PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR SEDE ESMERALDAS

ESCUELA DE INGENIERÍA EN SISTEMAS Y COMPUTACIÓN

TEMA:

CONTROL DE SERVICIOS DE RED Y SERVIDORES BASADO EN HERRAMIENTAS DE ADMINISTRACIÓN DE RED Y POLÍTICAS DE GESTIÓN DE CALIDAD

Previo a la obtención del título de Ingeniero de Sistemas y Computación

LÍNEA DE INVESTIGACIÓN

Redes y Desarrollo

AUTOR:

Cesar Saavedra Drouet

ASESOR:

Mgt. Cesar Godoy Rosero

Diciembre del 2017

Tesis de grado aprobada luego de haber dado cumplimiento a los requisitos exigidos, previo a la obtención del título de INGENIERO EN SISTEMAS Y COMPUTACIÓN.

TRIBUNAL DE GRADUACIÓN

Título: "CONTROL DE SERVICIOS DE RED Y SERVIDORES BASADO EN HERRAMIENTAS DE ADMINISTRACIÓN DE RED Y POLÍTICAS DE GESTIÓN DE CALIDAD**"**

Autor: CESAR ABRAHAM SAAVEDRA DROUET

Mgt. Cesar Godoy **f.-…….**

Asesor

Mgt. Juan Casierra **f.-…….**

Lector #1

Lector #2

Mgt. Fabián Martínez **f.-……**

Director de Escuela

Mgt. Xavier Quiñonez Ku **f.-……**

Ing. Maritza Demera Mejía **f.-……....**

Secretaria general PUCESE

Esmeraldas, Ecuador, noviembre 2017

DECLARACIÓN DE AUTENTICIDAD Y RESPONSABILIDAD

Yo, CESAR ABRAHAN SAAVEDRA DROUET portador de la cédula de identidad No. **0803287911 declaro** que los resultados obtenidos en la investigación que presento como tesis de grado, previo a la obtención del título de **"Ingeniero en Sistemas y Computación**" son absolutamente originales, auténticos y personales.

En tal virtud, declaro que el contenido, las conclusiones y los efectos legales y académicos que se desprenden del trabajo propuesto de investigación y luego de la redacción de este documento son y serán de mi sola, exclusiva responsabilidad legal y académica.

CESAR ABRAHAN SAAVEDRA DROUET

CI 0803287911

CERTIFICACIÓN

Cesar Godoy Rosero, docente investigador de la PUCE-Esmeraldas, certifica que:

El estudio de caso realizado por CESAR ABRAHAM SAAVEDRA DROUET bajo el título "CONTROL DE SERVICIOS DE RED Y SERVIDORES BASADO EN HERRAMIENTAS DE ADMINISTRACIÓN DE RED Y POLÍTICAS DE GESTIÓN DE CALIDAD" reúne los requisitos de calidad, originalidad y presentación exigibles a una investigación científica y que han sido incorporadas al documento final, las sugerencias realizadas, en consecuencia, está en condiciones de ser sometida a la valoración del Tribunal encargada de juzgarla.

Y para que conste a los efectos oportunos, firma la presente en Esmeraldas, 3 de diciembre de 2017.

Fdo. Mgt. Cesar Godoy Rosero

DEDICATORIA

Dedico todo el esfuerzo aplicado a este trabajo de investigación a mis padres, por ser los faros que guían mi destino en épocas tormentosas. ¡Padres, los amo!

Cesar Saavedra

AGRADECIMIENTO

Agradezco a Dios.

Agradezco a mis padres por apoyarme en el transcurso de mi vida académica

Agradezco a mis hermanos por darme siempre palabras de aliento frente a la adversidad.

Agradezco a mi novia por su apoyo incondicional y motivación para realizar este trabajo.

Cesar Saavedra

RESUMEN

Actualmente, las redes informáticas forman parte vital de las empresas y su administración garantiza la fluidez con la que se gestiona y accede a los datos. El monitoreo, control de equipos y servicios, permite conocer el estado de la red, el cual, en base a la respectiva planificación, permite prever a tiempo problemas de red, generando ahorro de recursos en la empresa. Esta investigación se realizó en el departamento de TIC de la PUCE sede Esmeraldas, para tal efecto, se aplicó la metodología descriptiva, utilizando técnicas cualitativas y cuantitativas bajo los métodos analítico e inductivo, esto permitió realizar un análisis del estado actual de la red utilizando herramientas de monitoreo, siendo la más óptima para el caso ZABBIX como software de información de seguridad y gestión de eventos (SIEM).

Palabras clave: Zabbix, network monitoring, monitoring tools

ABSTRACT

Currently, computer networks are a vital part of companies and their administration guarantees the fluidity with which data is managed and accessed. The monitoring, control of equipment and services, allows knowing the state of the network, which, based on the respective planning, allows to anticipate network problems in time, generating savings of resources in the company. This research was carried out in the ICT department of the PUCE headquarters Esmeraldas, for this purpose, the descriptive methodology was applied, using qualitative and quantitative techniques under the analytical and inductive methods, this allowed to perform an analysis of the current state of the network using tools of monitoring, being the most optimal for the ZABBIX case as security information and event management software (SIEM).

Keywords:, PUCE Esmeraldas, network, administration, protocol SNMP

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

Presentación de la investigación

La investigación se desarrolló bajo el tema “control de dispositivos y servidores basado en herramientas de administración de red y políticas de gestión de calidad y seguridad”, propone la implementación de un sistema para el monitoreo y control de dispositivos de comunicación de la Pontificia Universidad Católica del Ecuador Sede Esmeraldas a través de evaluar y comparar distintas herramientas en base a indicadores de calidad estandarizados.

Planteamiento Del Problema

Las redes de telecomunicaciones experimentaron un gran crecimiento en la década de los años 90, lo cual ha provocado que se preste una mayor atención al control y monitoreo por parte de los responsables de redes. Los problemas que ocurren en las horas picos, donde se incrementa el tráfico de la red y la carga de los servidores, provocando fallos en los servicios que estos ofrecen a sus usuarios, se han convertido en un inconveniente para los responsables de redes.

Las redes LAN son de gran importancia para una empresa, no solo para la conectividad que ofrece entre las áreas de la infraestructura sino también por los servicios que presta como son: acceso a información, impresiones, aplicaciones, correo, web, etc. El mayor problema que se encuentra en las redes LAN es su tamaño, mientras más grande sea la red más complicado es administrar y monitorear los enlaces y servicios de red que brinda.

Desconocer cuanto tráfico hay en el ancho de banda o que servicio está produciendo que la carga del servidor aumente, impide tener un rendimiento de red óptimo, debido a que un servicio web o un servidor pueden colapsar en cualquier momento sin que los responsables de redes estén enterados.

Otro inconveniente que puede ocurrir debido a un inadecuado monitoreo de las redes de comunicación es que los administradores de redes están obligados a moverse al punto donde se encuentra la falla, ocasionando que aumente la dificultad y el riesgo

del trabajo en los casos donde los equipos de comunicación están ubicados en lugares de difícil acceso, lo que produce que se pierda tiempo y recursos. Además, un monitoreo deficiente de la red combinado con un nivel de seguridad bajo, le da la posibilidad a los usuarios de realizar configuraciones en los dispositivos de comunicación de la institución, ocasionando posibles problemas en el funcionamiento de la red.

Para orientar de mejor manera el desarrollo de la presente investigación, se formulan a continuación las siguientes interrogantes:

- ¿Cuáles son los estándares que se debe cumplir para la gestión de calidad y seguridad de los servicios tecnológicos?
- ¿Cuáles son los servicios y servidores que serán administrados?
- ¿Qué indicadores deben ser tomados en cuenta al momento de administrar una red?
- ¿Qué herramienta es la más adecuada para la administración de red en la PUCESE?

Justificación

Desde que empezó la era del internet en los años 90, las redes informáticas se vieron en la necesidad de expandirse volviéndose más complejas, haciendo que la gestión de administración de las redes LAN sea más complicada conforme van creciendo, debido a esto se vuelve imprescindible la implementación de un sistema que permita monitorear el estado en el que se encuentra la red.

Este es el caso de la Pontificia Universidad Católica del Ecuador sede Esmeraldas la cual requiere de un servidor con el sistema de monitoreo con la intención de optimizar la red informática y sus equipos a través de la gestión de los dispositivos de comunicación.

Existen diversos tipos de sistemas de monitoreo; entre los cuales se encuentran los sistemas pagados, estos no se convierten en la primera opción de todas las organizaciones, debido a sus altos costos de licencias; otros solo se pueden utilizar bajo un equipo de comunicación específico como mikrotik o cisco, lo cual tiene el mismo problema de costos altos; por último están los de código abierto, estos

sistemas ofrecen funcionalidades similares a los otros tipos de sistemas pagados, además poseen una comunidad de soporte muy grande alrededor del mundo que se actualiza periódicamente.

Disponer de un sistema de monitoreo basado en SNMP (Simple Network Management Protocol) es muy eficiente porque permite, monitorizar los enlaces punto a punto y actuar cuando un indicador se active en el sistema, por ejemplo, bloquear un host que hace repetidas peticiones a un switch generando tráfico. Además, el sistema proporciona estadísticos que pueden ayudar al administrador de redes a corregir fallos, cuellos de botellas y dar mantenimiento a los servicios en los que ocurren más incidentes. Monitorizar los recursos de un CPU (carga del microprocesador, memoria, disco duro etc.).

Los beneficios que se obtendrán de esta investigación serán de gran ayuda para la red informática de la universidad, lo cual permitirá alcanzar una optimización de la infraestructura de red.

La PUCESE siendo una entidad que proporciona servicios tanto al personal administrativo como académico, necesita garantizar disponibilidad de sus diferentes servicios a todos sus usuarios. Los beneficiarios directos son todas las personas que necesitan tener acceso a los recursos que ofrece la universidad, el departamento de TIC, y el administrador de red, debido a que esta investigación facilitará la gestión de la red.

Objetivos

General

Analizar los dispositivos de comunicación y servidores de la infraestructura de red LAN de la PUCESE, mediante la aplicación de modelos de administración de red para establecer la herramienta que más se ajustan a los requerimientos institucionales.

Específicos

- Describir la infraestructura y requerimientos de la administración de la red LAN para conocer sus características e indicadores en las herramientas de monitoreo.
- Clasificar los recursos tecnológicos que componen la red LAN de la PUCESE para el proceso de la monitorización.
- Establecer la herramienta que se ajuste a los requerimientos de monitoreo y control de redes LAN en la PUCESE.

CAPÍTULO 1

MARCO TEORICO

1.1. Antecedentes

Con el rápido desarrollo de la tecnología de redes de computadoras, las redes internas de las grandes y medianas empresas han ido creciendo cada vez más, esto hace que sea necesario buscar una forma eficaz de monitorizar y administrar dispositivos de red, existen varios softwares administradores de red, herramientas que ayudan a los responsables de redes a gestionar los dispositivos de red.

Un software de administración de red es un sistema encargado de la monitorización, control y gestión de los diferentes equipos de comunicación de la red. La mayoría de los sistemas que realizan administración de red poseen herramientas que permiten al usuario obtener diferentes datos de los objetos de monitoreo como: visualizar y analizar el tráfico que pasa por el ancho de banda, disponibilidad de un host o servicio, uso de memoria, disco o CPU. En estudios realizados por investigadores que utilizaron la herramienta CNAM afirman que:

> CNAM (Administrador de Computadoras y Redes Activas) es una aplicación de gestión de redes que ayuda a las grandes empresas y a los proveedores de servicios de pequeñas y medianas empresas a gestionar sus datas centers e infraestructura de TI de manera eficiente y rentable. CNAM recopila información sobre todos los componentes de hardware de los instrumentos de comunicación que están en la red. (Arman, Khashayar, & Suhaimi, 2014, p.1).

