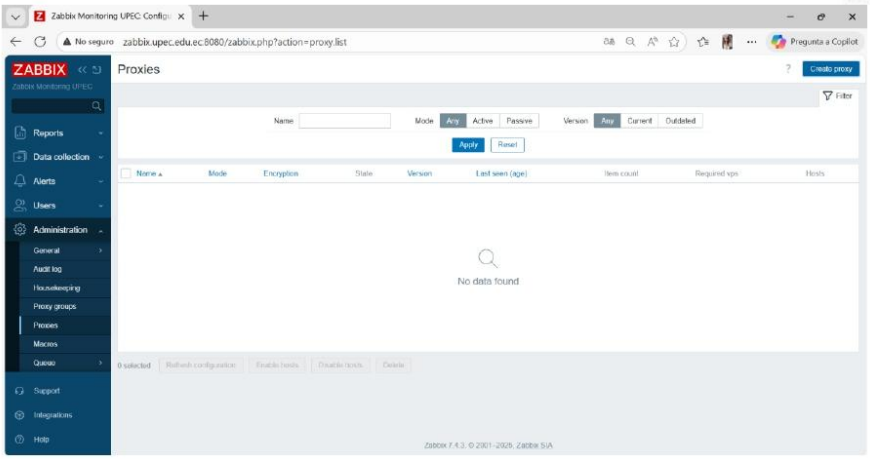


Figura 53. Vista del submódulo Proxies dentro del módulo Administration en Zabbix Monitoring UPEC, donde se pueden configurar y administrar los proxies encargados de la recolección de datos en redes distribuidas.

10.6 Macros

El submódulo Macros dentro del apartado Administration permite definir variables globales reutilizables que simplifican la configuración y el mantenimiento de todo el sistema de monitoreo en Zabbix. Estas macros se utilizan como parámetros dinámicos, que pueden insertarse en diferentes plantillas, hosts o ítems, evitando la necesidad de repetir información en múltiples configuraciones.

En la figura se observa un ejemplo de macro global configurada bajo la etiqueta {$SNMP_COMMUNITY}, con el valor public. Este tipo de macro es de uso frecuente cuando se emplea el protocolo SNMP (Simple Network Management Protocol), ya que facilita la autenticación y comunicación con dispositivos de red. Además, el sistema permite incluir una descripción opcional para documentar su propósito dentro de la infraestructura de monitoreo.

El uso de macros no solo agiliza la administración y estandarización de configuraciones, sino que también contribuye a una gestión más ordenada y segura del entorno de monitoreo, ya que los cambios pueden aplicarse globalmente con una sola modificación. En el contexto de la Universidad Politécnica Estatal del Carchi (UPEC), esta función garantiza que la administración de los parámetros de red sea más eficiente, escalable y menos propensa a errores humanos.

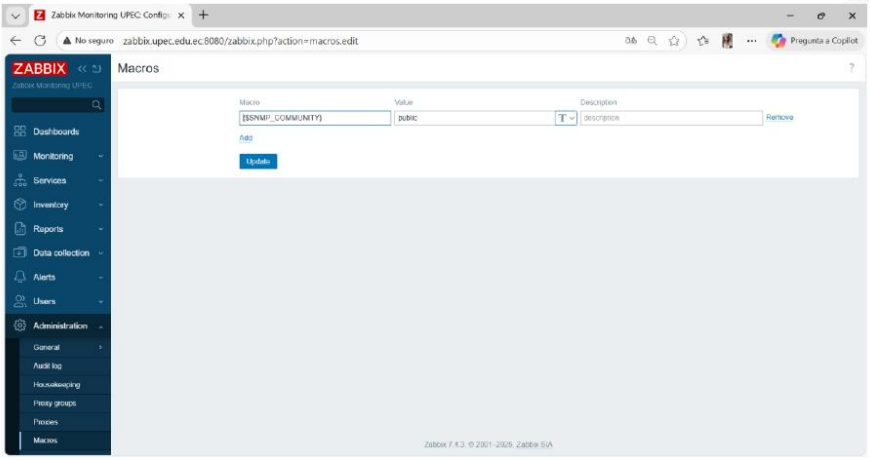


Figura 54. Vista del submódulo Macros dentro del módulo Administration en Zabbix Monitoring UPEC, donde se configuran las variables globales reutilizables del sistema.