Existe una amplia oferta de sistemas de monitoreo, ya sean open sourse o sistemas privados, además se puede contar con personas que poseen amplios conocimientos sobre programación y protocolos de comunicación de red que han desarrollado sus propios sistemas de monitoreo, como es el caso del sistema TASPAS realizado por un grupo de investigadores donde concluyeron que:

> Una solución flexible para el monitoreo es mediante el uso del framework de servicios TAPAS para sistemas adaptables. La función de supervisión es

> realizada por dos niveles, administradores de monitoreo y agentes SNMP (Simple Network Manager Protocol). Los principales administradores de monitoreo controlan los gerentes de monitoreo intermedio que se comunican con los agentes SNMP ordinarios. (Patcharee & Finn, 2010, p.79).

Algunas herramientas de monitoreo están desarrolladas de tal forma que puedan ser utilizadas incluso por personas que poseen poco conocimiento en administración de red. Este es el caso de la herramienta SAGE2 que fue desarrollada y desplegada para monitorear los recursos de un laboratorio en la universidad de Illinois en Chicago, y se comprobó que usuario sin amplios conocimientos de protocolos de red podían monitorear y administrar las funciones con las que contaba la herramienta (Bharadwaj, Flores, Rodriguez, Long, & Marai, 2016). Se puede notar que algunas herramientas optan por desarrollar sus interfaces y configuraciones lo más simple posible para ayudar a los usuarios que no poseen un conocimiento profundo sobre la administración de red.

Los sistemas de monitorización de redes por lo general utilizan una combinación de varios protocolos de red para obtener datos de los objetos que monitorean, uno de estos protocolos es SNMP. El mismo fue creado con el objetivo de resolver problemas de gestión de red como monitoreo, control y configuración el cual puede dividirse en dos partes, la estación de administración y las MIBs (Management Information Base) que son base de datos utilizados por el SNMP que contienen información de los equipos de comunicación, según estudios realizados por investigaciones anteriores afirman que:

> SNMP primero recopila datos para la interacción de inicio entre los equipos en el data center específico, para recopilar estos datos SNMP necesita solicitarlo a los MIBs que sirven como una base de datos para la información almacenada. (Arman, Khashayar, & Suhaimi, 2014, p.2).

Un aspecto importante para la resolución de problemas de red es que los sistemas de monitoreo usen métodos para control en tiempo real ya que, estos permiten conocer el estado de equipos críticos para la organización con la finalidad de atender los problemas en el momento que se estén suscitando.

El método que se suele usar para un monitoreo en tiempo real es polling. Este método se basa en ejecutar mensajes periódicos de peticiones y respuesta de los diferentes elementos de red, por otro lado, el método polling puede crear tráfico excesivo al momento de realizar los mensajes de petición y respuesta. Kwang, Jin, & Jin (2007). El nivel de tráfico generado por la estación de administración es importante a la hora de seleccionar una herramienta de administración.

Al ver este inconveniente Kwang, Jin y Jin (2007) desarrollaron una estrategia de monitoreo en tiempo real basada en SNMP que produce menos tráfico de red causado por el administrador de red. Este consiste en que cada agente decida cuando reportar a la estación de administración.

En los casos donde los niveles de tráfico causado por la estación de administración son muy altos, se puede sustituir un modelo basado en SNMP por un modelo de agente móvil, que posee una administración de red distribuida. (Pugazendi & Duraiswamy, 2009) en su investigación sobre alternativas de monitoreo de redes refiere que los agentes móviles se mueven a los lugares donde los datos son almacenados y seleccionan la información que quiere el usuario. Ellos descentralizan el proceso y el control y por consecuencia, reducen el tráfico alrededor de la estación de administración y distribuyen la carga del proceso. Esta alternativa es muy conveniente en redes que no poseen un ancho de banda de red muy potente. Al final de su investigación Pugazendi & Duraiswamy (2009) concluyo:

> Se ha encontrado que el uso de agentes móviles en el monitoreo de la red no sólo reduce la sobrecarga en la red, sino que también aumenta la eficiencia del proceso de monitoreo en gran medida siempre que se eligen mecanismos apropiados. Nuestro modelo ha dado mejores resultados. (p.579).

Otra alternativa al monitoreo de red tradicional basados en SNMP es el uso de servicios web especializados en monitoreo de red. Esta opción fue puesta en comparación con los sistemas basados en SNMP y se encontró que es una mejor opción cuando se intenta recuperar más de un dato de los agentes, que los sistemas basados en SNMP (Pras, Van de Meent, & Quartel, 2004).

Otros estudios proporcionan información sobre cómo realizar mediciones de tráfico SNMP a gran escala con el fin de desarrollar una mejor comprensión de cómo este

protocolo se utiliza en las redes de grandes empresas Jurgen, Aiko, Matus, Jorrit, & Remco (2007) ya que el desempeño de la red afecta directamente a la comunicación de las personas que trabajan dentro y fuera de una empresa, y cualquier perturbación en el proceso de producción cambia directamente al resultado final.

1.2. Bases teórico científico

1.2.1. Servicios de red

A pesar de que los verbos monitorizar y monitorear se crearon a partir del sustantivo monitor, ambos términos son acciones vinculadas a la vigilancia y control, su definición más general menciona la supervisión y el análisis con el objetivo de asegurar el correcto funcionamiento de algo (Diccionario panhispánico de dudas, 2005). La necesidad de mantener todo bajo control es uno de los principios fundamentales de la administración.

Si no existen mecanismos de control en una organización, no se podrá saber de ninguna manera cual es la situación actual de la empresa y por lo tanto se afectará de manera directa a la toma de decisiones y el rumbo de la misma.

La búsqueda por evaluar el desempeño está orientada a la mejora continua en cualquier tipo de gestión, sobre todo en cuanto a tecnología de la información se refiere, pero el correcto desempeño de TIC requiere la aplicación de prácticas y estándares que se ajusten a los objetivos de mejora.

Entre las prácticas internacionales más utilizadas para gobierno de TI se encuentra la Biblioteca de Infraestructura de Tecnologías de la Información más conocida como ITIL

> "ITIL es un estándar de facto introducido y distribuido por la Oficina de Comercio Gubernamental en el Reino Unido e incluye todas las áreas de TI en las organizaciones" (Sahibudin, Sharifi, & Ayat, 2008)

ITIL es el enfoque de gobierno de tecnologías de la información más utilizado a nivel mundial ya que proporciona orientación sobre como diseñar y manejar los servicios de TI que consume la organización (Sahibudin, Sharifi, & Ayat, 2008)

Todas las disciplinas de ITIL interactúan entre sí, una de ellas está relacionada con garantizar que el servicio este cuando el usuario lo necesite, esta disciplina es la

Gestión de la disponibilidad (Ritchie s.f). Al ser la conectividad un servicio que presta la universidad, una de las prioridades de la institución es mantener el servicio de red sin interrupción alguna, para asegurar la satisfacción de los usuarios.

Se llama servicio de red al conjunto de computadoras conectadas en una misma red y comparten datos y recursos a través de esta. Por el tamaño de la red se clasifican en redes WAN para empresas grandes que poseen más de un edificio conectado, redes LAN que son implementadas en organizaciones pequeñas, y redes MAN que son redes de área metropolitana y están desplegadas a lo largo de una ciudad, y poseen grandes velocidades de ancho de banda.

Los servicios de red suelen ser instalados en servidores, los cuales generalmente poseen mejores características en comparación a un host común, debido a que estos servidores manejarán las peticiones realizadas por los equipos conectados a la red.

Entre los servicios de red más comunes está el servidor DHCP (Protocolo de Configuración Dinámica de Host), este protocolo se encarga de aliviar la carga del host resolviendo la configuración de TCP/IP de manera automática. Así mismo, se tiene el protocolo SNMP el cual ya ha sido anteriormente mencionado en esta investigación, este protocolo es usado comúnmente para establecer comunicación entre los elementos de red. Además de estos servicios de red, existe el servicio DNS (Sistema de Dominio de Nombres), El mismo se encarga de resolver los nombres de los sitios web para que el navegador pueda entenderlos. Sin este servicio de red solo se podría navegar usando las direcciones IP de las páginas web más no su alias (www.) (Mifsud & Lerma , 2013)

1.2.2. Administración de red

La administración de redes consiste “asegurar un óptimo funcionamiento de las principales operaciones de la red, realizando supervisión y control, aplicando sistemas de administración, aplicaciones o dispositivos” (Case, Fedor, Shhhoffstall, & Davin, 1990).

Las principales funciones de red son aquellas que dan soporte directamente a los requerimientos del usuario. Permiten que el usuario acceda a la red y se encargan del intercambio de datos del usuario.

De la misma forma que las redes han tenido un aumento exponencial desde la década de los 70 hasta el 2017, la administración de estas ha ganado importancia debido a que una buena administración puede provocar que el rendimiento de la empresa aumente. Gracias a esto y a la dificultad de administrar todos los componentes y recursos que conforman una red, la organización internacional de estándares (ISO) desarrollo un modelo de administración de redes (ISO 10164), bajo la dirección del grupo OSI (Open System Interconnection) el cual consta de cuatro sub modelos (Cisco Systems, 2003). Entre estos sub modelos está el sub modelo funcional, este modelo está conformado por cinco áreas funcionales, donde especifica los principales funcionamientos de los sistemas de administración de redes

- Administración de fallas
- Administración de estadística
- Administración de configuración
- Administración de rendimiento
- Administración de seguridad

Las funciones de gestión específicas, dentro de estas áreas funcionales, son proporcionadas por mecanismos de gestión OSI. Muchos de los mecanismos son generales en el sentido de que se utilizan para cumplir con los requisitos en más de un área funcional. Del mismo modo, los objetos gestionados son generales en el sentido de que pueden ser comunes a más de un área funcional. En la tabla 1, se propone una síntesis de las investigaciones de diferentes autores (Brad, 2003), (Cisco Systems, 2003). (Clemm, 2007), sobre las áreas funcionales del modelo de administración de redes, los cuales coinciden en tomar como base la ISO 10164 para el desarrollo de sus trabajos.

El monitoreo y control de red son aspectos ligados e importantes para la administración de redes, porque a través de estas operaciones se consiguen las funciones específicas de las áreas funcionales. Clemm (2007) refiere que las áreas funcionales de administración, fallas y estadística son administraciones ligadas a las

características del monitoreo y las áreas funcionales de configuración y seguridad son contenidas en las funciones de control.