10.7 Queue

El submódulo Queue dentro del apartado Administration permite supervisar el estado de las colas de procesamiento de ítems que el servidor Zabbix debe gestionar. Su función principal es detectar posibles retrasos en la recolección de información proveniente de agentes o servicios, lo que permite mantener la estabilidad y eficiencia del sistema.

En esta sección, Zabbix ofrece diferentes subpuntos que facilitan una observación detallada del comportamiento de las colas, ayudando a los administradores a identificar cuellos de botella y optimizar el rendimiento del sistema de monitoreo.

10.7.1 Queue Overview

En este primer subpunto se muestra una visión general del estado de las colas de procesamiento. La interfaz lista los diferentes tipos de ítems monitoreados —como Zabbix agent, SNMP agent, HTTP agent, SSH agent, TELNET agent, entre otros— junto con sus intervalos de respuesta: 5 segundos, 10 segundos, 30 segundos, 1 minuto, 5 minutos y más de 10 minutos.

Como se aprecia en la siguiente figura, el entorno implementado en la Universidad Politécnica Estatal del Carchi (UPEC) no presenta demoras en ninguna de las colas, mostrando valores de cero en todos los intervalos. Esto refleja un funcionamiento estable y eficiente del sistema, con una comunicación fluida entre el servidor Zabbix y los agentes distribuidos en la red institucional.

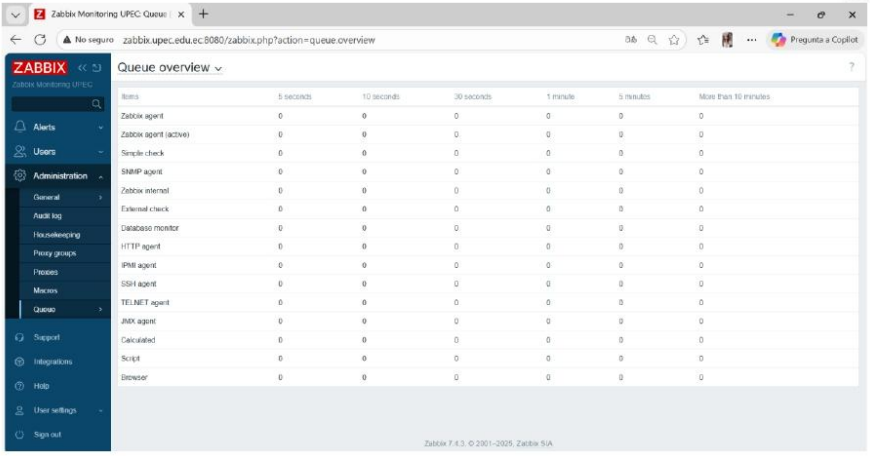


Figura 55. Vista del subpunto Queue overview dentro del módulo Administration en Zabbix Monitoring UPEC, donde se observa la ausencia de retrasos en las colas de procesamiento de ítems.

10.7.2 Queue Details

Este subpunto permite acceder a una vista detallada de los ítems que podrían presentar demoras en su procesamiento. Aquí se muestran parámetros como el nombre del host, el ítem afectado, el tipo de chequeo, y el tiempo de espera acumulado. Esta vista resulta especialmente útil para diagnosticar problemas de rendimiento o identificar agentes que responden con lentitud, lo cual facilita una respuesta proactiva del administrador antes de que los retrasos afecten al rendimiento global del sistema.

En el entorno de monitoreo de la UPEC, esta sección no presenta ítems en espera, lo que confirma que no existen congestiones ni interrupciones en el flujo de información entre los dispositivos y el servidor de monitoreo.