Áreas funcionales	Descripción	Funciones específicas de administración
Fallos	Engloba errores de detección, aislamiento y la corrección de funcionamiento anormal.	• Mantener y examinar registro de errores. • Aceptar y actuar sobre notificaciones de detección de error. • Rastrear e identificar errores. • Llevar a cabo secuencias de pruebas de diagnóstico. • Corregir errores.
Estadística	El objetivo de la gestión de la contabilidad es medir los parámetros de utilización de la red para que los usuarios individuales o de grupo en la red puedan ser regulados adecuadamente	• Recolección de datos de uso. • Informar a usuarios de costos incurridos o recursos consumidos. • Permitir establecer límites a las cuentas y horarios de tarifas asociados al uso de recursos. • Permitir combinar costos cuando múltiples recursos son invocados para logar dar una comunicación objetiva.
Configuración	La gestión de la configuración identifica, ejerce control sobre, recopila datos y proporción de datos a sistemas abiertos con el propósito de prepararse para, inicializar, comenzar, proporcionar funcionamiento continuo y terminar los servicios de interconexión.	• Establecer los parámetros que controlan los funcionamientos rutinarios de los sistemas abiertos. • Asociar nombres a los objetos administrados y al conjunto de objetos administrados. • Inicializar y cerrar objetos administrados. • Recopilar información sobre la demanda de la condición actual de los sistemas abiertos. • Obtener avisos de cambios significativos en la condición de los sistemas abiertos. • Cambiar la configuración de los sistemas abiertos.
Rendimiento	Su objetivo es medir y evaluar el rendimiento de la red para verificar que el sistema se comporta como se espera, a través de la definición de la calidad del servicio.	• Obtener información estadística. • Mantener y examinar registros del estado del sistema a través del tiempo. • Determinar el rendimiento del sistema en condiciones naturales y artificiales. • Alterar los modos de operación del sistema con el propósito de realizar actividades de gestión de rendimiento.
Seguridad	Su objetivo es controlar el acceso a los recursos de la red dando soporte a las políticas de seguridad de las aplicaciones.	• Crear, detectar o controlar los servicios y mecanismos de seguridad. • Distribuir la información relevante de la seguridad. • Reportar eventos relevantes de la seguridad.

Tabla 1 Resumen de las áreas de funcionamiento

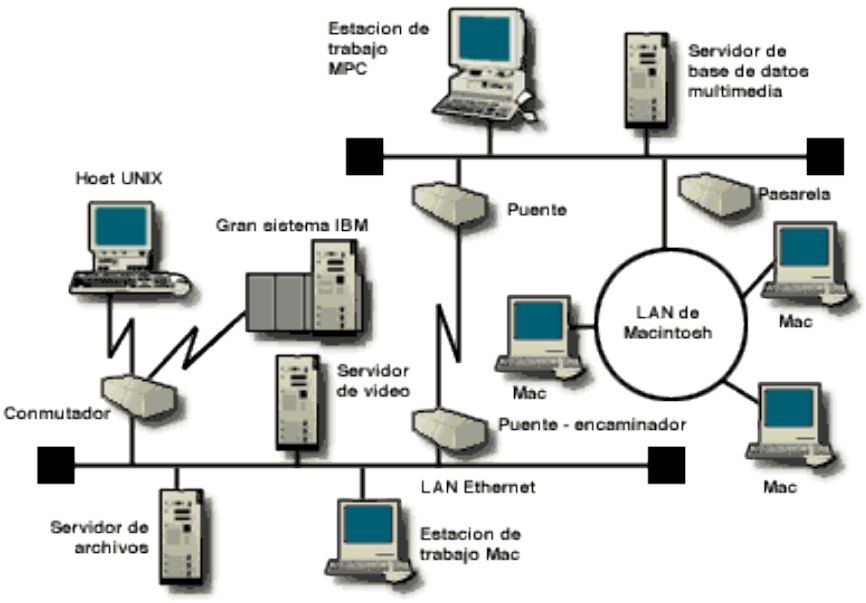
1.1.1.1. Monitoreo de red

El monitoreo de red se define como la acción de estudio en la recopilación de información a la hora de predecir un problema en la red. Por lo tanto, se lo puede comparar con un algoritmo, ya que predice y resuelve un problema siguiendo una secuencia lógica, el monitoreo sistematiza y da una solución eficaz y óptima. Debido a esto, algunas empresas mencionan:

> Hoy en día se utilizan como uno de sus principales recursos de operación a las computadoras, especialmente si están conectadas en red. Debido a ello, la confiabilidad y velocidad de la red de la empresa es crucial para que un negocio sea exitoso. Los administradores de red tienen que asegurarse que la red esté funcionando, sea confiable y veloz, así como que sea utilizada eficientemente. Para lograr todo esto es necesario monitorear la red. (Mogu, 1990).

Cuando se monitorea la red se deben tomar en cuenta los diversos elementos que serán monitorizados, los cuales pueden ser: servicios de red, hosts, servidores y equipos de comunicación como switchs, routers, accesspoint.

Ilustración 1 Equipos de Comunicación



Fuente: (IBM, 2014)

Los servidores son equipos con características especiales diseñados para soportar aplicaciones de control que devuelve una respuesta acorde a las peticiones del usuario o cliente, por tanto, son elementos esenciales dentro de la red, según (Robert, 2009) afirma:

> Los servidores corren aplicaciones críticas, así como servicios TI tal como correo electrónico, archivo, servicios de impresora y base de datos, disponibilidad y rendimiento de tus servidores. Los registros de eventos contienen la información más importante para diagnosticar aplicaciones y fallas del sistema operativo, determinando la vitalidad y estado de tu sistema y verificar que el sistema y las aplicaciones estén operando correctamente.

Estos equipos al ser de gran importancia para la organización deben tener alto desempeño en el manejo de seguridad y de las herramientas funcionales, para evitar crear errores o que la estructura de red colapse el sistema integrado en el servidor, por lo que según Gartner (2004) afirma:

> Las penetraciones más dañinas a un sistema de seguridad en una compañía a menudo provienen de agentes internos, El estudio manifiesta que el 70% de los incidentes de seguridad que en realidad causan perdidas a una organización involucra miembros de esta. Teniendo Firewalls y antivirus puedes protegerte de hackers del mundo exterior pero no ayudará contra ataques generados dentro de la empresa. La única manera de proteger un sistema de tales ataques es monitoreando los registros de servidores y auto generar alertas en tiempo real.

Además de los servidores también se pueden monitorizar equipos (o hosts) que se encuentran conectados a la red y consumen servicios de red. El control de estos dispositivos ayuda a detectar cuantos recursos de la red está consumiendo cada host, además se puede detectar la cantidad y el tipo de tráfico que genera.

Para realizar un monitoreo completo de red se deben tomar en cuenta los switchs y routers debido a que estos funcionan como la estructura principal de la red, brindando conectividad a todos los hosts de la organización. Es de gran importancia monitorear estos dispositivos, porque a través de estos pasa el tráfico que se genera en los hosts y servidores.

1.1.1.2. Control de red

El control de red es un proceso considerado activo en comparación con el monitoreo que se asocia a procesos pasivos. El control toma los resultados del monitoreo y realiza acciones en función de estos, funciones como gestionar el ancho de banda, logs de firewall Ips entre otras. Dichas acciones son orientadas a la administración de configuración y seguridad de la red.

En el área de administración de la seguridad las acciones de control se despliegan al establecer de manera correcta las políticas que rigen las ACL (Access Control List). Liu, Torng, & Meiners (2012) refiere que las ACL proveen seguridad a las redes privadas controlando todo el flujo de los paquetes que entran y salen entre una red privada y el internet, a traves de una secuencia de reglas. Cada paquete es comparado con las reglas y estas deciden que hacer con él. Se debe tomar en cuenta si existen conflitos al declarar reglas para no tener problemas de admininstracion.

1.2.3. Protocolos de administración de red

Los protocolos de administración de red fueron creados para administrar los dispositivos y diagnosticar los problemas de la red. Brad (2003) afirma:

> Los protocolos fundamentales de red son Internet Control Message Protocol (ICMP) y SNMP. Estos dos protocolos son útiles como herramientas básicas para solucionar problemas y administrar redes. (p.90)

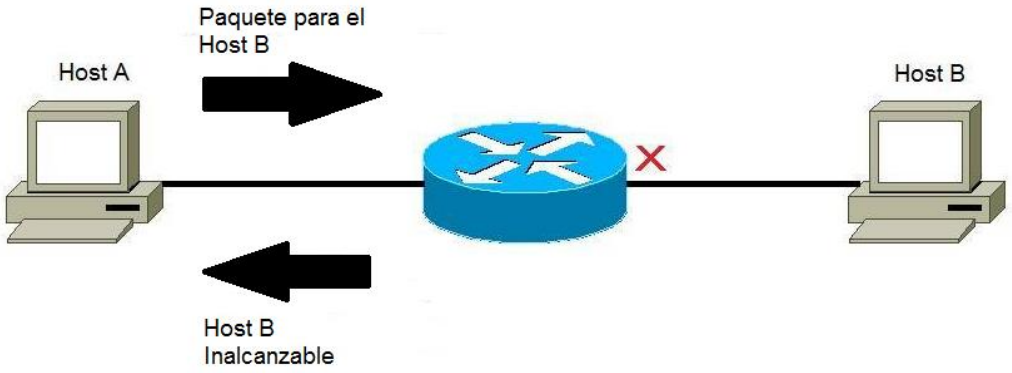
ICMP crea una solicitud y una respuesta de bajo nivel que garantiza la conectividad básica entre dos puntos finales de red. Mientras que, SNMP va un paso más allá. Eleva ese nivel de datos recopilados mediante la habilitación de dispositivos para compartir su configuración básica y métricas integradas.

Estos protocolos de red son utilizados por los sistemas de administración para realizar monitoreo de red.

1.1.1.1. Protocolo ICMP

El protocolo ICMP es uno de los principales protocolos de internet en administración de redes. Se utiliza para enviar mensajes de error a través de la red, además estos mensajes no llevan datos sobre aplicaciones, sino información propia del estado de la red. ICMP también es utilizado para detectar errores en las comunicaciones, disponibilidad de hosts, congestión de red y latencia.

Ilustración 2 Ejemplo del uso de ICMP



Fuente: (Autor)

Según la RFC 792 los mensajes ICMP son enviados en varias situaciones; por ejemplo, cuando los datos no pueden llegar a su destino, cuando un dispositivo de comunicación no tiene la suficiente cantidad de buffer para reenviar un paquete de datos y cuando un dispositivo de comunicación puede dirigir a un host para enviar tráfico en una ruta más corta.

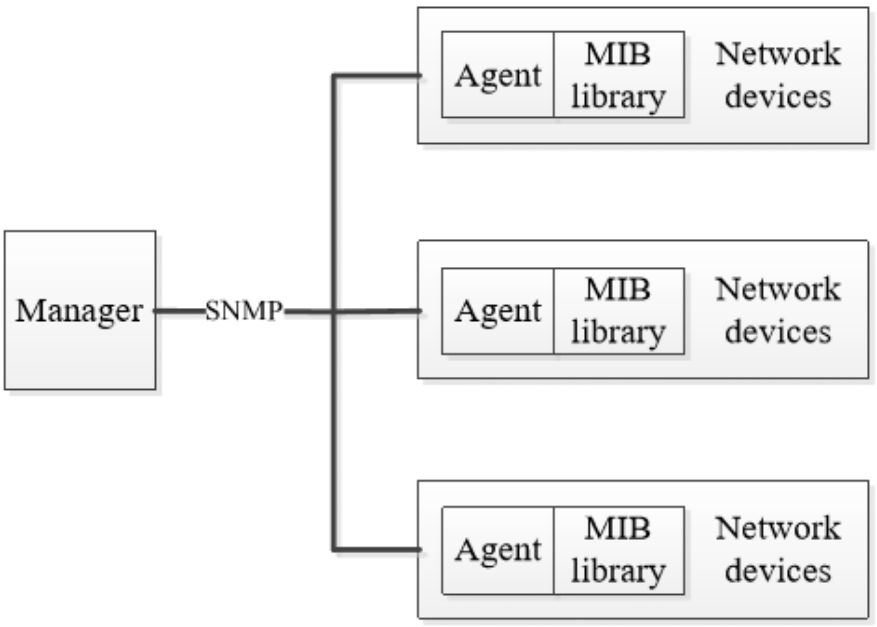
1.1.1.2. Protocolo SNMP

El protocolo SNMP fue diseñado bajo la necesidad de tener un control de los diferentes dispositivos que se encuentran en una red, estos pueden ser switchs, routers, host (entre otros), para lo cual utiliza una comunicación entre los dispositivos para obtener información del estado del equipo.

Según la RFC 1157 referente al protocolo SNMP define que su modelo de arquitectura es una colección de estaciones de administración y elementos de red. La estación de administración no es más que la ejecución de una aplicación para gestionar el control y monitoreo de los elementos de red. Los elementos de red son dispositivos como host, servidores o dispositivos de comunicación que tendrán un agente responsable de realizar las funciones de gestión de red solicitada por la estación de administración de red.

El protocolo SNMP es usado para gestionar la comunicación entre las estaciones de administración de red con los agentes en los elementos de red (Case, Fedor, Shhhoffstall, & Davin, 1990). Como se muestra en la ilustración 3 el administrador se comunica con todos los agentes instalados en los dispositivos que se encuentran en la red obteniendo así una administración centralizada.

Ilustración 3 Diagrama de la arquitectura SNMP



(Liang, Weifeng, & Wang, 2013)

La funcionalidad del protocolo SNMP puede ser dividido en dos partes, el protocolo en sí y la base de información gestionada (MIB). Existe un tercer elemento, la interface de usuario. Sin embargo, este elemento es estrictamente una implementación específica y no está definido en la RFC.

Las MIBs son las bases de datos que utiliza el protocolo SNMP para conocer las propiedades de los elementos de red. Por cada elemento de red se dispone de un objeto de representación y el conjunto de estos objetos forman la base de información gestionada. La estación de administración de red lee y configura los valores de los objetos de los MIBs.

El uso de las MIBs es requerido para el funcionamiento de la estación de administración de red, en investigaciones realizadas sobre las MIBs han determinado que estas deben ser clasificadas y categorizadas en un árbol jerárquico de objetos (Arman, Khashayar, & Suhaimi, 2014). Esto permitirá tener un acceso más eficiente para la estación de administración de red.

El método que utiliza el protocolo SNMP para enviar y recibir información de los MIBs y del estado de los dispositivos, es a través de los diferentes tipos de mensajes (PDU). Los PDU están contenidos en los paquetes que envían el administrador y los agentes a través de la red, además de los mensajes PDUs, el paquete contiene la versión del protocolo SNMP que se está usando, y el nombre de la comunidad que es usada para la autentificación. Para realizar esta comunicación entre los agentes y el administrador el protocolo SNMP utiliza el servicio UDP (User Datagram Protocol), el cual es un servicio no orientado a la comunicación (Chunkyun, 2012), por tanto, no genera mucha carga adicional a la red, puesto que el servicio UDP no añade bits adicionales para confirmar el envío y recepción de paquetes.

Los mensajes que utiliza el protocolo SNMP han ido evolucionando junto con las versiones del mismo protocolo. Así, SNMPv1 presentó solo cinco mensajes para el intercambio de información que son: GetRequest, GetNextRequest, GetResponse, SetRequest, y Trap. SNMPv2 implemento los mensajes GetBulkRequest e InformRequest.

GetBulkRequest es una alternativa al mensaje GetNextRequest con la adición de poder transmitir grandes cantidades de datos. Por otro lado, InformRequest además de cumplir una función similar al mensaje Trap, añadiendo la funcionalidad de reenvio si el origen no recibe una respuesta por el informe. SNMPv3 no realiza ninguna configuración sobre los mensajes del protocolo.

GetRequest

Esta PDU es utilizada por el administrador y pregunta por valores de algunas variables de la lista VarBindList, además sus parámetros error-status y error-index siempre son 0, asimismo siempre espera una respuesta del agente con el PDU Get Response. Si el agente no puede dar un valor a todas las variables solicitadas no se generará la respuesta.

GetNextRequest

Este PDU al igual que el GetRequest es solo utilizada por el administrador y espera una respuesta del agente tipo Get Response. La PDU consiste en obtener valores de la siguiente instancia del objeto en un orden lexicográfico de la tabla de objetos del agente. Es utilizado comúnmente para recorrer y obtener todos los valores de una tabla.

GetResponse

La operación GetResponse es utilizada solo por los agentes y esta varía dependiendo del tipo de petición que reciba del administrador (GetRequest, GetNextRequest, SetRequest etc).

SetRequest

Es utilizado por el administrador para modificar el valor de algunas variables contenidas en la lista VarBindList del agente. Para realizar la modificación el administrador envía el valor al lado de la variable a modificar.

GetBulkRequest

Se implementó a partir de la versión 2 del protocolo SNMP y fue diseñada para obtener toda la información de las tablas de los agentes de una manera más rápida y eficiente que en comparación con GetNextRequest.

El protocolo SNMP utiliza el puerto UDP 161 para enviar peticiones al agente, el cual enviará su respuesta por el puerto de origen. El administrador recibirá notificaciones del tipo trap e InformRequest por el puerto UDP 162

Entre los mensajes del protocolo SNMP, el mensaje Trap es utilizado para el reporte de eventos. Según (Lago, Mera, & Medina) SNMP tiene dos diferentes tipos de PDUs Trap, uno definido por SNMPv1 y otro por SNMPv2, los cuales están compuestos por tres partes principales: una cabecera de autentificación, una cabecera PDU y una lista de variables enlazadas, que sirven para proporcionar información adicional de la causa del problema.

La cabecera PDU de los mensajes tipo Trap e InformRequest son diferentes del resto de PDUs. Debido a que contiene información detallada del mensaje Trap, como el tipo genérico de Trap, el cual tiene siete distintos tipos de información que son:

- Cold start (0)
- Warm start (1)
- Link down (2)
- Link up (3)
- Authentication failure (4)
- EGP neighbor loss (5)
- Enterprise (6)

Además, la cabecera PDU contiene información como el tiempo transcurrido entre la re inicialización del agente y la generación del Trap, el cual está definido en la sección Timestamps. Así como el tipo. (Patcharee & Finn, 2010)

Para recopilar información desde el equipo de red puede utilizar dos técnicas: roll polling y el informe de eventos. Roll polling es un proceso de solicitudes y respuestas entre el administrador de red y el agente. Los administradores pueden consultar el comando y envió a sus agentes dentro del ámbito de la autorización y la solicitud de todo tipo de valor de la información, el agente será la información en el MIB como una respuesta. Para el monitoreo en tiempo real, los administradores realizan peticiones constantes a los agentes sobre los datos y el estado de la red.

El informe del evento es iniciado por el agente, los administradores de monitoreo tienen el rol de recibir la información. El agente puede tener un ciclo regular o predefinido, también es posible cuando eventos importantes o eventos anormales toman la iniciativa de generar informes, que son muy efectivos para el monitoreo en

tiempo real. Para el estado o el valor de los cambios relativamente pequeños en el objeto supervisado puede ser más eficiente que el sondeo de roll polling.

Roll polling y el informe de eventos son los métodos de monitoreo de red más eficaces, sin embargo, para diferentes sistemas de gestión, ambos tienen distintos énfasis. El sistema de gestión de telecomunicaciones utiliza más informes de eventos en comparación con la gestión SNMP la cual no depende estos. En la gestión del sistema OSI es más probable encontrar un punto de equilibrio entre los dos métodos, haciendo que la selección puede basarse en lo siguiente:

- El tráfico de datos de red generado por cada método
- El retardo requerido
- Soporte a la aplicación de supervisión de red

Desde la creación del protocolo SNMP en el año 1990 hasta la actualidad, el protocolo ha pasado por varias versiones hasta llegar a la actual (SNMP v3). Cabe mencionar que con cada versión se han corregido algunos aspectos, como es el caso de la versión 3, donde su principal mejora fue la seguridad, incluyendo la autentificación, el control de acceso y la privacidad. SNMPv3 no trata de reemplazar a las versiones anteriores, en cambio puede considerarse como un conjunto de herramientas adicionales para trabajar en junto con las anteriores versiones.

1.2.4. Gestión de calidad de los servicios de red

El ministerio de tecnología de la información y la comunicación (MinTIC) de Colombia ha desarrollado algunas políticas enfocada a la calidad y seguridad que deberían cumplir los servicios tecnológicos brindados desde la administración de TI/SI. Entre estas políticas para la presente investigación, se tomaron las que involucran a la administración de la red, las cuales son:

Tener el control de los consumos de los recursos compartidos por los servicios tecnológicos, y como medida para llevar este control menciona las acciones de monitorear, identificar y controlar el nivel de consumo de los recursos compartidos y administrar su disponibilidad.

Otra política que emplean es la gestión preventiva de los servicios tecnológicos, a través de un monitoreo de la infraestructura que genere alertas preventivas de acuerdo con la configuración de los indicadores que se tengan definidos. Esta medida ayudara a realizar una planificación de red más eficiente al distribuir el tráfico de red evitando cuellos de botella.

Como tercera política para la calidad y seguridad de los servicios tecnológicos está el monitoreo de la seguridad de la infraestructura, que pide implementar medidas de control sobre los accesos, modificación o perdida de la información que afecten a la disponibilidad y la integridad de la información.

Además de las políticas que sugiere MinTIC se implantaron algunas medidas de ITIL y Quality of Service (QoS) como bases para determinar los criterios de evaluación de las herramientas de monitoreo.

Una de las metodologías utilizadas para realizar esta investigación fue el marco de referencia ITIL, el cual incorpora en su ciclo de vida del servicio la fase de diseño, esta fase es la responsable de crear o renovar los servicios prestados, además de detallarlos y garantizar que estos se acoplen a las estrategias pre definidas. La fase de diseño utiliza varias gestiones para asegurarse de cumplir su objetivo, entre estas gestiones se encuentra la gestión de la disponibilidad, por medio de ella se garantiza que los servicios estén habilitados cuando se los necesite. Según (Luque, 2015) "La Gestión de la Disponibilidad es esencial para asegurar la provisión de los Niveles de Servicio correctos, y así impactar positivamente en los objetivos del Negocio"

La gestión de la disponibilidad es un aspecto fundamental dentro de las instituciones, según (Ritchie, s.f.) existen tres principios básicos para lograr una buena gestión de la disponibilidad:

- "La Disponibilidad es esencial para el negocio y para la satisfacción de los usuarios"
- "Reconocer incluso que cuando las cosas fallan aún se puede lograr la satisfacción tanto del cliente como del negocio"
- "La mejora de la Disponibilidad sólo puede empezar después de entender cómo los Servicios TI apoyan a la empresa"

Desde un punto de vista genérico, se entiende a la red como un servicio que brinda TI y este servicio debe acoplarse al concepto del ciclo de vida del servicio que propone ITIL y en especial a la fase de mejora continua, valiéndose de mediciones y métricas para la constante evaluación.

Una de las formas que ITIL propone para evaluar un servicio, son los KPIs o indicadores claves de rendimiento por sus siglas en inglés (Key Performance Indicators) estos indicadores proporcionan una manera de constatar que el proceso marcha exitosamente. Uno de los KPIs diseñados para la gestión de la disponibilidad menciona el número de interrupciones en el servicio, lo que supondría que el objetivo de esta métrica es mantener la cantidad resultante lo más cercana a cero. (Min, Zhiheng, & Weiping, 2011).