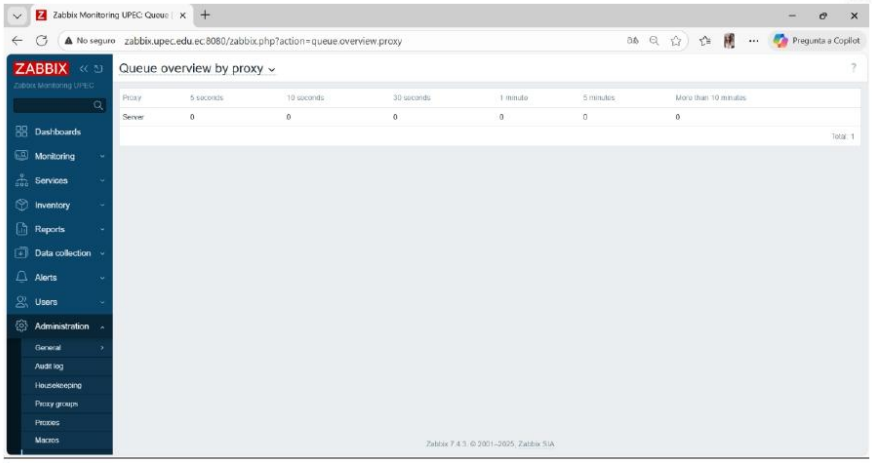


Figura 56. Vista del subpunto Queue details dentro del módulo Administration en Zabbix Monitoring UPEC, donde se listan los ítems con posibles retrasos en la recolección de datos.

10.7.3 Internal Queue

El subpunto Internal Queue permite visualizar las tareas internas del servidor Zabbix que están pendientes de ejecución, como la limpieza automática de bases de datos (housekeeping), la actualización de elementos de configuración o la ejecución de acciones automatizadas.
Este componente resulta esencial para garantizar la integridad operativa del sistema, ya que proporciona una visión del rendimiento interno de los procesos del servidor, permitiendo anticipar y resolver problemas antes de que afecten a las tareas principales de monitoreo.

Durante la implementación en la UPEC, esta sección se mantuvo sin registros pendientes, lo cual evidencia que el servidor está procesando sus tareas internas correctamente y sin acumulación de operaciones.

10.7.3 Queue Overview by Proxy

El subpunto Queue Overview by Proxy ofrece una visión de las colas de procesamiento clasificadas por los servidores proxy configurados en Zabbix. Esta vista permite evaluar el desempeño individual de cada proxy en la recolección y envío de información al servidor principal.
En el caso del sistema implementado en la UPEC, los resultados muestran que el único servidor registrado no presenta retrasos en ningún intervalo de tiempo. Esto evidencia que

la comunicación entre el proxy y el servidor central es óptima, garantizando que los datos recopilados se transmitan sin pérdida ni demora.

Esta funcionalidad es especialmente útil cuando se monitorean infraestructuras distribuidas, ya que permite detectar de manera precisa si algún proxy presenta saturación o interrupciones en su enlace con el servidor principal.

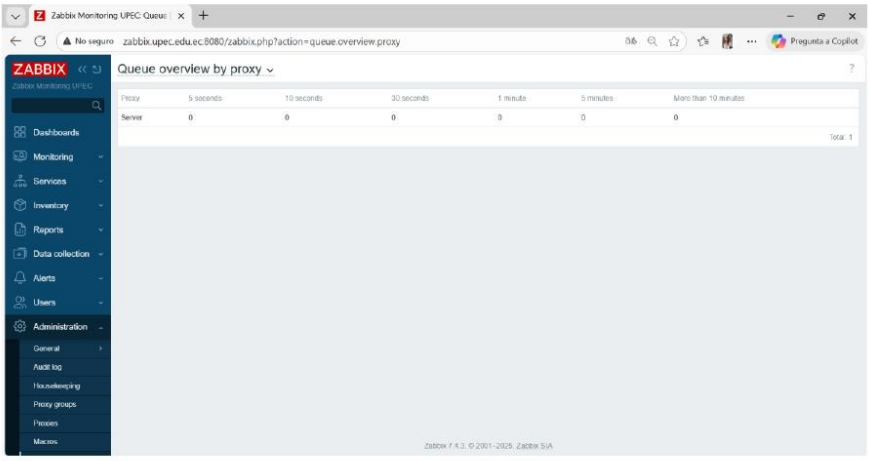


Figura 57. Vista del subpunto Queue overview by proxy dentro del módulo Administration en Zabbix Monitoring UPEC, donde se evidencia la correcta comunicación entre el servidor y el proxy sin tiempos de espera.