Tabla 2 KPI Gestión de la disponibilidad

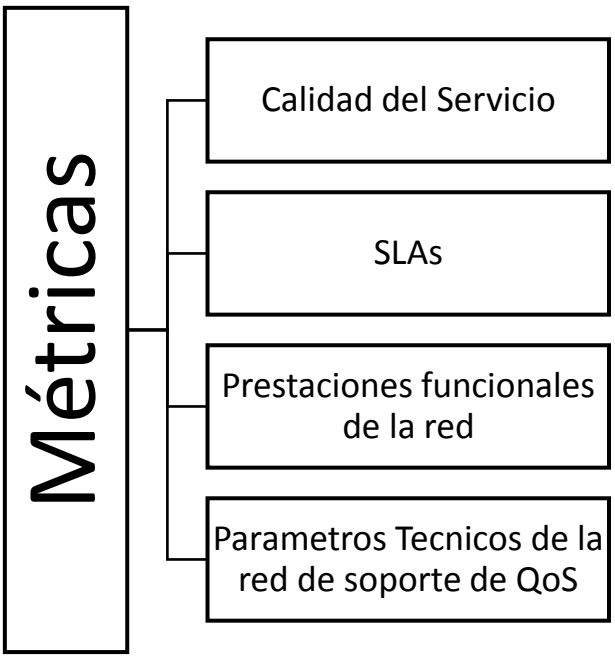
KPI	Descripción
Disponibilidad de servicio	Disponibilidad de servicios en relación con la disponibilidad acordada en los SLA's y OLA's
Cantidad de interrupciones de servicio	Cantidad de interrupciones de servicio
Duración de interrupciones de servicio	Duración media de interrupciones de servicio
Monitorización de disponibilidad	Porcentaje de servicios y componentes de infraestructura sujetos a monitorización de disponibilidad
Medidas de disponibilidad	Cantidad de medidas implementadas con el objetivo de aumentar la disponibilidad
Número total de incidencias	Porcentaje de incidencias ocurridos en un periodo de tiempo

Fuente: (Luque, 2015)

Otra forma encaminada a la mejora del servicio es el mecanismo QoS o Calidad del servicio por sus siglas en ingles Quality of Service, este mecanismo es utilizado específicamente en los servicios de red, Según el IETF RFC 2386 el QoS es un "Conjunto de requisitos del servicio que debe cumplir la red en el transporte de un flujo", la calidad del servicio enmarca todos los elementos que componen una red, los usos tradicionales de este método son el control de gestión de redes, planificación y la ingeniería de tráfico, además de brindarle garantías al consumidor final. (Romero, 2010). También se suele referir a QoS como un cúmulo de tecnologías que brinda herramientas para la administración de red.

De la ilustración 4 podemos enmarcar que QoS dentro de sus principios de medidas, requiere de la definición del acuerdo de nivel de servicio (SLA), debido a que en este se detallan las prestaciones que ofrece dicho servicio, lo cual es de vital importancia para poder garantizar que se brinda un servicio de calidad. Otro beneficio de la declaración del SLA es que nos permite medir las prestaciones estipuladas y obtener parámetros esenciales que pueden ser monitorizados.

Ilustración 4 Métricas QoS



Fuente: (Romero, 2010)

La table 3 asocia los parámetros de calidad a una categoría principal. Todas las categorías y parámetros que ofrece QoS están enfocadas a cubrir los sub modelos de la administración de redes.

Tabla 3 Parámetros QoS

Categoría de QoS	Parámetros de QoS
Tiempo	Latencia
	retraso
	Tiempo de recuperación
	Garantía
Volumen de trafico	
	Intervalos de sincronización disponibles
	Tiempo de iniciación Throughput
	Picos de volumen
Precisión	Precisión de direccionamiento
	Tasa de erros
	Integridad
Robusteza	Confianza
	Mantenibilidad
	Resistencia
	Supervivencia
Contabilidad	Costos
	Auditabilidad
Manejabilidad	Monitorizabilidad
	Control
Seguridad	Autenticación
	Confiabilidad
	Seguridad del tráfico de flujo

Fuente: (Romero, 2010)

Muy cercana a la misión del mecanismo QoS para la calidad del servicio, se encuentra la ISO 27002 la cual provee practicas encaminadas a la seguridad de la información y que dentro de sus once clausulas contiene el control de acceso, necesario para evitar y controlar los accesos no autorizados a la red.

1.2.5. Herramientas de monitoreo de red

Un sistema eficaz de monitoreo de red debe cubrir todos los aspectos de una red, incluyendo tiempo de respuesta, disponibilidad, tiempo de actividad y seguridad. Esto hace que la supervisión de la red sea una tarea difícil y exigente. Los administradores de red se esfuerzan constantemente por mantener el buen funcionamiento de sus redes. "Si una red estuviera abajo incluso durante un pequeño período de tiempo, la productividad dentro de una compañía se reducirá; Y en el caso de los departamentos de servicio público, la capacidad de prestar servicios esenciales quedaría comprometida" (Brad, 2003). Para ofrecer servicios proactivos, los administradores deben optimizar el flujo de datos y el acceso en un entorno complejo y cambiante. Por lo tanto, estos sistemas pueden ayudar a identificar actividades específicas y métricas de rendimiento, generando resultados que permiten a una empresa atender una variedad de necesidades, incluyendo el cumplimiento de requisitos, la eliminación de amenazas de seguridad interna y proporcionar una visibilidad más operativa.

Los sistemas de monitoreo también pueden definirse como elementos que implementan en una red de destino. "Verifica periódicamente la disponibilidad y el estado de cada nodo y enlace. En el caso de que haya algún problema o que algunos elementos no estén disponibles, notificará automáticamente a la persona responsable " (Clemm, 2007). En algunos casos es posible gestionar activamente la red utilizando el sistema de monitorización. También podemos definir las maneras que se utilizarían en un caso en que un nodo definido como critico no esté disponible. Pero depende del tipo de sistema de monitoreo que se esté utilizando. Analizando los sistemas de monitoreo podemos clasificarlos en tres tipos.

a. Sistema de monitoreo básico

Estos sistemas usualmente trabajan con el protocolo ICMP. "Estos sistemas periódicamente comprueban sólo un estado del elemento en vista y son capaces de proporcionar información acerca de la disponibilidad sólo en el nivel disponible o no disponible o posiblemente añaden una información sobre la respuesta temporal" (Drake, s.f.). Este tipo de sistemas de monitoreo es adecuado solo para redes LAN pequeñas.

b. Sistema de monitoreo avanzados

Este tipo de sistema trabaja con más protocolos como SNMP y SSH. Este factor permite a los sistemas ver prácticamente toda la información de los dispositivos conectados a la red como el estado de los servicios que está corriendo, uso de los recursos del sistema, el tráfico que generan entre otros. Con los hosts, los sistemas de monitoreo requieren de instalar agentes que obtienen datos que no están disponibles a través de los protocolos.

c. Sistema de monitoreo proactivos

Son sistemas avanzados que tienen la capacidad de administrar dispositivos de la red. Permitiendo al administrador la posibilidad de implementar scripts que se ejecutan en respuesta de un evento predefinido. Este tipo de sistemas son utilizados en entornos con niveles altos de automatización como, data centers, redes extensas, clúster de alta disponibilidad entre otros.

Algunos wjemplos de herramientas bien conocidas de monitoreo de red de código abierto son Nagios, Icinga 2, Pandora FMS, Shinken, OpenNMS, Hyperic.

Nagios es un software de monitoreo de red de código abierto que es ampliamente utilizado por los administradores de red, ISPs, gobiernos, así como grandes empresas, como Yahoo, Amazon, Google. Nagios ha demostrado ser escalable para una gran red con hasta 100.000 hosts y 1.000.000 de servicios. Además, ha recibido varios premios de las comunidades de Linux y redes.

Nagios es muy flexible y configurable. Las principales tareas de Nagios son monitorear el estado de los dispositivos de red y sus servicios y notificar a los administradores del sistema cuando se han encontrado problemas. El núcleo del motor de Nagios es un planificador que examina regularmente los dispositivos de red especificados y sus servicios. Cuando ocurren problemas, Nagios alerta a los administradores de red a través de canales de notificación como correo electrónico y servicio de mensajes instantáneos. Los administradores pueden abrir la interfaz web para buscar la información de estado, los registros de eventos y los informes desde cualquier lugar a través de Internet.

Nagios posee dos versiones disponibles: Nagios Core la cual es totalmente gratis y limitada, esta se encuentra en su versión 4.x.x y Nagios XI que es una versión pagada con muchas funciones adicionales.

Pandora FMS Es un software de monitoreo de red de código abierto al igual que nagios esta dispone de varias versiones: la versión community que es totalmente gratis, y dos versiones pagadas (NMS y Enterprice) entre ellas la versión Enterprice es la más completa, Pandora tiene además la capacidad de generar alertas.

Icinga 2 es un sistema de monitoreo de código abierto que verifica la disponibilidad de sus recursos de red, notifica a los usuarios de interrupciones y genera datos de rendimiento para la generación de informes.

Escalable y extensible, Icinga 2 puede monitorizar entornos grandes y complejos en múltiples ubicaciones.

Icinga 2 está bajo los términos de la Licencia Pública General GNU Versión 2, lo que indica que es totalmente gratuito y no posee una versión pagada.

Shinken es un marco de monitoreo de código abierto escrito en Python bajo los términos de GNU Affero General Public License. Fue creado en el 2009 como una simple prueba de concepto de un parche de Nagios. El primer lanzamiento de Shinken fue el 1 de diciembre de 2009 como simple herramienta de monitoreo. Desde la versión 2.0 (abril de 2014) Shinken se describe como un marco de monitoreo debido a su alto número de módulos.

Según (Aryachandra , Fazmah, & Novian, 2016) la debilidad de los sistemas de monitoreo es la administración de la seguridad, pues este apartado requiere de mayor atención para su completa cobertura. Es en estos casos donde se presentan los IDS (Sistemas de detección de intrusos) para cubrir esta área de la administración de las redes.

1.2.6. Indicadores de monitoreo

Los indicadores de monitoreo están enfocadas a cubrir las funciones específicas del modelo de administración de red. Los administradores se enfrentan a la forma de elegir los indicadores de rendimiento adecuados, la selección de indicadores de datos de la red relacionados con una variedad de factores, Según (Yongqi, Yun, Yaihao, & Liying, 2013) los indicadores más utilizado de la mayoría del sistema de monitoreo de

red son básicamente los mismos, el rendimiento, la utilización y la tasa de pérdida de paquetes.

El rendimiento se refiere a la velocidad de los datos enviados a través de la red, es decir, los indicadores orientados a la aplicación, generalmente representados como bits por segundo (bps), el número de bytes por segundo (Bps) o el número de paquetes por segundo (pps). Su fórmula es:

Rendimiento = bytes/times
Número de bytes transmitidos / en un intervalo de tiempo

La tasa de utilización es la frecuencia del uso de recursos de red, es más refinado que el indicador de rendimiento. Se utiliza para buscar cuellos de botella potenciales de la red y el área de la congestión, también se puede conocer qué recursos no se han utilizado totalmente. A través del análisis de la gestión de la red puede encontrar que recurso es más utilizado, ajustar la planificación de la red, equilibrar la carga y el uso eficaz de los recursos. Haciendo referencia a los gestores de resultados se puede ajustar todos estos parámetros.

La utilización de la interfaz es el principal indicador de la utilización de la red. El estado operativo de la interfaz se puede lograr mediante el seguimiento de la tasa de utilización, la tasa de utilización se puede expresar en porcentaje con respecto al ancho de banda, como el número de bytes que fluye la interfaz. Los cálculos se realizan utilizando la colección de variables de grupo de interfaces, la fórmula es la siguiente:

$$\text{IfUtilizatinRate} = \frac{(\triangle\, ifInOctets + \triangle\, ifOutOctets)\ x\ 8\ x\ 100}{(\triangle\, t)\ x\ ifSpeed}$$

Dónde: ∆t es el intervalo de tiempo, ∆ifInOctets es el número de entradas de las colecciones de bytes, ∆ifOutOctets es el número de salidas de colecciones de bytes, ifSpeed es la velocidad de transmisión de la interface.

La Utilización de la CPU refleja el equipo ocupado y desempeña un papel importante en el descubrimiento de la congestión de la red y el equilibrio de la carga de la red. Sin embargo, la Utilización de la CPU no está definida en la MIB pública, en su mayoría son variables privadas definidas por el proveedor.

Según (Luque, 2015) ITIL en su fase de diseño, dentro de los KPI de la gestión de disponibilidad se encuentra la duración de interrupción de servicio, el cual se relaciona con los paquetes perdidos en la red. La pérdida de paquetes en ocasiones es una señal de un funcionamiento de red anormal, por lo que la tasa de pérdida de paquetes es otro indicador importante de la monitorización de la red.

Para obtener los paquetes perdidos de un intervalo de red es necesario saber el tráfico que pasa por la red. El cual puede ser obtenido a través de algunos programas especializados como DU Meter, NetWorkx o utilizando los métodos del protocolo SNMP.

Según (Romero, 2010) para garantizar que exista calidad de servicio (QoS) en la red son necesarios diversos parámetros como: disponibilidad, ancho de banda, perdida de paquetes, round trip deley y jitter

Tanto ITIL como QoS poseen el parámetro de disponibilidad del servicio como un indicador de gran importancia, debido a que permite conocer el porcentaje está disponible en un intervalo de tiempo en la red. ITIL propone la siguiente fórmula para el cálculo de la disponibilidad.

$$\%disponibilidad = \left(\frac{A - B}{A}\right) X100$$

Donde A es el número de horas que el servicio está disponible. B es el número de horas que el servicio está inactivo (caídas del sistema, errores de aplicaciones, mantenimiento no planeado). El resultado de la fracción es multiplicado por 100 para obtener el resultado en porcentaje.

Además de estos indicadores que ayudan a realizar una evaluación de las diversas herramientas de monitoreo de red, también hay que tomar en cuenta algunas funcionalidades o características adicionales con las que deberían cumplir para que sean más completos, algunas investigaciones realizadas mencionan las siguientes características: capacidad de guardar y analizar históricos, monitorización remota, creación de informe y envió de los mismos, posibilidad de ofrecer la monitorización con o sin agente, que la herramienta no solo sirva para monitorizar redes y que disponga de una API.

1.2.7. Método para evaluar la calidad del software de monitoreo

Teniendo en consideración que la calidad es el principal objetivo en la elaboración de todo producto, y que el desarrollo de un software en parte es comparado con una construcción, es necesario mencionar alguna estandarización para poder comprobar, analizar y evaluar su calidad.

> Uno de los estándares considerados en esta investigación fue la ISO 9126 la cual se centra en la calidad del software. La norma ISO 9126 presenta dos partes, la primera es el modelo de calidad para tratar la calidad externa e interna, y la segunda es el modelo de calidad uso para tratar la calidad en uso además de establecer un modelo de calidad y uso como marco para la evaluación de software. En esta norma se distingue entre calidad interna y calidad externa, y se introduce también el concepto de calidad en uso (Vargas, 2016)

En la investigación realizada por (Abud Figueroa, 2006) son seis las características puntuales que dicta la ISO 9126 para determinar la calidad de un software. Lógicamente entre esas características se encuentra la funcionalidad y la usabilidad, es decir constatar que las funcionalidades del software logren satisfacer todas las necesidades del cliente y si este es simple y fácil de entender, la rapidez y el uso de recursos de manera correcta reciben el nombre de eficiencia y conforma la tercera característica, seguido por la confiabilidad, portabilidad y mantenibilidad que responden al rendimiento, el traspaso de un ambiente a otro y la facilidad de modificación respectivamente.

Entre los principales beneficios de utilizar cualquier tipo de estándar internacional, está la garantía de tener una guía para realizar lo que deseamos, de hecho, los estándares sirven para tener metas claras, o un estado mínimo al cual se debe llegar para ser bueno o superar para ser el mejor. El objetivo de utilizar la ISO 9126 en esta investigación, fue poder definir el mejor software de monitoreo de redes en base a normas internacionales.

CAPÍTULO 2

METODOLOGÍA

2.1. Descripción del lugar

La presente investigación se realizó en el departamento de TIC de la PUCE sede Esmeraldas, específicamente en las instalaciones principales de la institución, en el primer periodo del 2017. En el indicado departamento, trabajan siete personas las cuales aportaron con información para realizar la investigación, con la finalidad de obtener un sistema administrador de red que se ajuste a los requerimientos de la institución.

La organización cuenta con una gran variedad de dispositivos que estarán sometidos al monitoreo, los cuales se detallan

Tabla 4 Dispositivos

Dispositivos	Cantidad
• **Cámaras IP**	14
• **Servidores**	7
• **Routers**	20
• **Switchs**	70
• **Host**	307
	418

2.2. Tipo de investigación

Esta investigación es de tipo cuantitativa y cualitativa, porque se utilizaron técnicas de recolección de información como la entrevista y observación para luego por medio

de técnicas estadísticas obtener valores numéricos que ayuden a la toma de decisiones, según investigadores:

La investigación cualitativa es aquella donde se estudia la calidad de las actividades, relaciones, asuntos, medios, materiales o instrumentos en una determinada situación o problema. La misma procura por lograr una descripción holística, esto es, que intenta analizar exhaustivamente, con sumo detalle, un asunto o actividad en particular (Lamberto, s.f.)

Este tipo de investigación se adecuó al trabajo realizado, apoyándose en el análisis de las diferentes herramientas de monitoreo para determinar en base a indicadores cuál de estas se ajusta a las necesidades de la infraestructura de redes de la PUCESE. Además posee características de una investigación cuantitativa debido a que existen variables medibles como el tráfico generado en la red, y como este afecta a la selección de una herramienta de monitoreo, según (Carlos, 2011) determino en su investigación que la metodología cuantitativa parte de cuerpos teóricos aceptados por la comunidad científica con base en los cuales formula hipótesis sobre relaciones esperadas entre las variables que hacen parte del problema que se estudia.

En este estudio, se utilizó la investigación aplicada y la investigación descriptiva basada en la observación de los objetos sin intervenir en su funcionamiento, debido a que se desplegará el conocimiento para la solución de los problemas previamente observados y analizados. Así mismo, se aplicará una investigación exploratoria gracias a que la definición de las variables de tema se realizó por medio de investigación en libros, medios electrónicos y artículos científicos que se enfoquen en la administración de redes y monitoreo.

Se realizó una investigación de campo debido a que se implementará la técnica de la observación para la recolección de datos que ayudará a determinar las variables de estudio.

2.3. Métodos y Técnicas

2.3.1. Métodos

Desde que el hombre apareció en la tierra ha intentado entender el origen del mundo, empezando desde cada una de sus partes primarias, intentando comprender el origen y la composición del mismo y todos los fenómenos que parten del universo. Los griegos son los precursores en el afán de entender los elementos primarios, como el fuego, el agua, el aire y todo lo que de origen a lo existente. (Lopera, Ramírez, Zuluga, & Ortiz, 2010)

El análisis como medio para conocer la realidad que rodea al hombre ha sido utilizado como método de supervivencia, y la descomposición de esta realidad general en realidades más básicas para su comprensión, este método ha constituido la forma de resolución de problemas desde la antigüedad.

"El análisis y la síntesis desempeñan un importante papel en el proceso de la cognición humana y se dan en todos los estadios de la misma" (Rosental y Ludin, 1979, p. 11). En la presente investigación se implementó el método analítico debido a que se realizó un estudio detallado de los problemas que se presenten en la red, relacionados a los distintos elementos de red, para de esta manera establecer los puntos que requerirán de una mejora.

"El método inductivo se conoce como experimental y sus pasos son:1) Observación, 2) Formulación de hipótesis, 3) Verificación, 4) Tesis, 5) Ley y 6) Teoría" (Newman, 2006). Basado en estas premisas se manejará el método inductivo debido a que se utilizará la observación y los demás pasos del método inductivo para desarrollar una propuesta que permita corregir el problema de esta investigación.

2.3.2. Técnicas

Para la recolección de los datos se aplicó la técnica de la entrevista; la cual fue enfocada al área de redes del departamento de TIC de la PUCESE, con el objetivo obtener una visión amplia del estado y las necesidades de dicha red.

Además, se utilizó la observación para analizar la administración actual de la red y su relación con la disponibilidad de los servicios.

Selección de los sistemas de monitoreo

Para seleccionar los sistemas que se sometieron a evaluación se tomó en cuenta los siguientes aspectos:

- **Usabilidad**
- **Tipo de sistemas de monitoreo (avanzados o proactivos)**
- **Interfaz gráfica web**
- **Gratuidad**
- **Disponibilidad y accesibilidad del mercado**

Tomando en cuenta estos aspectos se seleccionaron los siguientes sistemas de monitoreo:

- **Pandora FMS**
- **Nagios**
- **Icinga**
- **Zabbix**
- **Paessler**

2.4. Población

Para desarrollar la investigación se consideró como población el personal del área de redes del departamento de TIC de la PUCESE, el cual está conformado por el jefe del departamento y tres asistentes; por lo tanto, debido a que la población es muy pequeña, no hay la necesidad de aplicar la técnica del muestreo.

2.5. Descripción del instrumento

Los datos obtenidos de la entrevista fueron analizados rigurosamente elaborando una síntesis con puntos claves para la presente investigación; las respuestas de los datos obtenidos a través de la aplicación de este instrumento incluyeron preguntas específicas y relevantes considerando inquietudes propias sin dejar de lado los objetivos claros de la entrevista.

La ficha de observación se creó a partir de un análisis de las 5 áreas funcionales en relación con la investigación realizada por Cesar Godoy, con la finalidad de que la observación estuviera relacionada a la problemática de este estudio y así poder obtener la disponibilidad de los servicios de la red de la institución.

2.6. Descripción de las técnicas de procesamiento y análisis

Los datos obtenidos por las entrevistas fueron rigurosamente analizados por el investigador, y comparados con estándares que deben cumplir los elementos de red, para determinar los indicadores esenciales que van a ser controlados por la herramienta de monitoreo.

2.7. Normas éticas

Los datos o credenciales de los elementos de red que se proporcionen al investigador para la implementación de la herramienta de monitoreo no serán divulgados bajo ningún concepto.

La información contenida en la presente investigación es de exclusiva responsabilidad del investigador; es decir que las citas expuestas en este trabajo están debidamente referenciadas tomando en cuenta la normativa APA.