10.8 Support

El módulo Support en Zabbix brinda acceso directo a los recursos oficiales de asistencia y documentación que ofrece la plataforma. Desde este apartado, los administradores pueden consultar la documentación técnica de Zabbix, acceder a la base de conocimientos, obtener información sobre la versión instalada, o contactar con el equipo de soporte oficial en caso de incidencias complejas.

En la Universidad Politécnica Estatal del Carchi (UPEC), este módulo representa un punto clave para el mantenimiento y actualización del sistema de monitoreo, ya que permite validar configuraciones y acceder a las guías que garantizan el correcto funcionamiento de la herramienta.

10.9 Integrations

El módulo Integrations ofrece la posibilidad de conectar Zabbix con aplicaciones externas, como herramientas de notificación, mensajería, automatización o almacenamiento.

A través de este módulo, se configuran integraciones nativas o personalizadas que amplían las capacidades del sistema, permitiendo que Zabbix envíe alertas automáticas a plataformas como Slack, Telegram, Microsoft Teams, o servicios REST API.

En la implementación realizada en la UPEC, esta sección se utiliza para garantizar la interoperabilidad entre Zabbix y otros sistemas institucionales, fortaleciendo la capacidad de respuesta ante incidentes de red y mejorando la eficiencia del monitoreo.

10.10 Help

El módulo Help proporciona acceso rápido a la ayuda interactiva y documentación oficial de Zabbix, facilitando la navegación y comprensión de sus múltiples funcionalidades. Desde esta sección, los usuarios pueden revisar guías, tutoriales y explicaciones de parámetros del sistema.
Su utilidad principal radica en orientar al administrador durante la configuración o resolución de errores, sin necesidad de abandonar la interfaz de monitoreo.

10.11 User Settings

El módulo User Settings permite la gestión de la configuración personal de cada usuario dentro del entorno de Zabbix.
Este módulo está dividido en tres subpuntos principales: Profile, Notifications y API Tokens, los cuales permiten personalizar la experiencia del usuario, definir métodos de notificación y administrar accesos programáticos.

10.11.1 Profile

En este subpunto, el usuario puede ajustar sus preferencias personales como el idioma, la zona horaria, el tema visual, el tiempo de actualización de la interfaz (refresh), y la cantidad de filas mostradas por página.
También se pueden modificar opciones como el inicio de sesión automático (auto-login) o el cierre automático por inactividad (auto-logout).

En la implementación de la UPEC, el perfil del administrador principal (Zabbix Administrator) mantiene la zona horaria establecida en (UTC-05:00) America/Guayaquil, garantizando la sincronización horaria con los equipos de red.

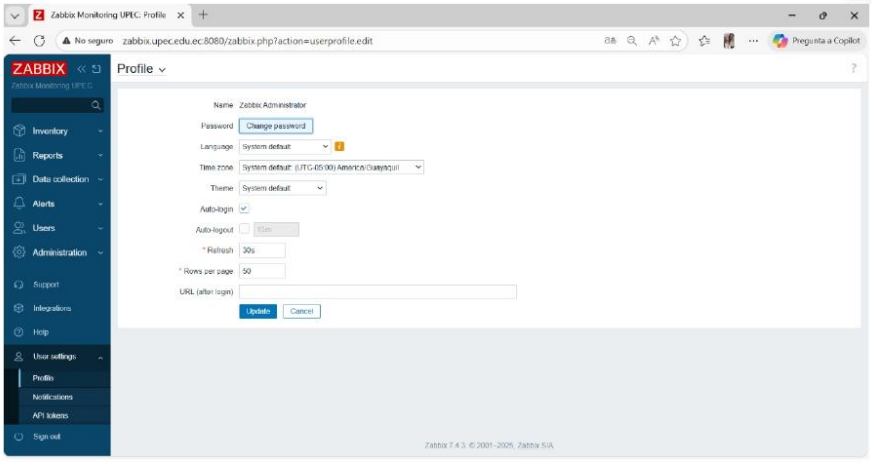


Figura 58. Vista del subpunto *Profile* dentro del módulo *User Settings* en Zabbix Monitoring UPEC, donde se configuran las preferencias del usuario administrador.