CAPÍTULO 3

RESULTADOS

2.1. Análisis e interpretación de resultados de la entrevista

Según la Universidad Internacional de Andalucía los departamentos de TIC o tecnologías de la información y comunicación son los encargados de dar soporte a los procesos administrativos, brindando a toda la organización los medios tecnológicos necesarios para cumplir sus objetivos. En la Pontificia Universidad Católica del Ecuador Sede Esmeraldas la misión del departamento de TIC no es muy diferente a la de los departamentos en las grandes empresas, pero la mayor diferencia radica en que este departamento, debe estar orientado a cumplir la meta principal de la institución, que es la excelencia académica.

Gracias a la entrevista formulada al jefe del departamento de TIC, se pudo conocer las principales funciones de esta área de la institución, las cuales son:

- Instalación y soporte de dispositivos de conectividad
- Soporte técnico al área administrativa y al cuerpo docente y al área academia
- Desarrollo y soporte de servicios web

En lo que se refiere al área de red la institución está conformada por 170 switch de los cuales 90 son administrables y cinco servidores principales que bajo tecnología Docker brindan 60 aplicaciones que suministra el departamento de TIC de las cuales 50 son creadas en la universidad y 10 son adaptadas a las necesidades de la PUCESE utilizando frameworks.

Analizando las respuestas de la entrevista, se identificó que utilizan el sistema The DUDE que es un software complementario que Mikrotik brinda como ayuda para monitorizar la red, pero debido a sus limitaciones funcionales como generación de

alertas, funcionamiento con traps, reportes entre otros, no cumple con todas las necesidades que requiere la institución.

A demás la institución se divide en una red administrativa y una académica, la red administrativa provee de servicios a trabajadores y cuerpo docente, mientras que la red académica brinda conexión a los estudiantes, estas redes realizan la conexión de los diferentes dispositivos en las instalaciones principales. La universidad está conectada por medio de una fibra óptica que parte desde el data center ubicado en el edificio principal en el departamento de TIC, hasta una bodega al lado de las escaleras en el edificio de aulas.

Otro aspecto que surgió al aplicar la técnica de investigación fue la falta de información cuando ocurre un error relacionado a la conectividad en el departamento de TIC, lo que provoca que el tiempo de respuesta para solucionar un problema sea mayor. Reduciendo el rendimiento de los servicios de red.

2.2. Comparación entre estándares de calidad y objetivos de administración de la PUCESE

Como se ha mencionado en repetidas ocasiones a lo largo de esta investigación, el monitoreo y el control son aspectos de suma importancia para la prosperidad de cualquier organización. En cuanto a tecnologías de la información se refiere, las redes juegan un papel protagónico, porque proveen de servicios vitales para las comunicaciones. Es por esta razón que las redes no deben estar exceptas a la administración, palabra que engloba a las actividades de monitoreo y control.

Uno de los estándares mayormente utilizado para la administración de red es el ISO 10164 el cual provee un modelo de administración basado en áreas funcionales que garantiza que al ser cumplidas se conseguirán los objetivos del departamento de TIC en cuanto a la administración de redes.

Tabla 5 Relación entre ISO 10164 y Requisitos de sistemas de monitoreo de la PUCESE

AREAS FUNCIONALES	FUNCIONALIDADES	DESCRIPCION DE FUNCIONALIDADES
Administración de fallos	Alertas	Capacidad del sistema de notificar a través de SMS o correo al encargado de redes cuando un host, switch o servicio este caído o sus valores de medición se encuentren fuera de lo establecido
	Traps	Capacidad del sistema para manipular traps de los objetos de monitorización
Administración de estadística	Ancho de banda	Capacidad del sistema para monitorizar el ancho de banda de que pasa por determinado segmento de red
Administración de rendimiento	Ancho de banda	Capacidad del sistema para monitorizar el ancho de banda de que pasa por determinado segmento de red
	Histórico	Capacidad del sistema para almacenar los datos obtenidos de los objetos de monitorización por determinado periodo de tiempo.
	Reportes	Capacidad del sistema para generar y personalizar los reportes de los objetos

		monitorizados.
	Graficas	Capacidad del sistema para presentar gráficas personalizables con información de los objetos de monitoreo
Administración de seguridad	ACL	Configurar servidor de control de accesos
	Detección de intrusos	Capacidad del sistema para detectar y registrar cuando se ingrese a los objetos de monitoreo

Fuente: Autor

La tabla 4 representa las áreas funcionales de la administración de redes, según la ISO 10164 y como estas áreas se compenetran con los requerimientos que según el jefe del departamento de TIC deben ser cumplidos por el sistema que se encargue de administrar la red en la institución.

Entre las áreas funcionales destaca la administración de rendimiento, y esta a su vez se relaciona con la guía QoS, porque a través de los parámetros que ofrece, busca medir el rendimiento promedio de una red, para asegurar la calidad de la misma.

Cuando aparece la palabra guía, es imposible no mencionar al marco de referencia ITIL y la meta de este estándar, dirigido a asegurar la calidad de servicio. Uno de los resultados de esta investigación fue determinar la relación existente entre algunos aspectos de ITIL y administración de red, principalmente enfocándose en la gestión de la disponibilidad y gestión de la capacidad que se alinea a la administración de red en cuanto al área funcional administración de fallos y las interrupciones del servicio.

Tanto ITIL como QoS recomiendan la definición de un SLA entre proveedor y consumidor del servicio. En esta investigación se pudo constatar que la universidad no tiene delimitado un SLA con el departamento de TIC como proveedor de la disponibilidad del servicio de red, ni con terceros (ISP).

2.3. Análisis de la administración de red en la PUCESE

Según la interpretación de los datos obtenidos mediante la ficha de observación se pudo concluir que, en la Pontificia Universidad Católica del Ecuador Sede Esmeraldas, ocurren 49 incidentes relacionados con la administración de red en una semana.

Los cuales están divididos en 20 incidentes relacionados con el uso de impresoras en red, 6 asociados a los routers, 10 a los switchs, 8 conciernen a las cámaras ip y finalmente 5 de servidores, dando un promedio de 9.8 incidencias en un día

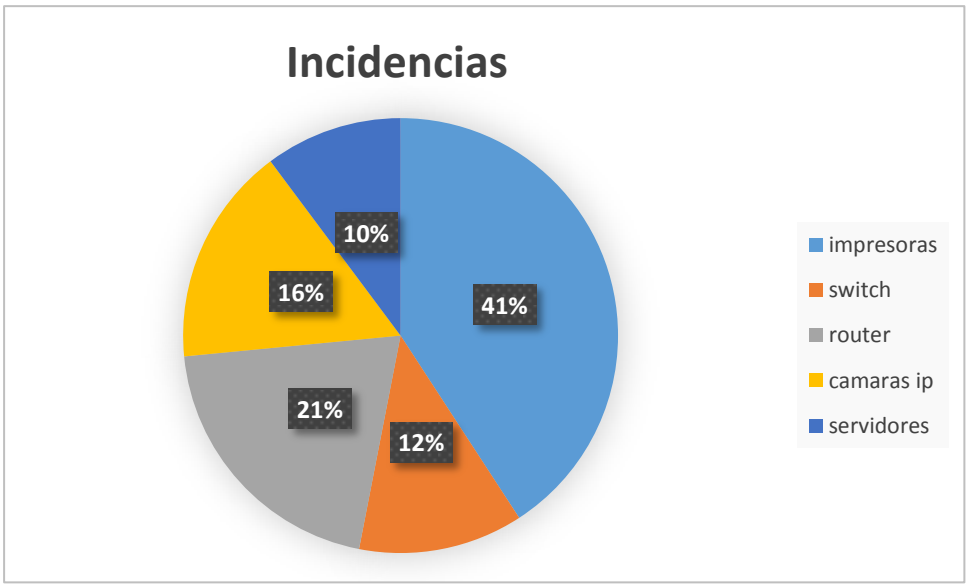


Ilustración 5 Grafico de incidencias de los dispositivos

Tabla 6 Resumen ficha de observación

Descripción	Día 1	Día 2	Día 3	Día 4	Día 5
Total de incidencias de red	14	9	12	8	6
Tiempo de respuesta	16	12,5	19,7	19	11
Total de incidencias Resueltas	8	7	10	7	6
Número de horas que el servicio está disponible (red) (12 horas)	49,3	55,3	51,1	52,8	56,5
Número de horas que el servicio está inactivo (red)	10,8	4,7	8,9	7,2	3,5

Fuente: Autor

Es importante mencionar que la disponibilidad es una relación entre el número de horas que el servicio está activo y el número de horas que este se encuentre inactivo, es así como, por ejemplo, un servicio que tenga muchas incidencias, pero su tiempo de respuesta y tiempo de resolución sean bajos, tendrá una disponibilidad muy alta en comparación con un servicio con menos incidencias, pero con tiempos con valores más altos. Los tiempos de inactividad para realizar el cálculo varían de acuerdo a las necesidades de la organización, y a lo que dicte el SLA, para el caso de esta investigación se consideró un servicio inactivo desde el momento que este falle para uno o más usuarios.

En este momento aparece la interrogante de cuál es el porcentaje ideal de disponibilidad para una organización, la respuesta a esta premisa la tiene ITIL y el concepto de alta disponibilidad el cual asegura un cierto grado de continuidad absoluta en la prestación de un servicio durante un periodo de tiempo determinado, el valor que de disponibilidad que se espera es del 99.9999%. (Min, Zhiheng, & Weiping, 2011).

Según la alta disponibilidad los valores obtenidos por el departamento de TIC de la PUCESE no son satisfactorios, pero cabe recalcar que llegar a la alta disponibilidad es una tarea compleja que no solo implica que no ocurran fallos, sino que se disminuyan tiempos de respuestas y por ende de inactividad

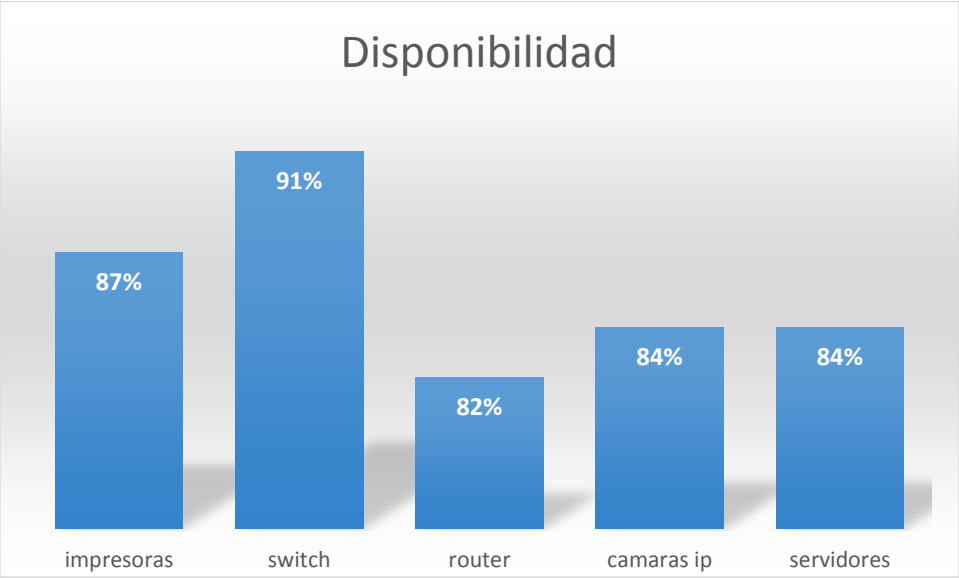


Ilustración 6 Disponibilidad de los dispositivos

Otro dato que se obtuvo de la observación fue que el departamento de TIC no cuenta con una persona encargada exclusivamente a la administración de las redes, estas funciones son repartidas entre todos los trabajadores del departamento, por lo que la segregación de las funciones resulta también en un tema a analizar.