10.11.2 Notifications

El subpunto Notifications está destinado a configurar los canales de comunicación mediante los cuales el sistema Zabbix envía alertas al usuario. Aquí se pueden definir métodos como correo electrónico, mensajería instantánea o integraciones externas (Telegram, Slack, entre otros), así como establecer horarios y condiciones para el envío de notificaciones.

Esta función garantiza que los administradores del área TIC en la UPEC sean notificados en tiempo real ante cualquier evento crítico o interrupción del servicio de red, mejorando la capacidad de respuesta institucional.

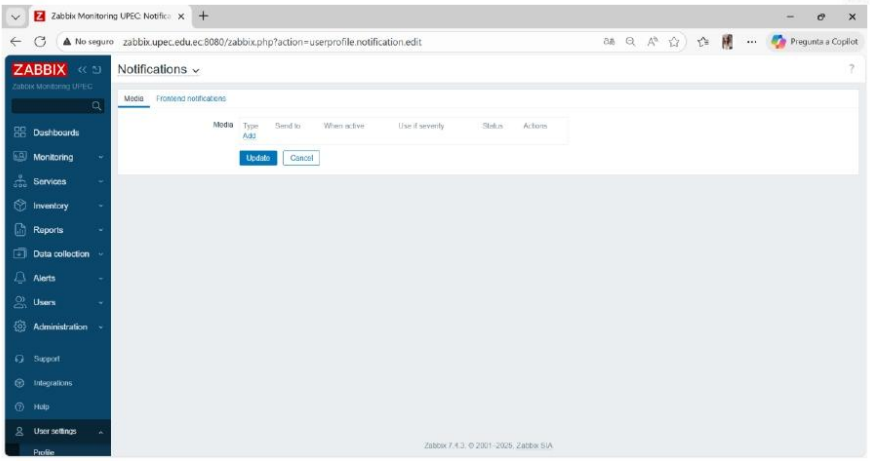


Figura 59. Vista del subpunto Notifications dentro del módulo User Settings, donde se definen los métodos de notificación y envío de alertas.

10.11.3 API Tokens

El subpunto API Tokens permite la generación y gestión de claves de acceso (tokens) que facilitan la interacción automatizada con Zabbix mediante la API REST. Gracias a estas credenciales, es posible conectar aplicaciones o scripts externos que necesiten obtener información del sistema, crear hosts, o generar reportes de manera automatizada.

En la UPEC, el uso de tokens API ofrece una ventaja importante en la automatización de tareas administrativas, permitiendo que Zabbix se integre con otros servicios de red o paneles de monitoreo adicionales sin comprometer la seguridad.

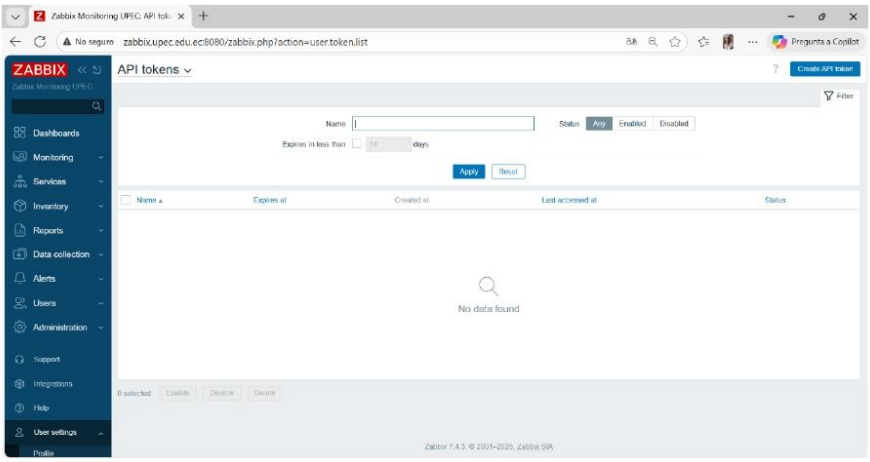


Figura 60. Vista del subpunto API Tokens dentro del módulo User Settings, donde se gestionan las credenciales de acceso para integraciones externas.

10.12 Sign Out

El módulo Sign Out permite cerrar de manera segura la sesión activa del usuario dentro de Zabbix.z Esta acción es fundamental para mantener la seguridad de la plataforma, especialmente cuando el acceso se realiza desde equipos compartidos o ubicaciones públicas.
El cierre de sesión garantiza que los privilegios de administración no queden disponibles a otros usuarios, protegiendo así la información sensible del sistema de monitoreo institucional.

Conclusión del Manual

El presente Manual de Usuario de Zabbix Monitoring – Universidad Politécnica Estatal del Carchi (UPEC) ha sido desarrollado con el propósito de guiar, capacitar y asistir al personal técnico y administrativo en el uso adecuado de la herramienta de monitoreo de red Zabbix.

A lo largo del manual se abordaron los principales módulos del sistema —desde la administración de usuarios, la configuración de hosts y servicios, hasta la creación de dashboards, alertas y reportes—, permitiendo al lector comprender el funcionamiento integral de la plataforma y su importancia dentro de la infraestructura tecnológica institucional.

La implementación de Zabbix en la UPEC representa un avance significativo en la gestión de la red universitaria, al ofrecer monitoreo en tiempo real, detección temprana de fallos y una administración eficiente de los recursos tecnológicos.

Gracias a su carácter open source, escalable y adaptable, Zabbix se consolida como una solución sostenible y de bajo costo para la supervisión de servicios críticos en entornos educativos.

Se recomienda mantener actualizado el sistema y las credenciales de acceso, así como documentar cualquier cambio en la infraestructura monitoreada, garantizando la continuidad y seguridad del servicio.

Finalmente, este manual busca convertirse en una herramienta de consulta y apoyo permanente para el Departamento de Tecnologías de la Información y Comunicación (TIC) de la UPEC, contribuyendo al fortalecimiento de la calidad del servicio de red y la optimización de los procesos tecnológicos institucionales.

Recomendaciones finales

- Realizar copias de seguridad periódicas de la base de datos de Zabbix.
- Mantener actualizado el software a la versión más reciente y estable.
- Revisar las políticas de notificación y autenticación cada semestre.
- Capacitar de forma continua al personal encargado del monitoreo.
- Documentar todos los cambios realizados en la configuración del sistema.

Créditos

Autora: Steffany Revelo

Tutor: Ing. Milton del Hierro Mosquera

Carrera: Ingeniería en Computación

Institución: Universidad Politécnica Estatal del Carchi (UPEC)

Año: 2025

Anexo 4. Manual de configuración de Agentes Zabbix

UNIVERSIDAD POLITECNICA ESTATAL DEL CARCHI

FACULTAD DE INDUSTRIAS AGROPECUARIAS Y CIENCIAS AMBIENTALES

CARRERA DE COMPUTACION

Educamos para transformar el mundo

MANUAL DE CONFIGURACION DE AGENTES ZABBIX

```
SW-DMZ(config)#snmp-server community public RO
SW-DMZ(config)#snmp-server community private RW
SW-DMZ(config)#snmp-server community UPEC-SNMP RO
SW-DMZ(config)#
```

Zabbix es una herramienta de monitoreo de red que permite supervisar, en tiempo real, el funcionamiento de servidores, equipos y servicios dentro de una institución. Su propósito es detectar fallos o lentitud en la red antes de que afecten a los usuarios, ofreciendo una visión clara del rendimiento y del uso de los recursos tecnológicos.

A diferencia de otras soluciones comerciales, Zabbix es completamente open source, lo que significa que no requiere licencias y puede adaptarse a las necesidades de cada organización. Gracias a su interfaz web, los administradores pueden observar el estado general de la red, recibir alertas automáticas y tomar decisiones preventivas para mantener la estabilidad del sistema.

Según TechRadar (2025), Zabbix se destaca como una de las herramientas de monitoreo de red más completas y potentes del mercado, gracias a su carácter open source, su alta capacidad de personalización y su escalabilidad, lo que la convierte en una opción ideal para entornos institucionales y educativos donde se requiere control total sin costos de licencia.

MANUAL PARA AGREGAR DISPOSITIVOS CON SNMP EN ZABBIX

1. Introducción

El presente manual describe de manera clara y ordenada el proceso para agregar dispositivos de red al sistema de monitoreo Zabbix utilizando el protocolo SNMP. Este procedimiento se aplica a equipos como switches, routers y otros dispositivos que forman parte de la infraestructura tecnológica de la institución.
El objetivo es garantizar una integración correcta que permita obtener métricas confiables sobre tráfico, disponibilidad y rendimiento de la red.

2. Requisitos previos

Antes de iniciar el proceso en Zabbix, es necesario verificar que el dispositivo a integrar cumpla con las siguientes condiciones:

1. El equipo debe tener habilitado el servicio SNMP.
2. Debe estar configurada una comunidad SNMP con permisos de lectura.

3. El servidor Zabbix debe tener acceso a la dirección IP del dispositivo.
4. Debe conocerse la comunidad SNMP, la versión del protocolo y la dirección IP del equipo.

En el caso de los switches Cisco, una configuración típica de comunidades SNMP puede ser la siguiente:

```
SW-DMZ(config)#snmp-server community public RO
SW-DMZ(config)#snmp-server community private RW
SW-DMZ(config)#snmp-server community UPEC-SNMP RO
SW-DMZ(config)#
```

Para el monitoreo en Zabbix se utilizará la comunidad configurada como lectura (RO), en este caso: UPEC-SNMP.

3. Acceso a la sección de creación de hosts

Para iniciar el proceso de incorporación del dispositivo:

1. Ingresar al panel de Zabbix.
2. En el menú lateral izquierdo seleccionar la opción “Monitoring”.
3. Dentro de esta sección, seleccionar “Hosts”.
4. Hacer clic en el botón “Create host”.

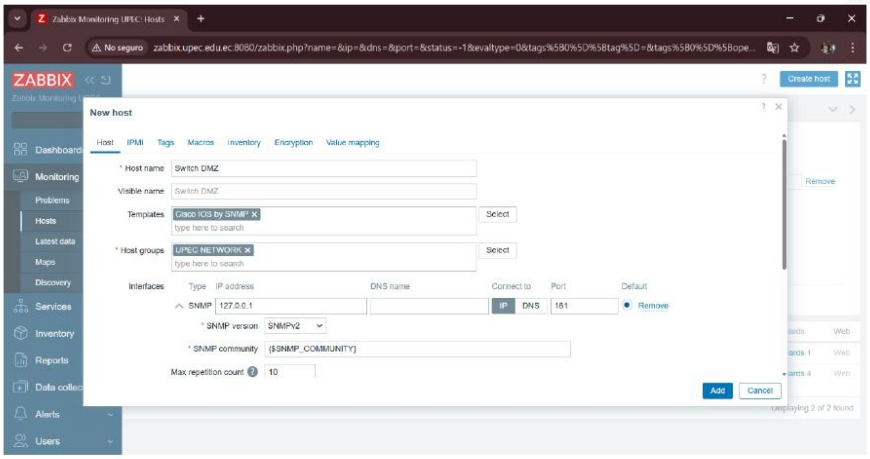
4. Configuración del nuevo host

Al abrirse la ventana de creación de host, se deben completar varios campos esenciales.

4.1. Datos generales del host

En la pestaña “Host”, completar los siguientes campos:

- **Host name:** Es el nombre con el cual se identificará el dispositivo dentro de Zabbix.
  Ejemplo: Switch DMZ.
- **Visible name:** Puede colocarse el mismo nombre del host o una descripción más detallada.
- **Templates:** Se selecciona la plantilla correspondiente al tipo de equipo que se va a monitorear.
  Para un switch Cisco se utiliza la plantilla “Cisco IOS by SNMP”.
- **Host groups:** Este campo permite organizar el dispositivo dentro de un grupo. Ejemplo: UPEC NETWORK.



4.2. Configuración de la interfaz SNMP

La interfaz SNMP es fundamental, ya que define la manera en que Zabbix se comunicará con el dispositivo.

Los campos deben completarse de la siguiente manera:

- **Type:** Seleccionar SNMP.
- **IP address:** Colocar la dirección IP del dispositivo a monitorear. Ejemplo mostrado: 172.20.1.3.
- **DNS name:** Dejar vacío si no se utiliza DNS.
- **Connect to:** Seleccionar IP.
- **Port:** Mantener el valor por defecto, 161.
- **SNMP version:** Seleccionar SNMPv2.
- **SNMP community:** Ingresar la comunidad configurada previamente en el equipo. Ejemplo: UPEC-SNMP.
- **Use combined requests:** Mantener activado si aparece disponible.

Una vez completados todos los datos, hacer clic en el botón “Add”.

5. Verificación del funcionamiento

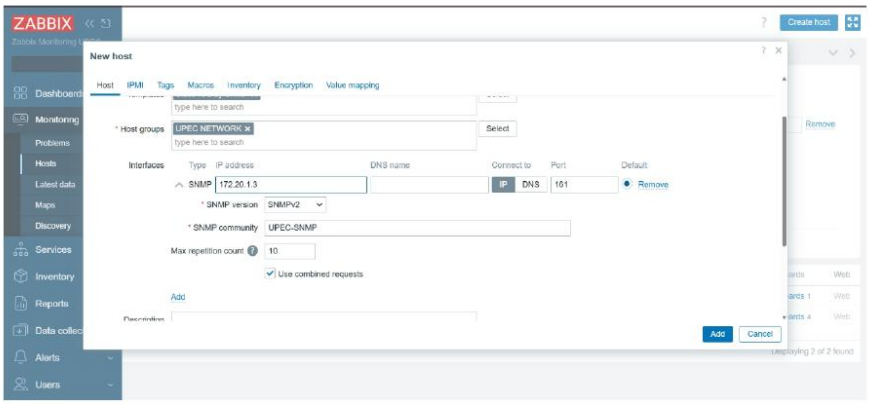
Después de agregar el dispositivo, es necesario confirmar que Zabbix está recibiendo información correctamente.

Para ello:

1. Ir al menú “Monitoring”.
2. Seleccionar “Latest data”.
3. Elegir el host recién creado.
4. Verificar que aparezcan métricas como tráfico, estado de interfaces, uptime, y otros parámetros.

Si no se visualizan datos, se recomienda revisar:

- Que la comunidad SNMP sea la correcta.
- Que el dispositivo permita consultas SNMP desde la IP del servidor Zabbix.
- Que no existan bloqueos de firewall.
- Que la dirección IP del host esté correctamente configurada.



6. Observaciones importantes

- La plantilla seleccionada determina qué tipo de información recopilará Zabbix. Para equipos Cisco es necesario usar una plantilla SNMP compatible.
- Si el host no genera datos, es conveniente realizar una prueba de conexión SNMP desde consola, utilizando comandos como snmpwalk, para confirmar que la comunidad y la IP son correctas.
- Las comunidades SNMP deben mantenerse seguras, evitando el uso de nombres genéricos como “public” o “private”.

Créditos

Autora: Steffany Revelo

Tutor: Ing. Milton del Hierro Mosquera

Carrera: Ingeniería en Computación

Institución: Universidad Politécnica Estatal del Carchi (UPEC)

Año: 2025