2.4. Evaluación de herramientas en base a funcionalidades e ISO 9126

Para que el proceso de monitoreo de las redes se cumpla a cabalidad, el departamento de TIC se debe apoyar en herramientas que faciliten el cumplimiento de las funcionalidades que se mencionan en la tabla 4, pero no todas las herramientas en el mercado se adaptan a las necesidades de la institución, siguiendo esta premisa la elección de una herramienta debe ser un proceso sujeto a una metodología, previamente definida en esta investigación. Paso seguido se obtuvieron los siguientes resultados:

Síntesis de requerimientos funcionales de las herramientas de monitoreo Anexo 4

- **Pandora FMS**

  Pandora FMS en su versión gratis cumple, con la mayoría de las funcionalidades requeridas, para realizar la detección de intrusos la cual se asocia al análisis de logs es necesario adquirir la versión pagada de pandora

FMS (Pandora Enterprise). Pandora FMS no tiene soporte para ACL en ninguna versión.

- **Nagios**

  La versión gratuita de nagios (Nagios Core) trae una amplia gama de addons los cuales cubren la mayoría de las funcionalidades requeridas, con excepción de ACL y detección de intrusos, los cuales son soportados en la versión pagada de nagios (Nagios Log Server).

- **Icinga2**

  Incinga2 trabaja con una amplia variedad de addons que añaden funcionalidades al sistema base, los cuales cubren la mayoría de las funcionalidades que se requiere. Icinga2 no está orientado a trabajar con traps directamente, para conseguir esto se requiere instalar y configurar herramientas adicionales en el sistema operativo donde está instalado. Icinga2 no trabaja con ACL.

- **Zabbix**

  Zabbix es una herramienta muy completa totalmente gratis, limitaciones y cumple con todas las funcionalidades que se requiere para la red de la PUCESE.

- **Paessler**

  Paessler en su versión freeware la cual es totalmente gratis cumple con todas las funcionalidades que se requiere, pero esta versión solo permite tener hasta 100 sensores, para monitorear más objetos se necesita comprar una de sus licencias.

La misión institucional de la PUCE en el literal d busca: "garantizar a sus miembros la libertad académica, salvaguardando los derechos de la persona y de la comunidad dentro de las exigencias de la verdad y del bien común" (PUCE, 2016). Otro motivo para que la herramienta ganadora siga la filosofía del "bien común" enmarcándose en

el hecho de que una herramienta libre se ajusta más a propósitos científicos y que la distribución de copias de versiones mejoradas de la misma, es completamente legal.

La creación de destrezas y habilidades solo se forman con la práctica, la cual solo se consigue creando o adaptando. Las herramientas que faciliten su código fuente y que provean la cooperación de una comunidad de programadores tiene la finalidad de obtener un sistema robusto que cumpla con los requisitos de la empresa lo que para la PUCESE significara una contribución a la formación del cuerpo estudiantil.

Tomando como base la misión de la PUCE y la de la escuela de sistemas de la sede Esmeraldas, una de las características a tener en consideración para obtener la herramienta ganadora fue la gratuidad de esta, puesto que por razones presupuestarias y de ideología empresarial, una herramienta libre significaría disminución de costos y potencial de personalización en la herramienta para así ajustarla a los requerimientos institucionales.

Una vez obtenidas las herramientas, el proceso de selección se volvió menos complejo puesto que se utilizó la matriz que la ISO 9126 propone, obteniendo como herramienta ganadora a Zabbix con un puntaje de 90.

Tabla 7 Resumen de la matriz de evaluación

Característica	Pandora FMS	Nagios	Zabbix	Icinga	Paessler
Total Funcionalidad	16,00	17,00	19,00	17,00	19,00
Total Usabilidad	12,00	12,00	13,00	13,00	12,00
Total Fiabilidad	7,00	6,00	8,00	7,00	7,00
Total Eficiencia	7,00	8,00	9,00	7,00	8,00
Total Manteniabilidad	10,00	7,00	9,00	6,00	9,00
Total Portabilidad	16,00	14,00	18,00	15,00	17,00
Total Calidad de Uso	11,00	10,00	14,00	12,00	12,00
Total General	**79,00**	**74,00**	**90,00**	**77,00**	**84,00**

Fuente: Autor

Cabe recalcar que el puntaje que se le asigna a cada herramienta equivale a la suma de los valores de sub características previamente definidas en la ISO 9126 y la tabla completa se puede apreciar en el Anexo 3.

CAPÍTULO 4

DISCUSIÓN

Un estándar, es el conjunto de normas pre establecidas que sirven como modelo para llegar a un objetivo. Como en todas las ciencias del saber humano, en informática se aplican una serie de modelos y estándares internacionales para cada una de las diferentes áreas. Para la administración de redes destaca la ISO 10164 la cual propone un modelo detallado, en el que describe cinco áreas funcionales para la correcta gestión de redes, las cuales son: Administración de fallas, Administración de estadística, Administración de configuración, Administración de rendimiento, Administración de seguridad (Cisco Systems, 2003).

Según el análisis de los resultados, los sistemas de administración estudiados, en su totalidad, cubren una gran parte de las áreas que plantea la ISO 10164, excepto a lo relacionado con el área de administración de seguridad, puesto que a la hora de evaluarlos se encontraron limitaciones en cuando a operaciones de seguridad. Ante este inconveniente, es necesario acudir a los IDS, para solventar esta área de la administración.

A nivel general uno de los mayores problemas que preocupa a la administración de redes es la seguridad, cabe recalcar que las actividades de control abarcan las funciones específicas que deben cumplirse para que la red sea segura según Liu, Torng, & Meiners (2012) las ACL proveen seguridad a las redes privadas controlando todo el flujo de los paquetes que entran y salen entre una red privada y el internet, a traves de una secuencia de reglas. En el transcurso de esta investigacion se pudo determinar que establecer correctamente las ACL requiere de mayor atencion, debido a que un error logico podria desembocar en grandes problemas como infiltracion de trafico a la red.

Otro factor de importancia para la investigacion realizada fue los protocolos de administracion de red, porque gracias a estos se realiza la mayor parte del monitoreo. En investigaciones realizadas se afirma que:

> Los protocolos fundamentales de red son Internet Control Message Protocol (ICMP) y SNMP. Estos dos protocolos son útiles como herramientas básicas para solucionar problemas y administrar redes. (Brad, 2003, p.90)

La teoria expuesta por este autor, concuerda con el trabajo realizado, debido a que la mayoria de los requisitos funcionales evaluados en los resultados dependen de estos dos protocolos, especialmente del protocolo SNMP, puesto que los mensajes get request y traps son los mas utilizados para realizar consultas del estado de los equipos y generar alertas. Ademas el protocolo ICMP se uttiliza para consultar la disponibilidad de los dispositivos monitoreados.

CAPITULO 5

PROPUESTA DE INTERVENCIÓN

5.1 Titulo

Zabbix como herramienta para la administracion de red para la Pontificia Universidad del Ecuador Sede Esmeraldas

5.2 Descripción

Después de obtener y analizar los resultados de la investigación, se propone al departamento de TIC la implementación de buenas prácticas para el gobierno de TI, específicamente la implementación de ITIL en la prestación de los servicios y la definicion de un SLA que delimite las funciones del departamento y las necesidades de la institucion.

Siguiendo el concepto de estandarización, se propone también hacer uso de la ISO 10164 la cual, pese a su amplitud y profundidad, define la administración de redes de manera muy clara y puede ser útil para la toma de decisiones, esta ISO está orientada a la administración de sistemas en general.

Como se ha indicado en el transcurso de este estudio, el monitoreo y control son claves para la gestion y administracion de cualquier entidad, bajo este concepto y entendiendo la importancia de las redes informaticas para una institucion, el monitoreo de estas toma sentido y se torna una necesidad. Es por esta razon que se propone a la PUCESE la implementacion de la herramienta Zabbix para una mejor administracion de redes.

Zabbix es un software empresarial de monitoreo de codigo abierto para redes y aplicaciones. Está diseñado para monitorear y rastrear el estado de varios servicios de red , servidores y hardware de red.

5.3 Desarrollo

La documentación oficial de Zabbix menciona los requerimientos de hardware y software que se necesitan para que el sistema funcione correctamente. Estos requerimientos van a cambiar dependiendo de la cantidad de equipos que se vayan a monitorear. La tabla 8 detalla los requerimientos de zabbix en base al numero de equipos que va a monitorear.

Tabla 8 Requerimientos de Zabbix

Tamaño	**Plataforma**	**CPU/Memoria**	**Base de datos**	**# Dispositivos**
Small	CentOS	Virtual Appliance	MySQL InnoDB	100
Medium	CentOS	2CPU/2GB	MySQL InnoDB	500
Large	RedHat Linux	4CPU/4GB	RAID10 MySQL InnoDB or PostgreSQL	>1000
Vary Large	RedHat Linux	8CPU/8GB	Fast RAID10 MySQL InnoDB or PostgreSQL	>10000

Basados en la cantidad de equipos que se tomaron para este estudio, se utilizo una configuracion para una organización de tamaño media.

Las principales funciones que brinda zabbix para administrar la red se encuentran detallada en los anexos del 5 al 11.

CAPITULO 6

6.1 CONCLUSIONES Y RECOMENDACIONES

6.1.1 Conclusiones

- La PUCESE cuenta con una infraestructura de red compuesta por dos áreas las cuales se conectan por medio de fibra óptica. El departamento de TI en su función de administrador de la red busca controlar todos los servicios, servidores y equipos de comunicación para garantizar un alto desempeño de la red para ello se establecieron requisitos funcionales los cuales fueron mencionados en los resultados y deben estar contenidos en las herramientas de monitoreo.
- La red de la PUCESE está conformada por 170 switch de los cuales 90 son administrables y cinco servidores principales que bajo tecnología Docker brindan todos los servicios que suministra el departamento de TIC.
- Un factor muy importante por mencionar fue el uso de herramientas de monitoreo y control de tipo avanzado o proactivo debido a que las herramientas de tipo básica no abarcaban los requisitos estipulados en los estándares internacionales y que requiere el departamento de TIC de la institución.

6.1.2 Recomendaciones

- La implementación del sistema de monitoreo ZABBIX, debido a que cumple gran parte de las funcionalidades específicas que están propuestas en el modelo de administración de red que facilita la ISO 10164, además de poseer una licencia GPL que brinda libertades como la modificación, el uso y la distribución del software, esta licencia está aprobada por la Fundación por el Software Libre y por la Open Source Initiative (OSI), conjuntamente cuenta con el respaldo de trabajar para empresas de peso internacional, como lo es la marca DELL.
- Trabajar en conjunto con algún IDS como Snort para cubrir el área de seguridad de la administración de red

7. REFERENCIAS

Abud Figueroa, M. A. (2006). Calidad en la Industria del Software. La Norma ISO-9126. *Revista Upiicsa*, 1-3.

Arman, R., Khashayar, R., & Suhaimi, I. (2014). *An Application for Management and Monitoring the Data Centers Based on SNMP.* Malaysia.

Aryachandra , A., Fazmah, A., & Novian, A. (2016). *Intrusion Detection System (IDS) Server Placement Analysis in Cloud Computing* . Bandung: Fourth International Conference on Information and Communication Technologies.

Bharadwaj, K., Flores, S., Rodriguez, J., Long, L., & Marai, E. (2016). *Developing a Scalable SNMP Monitor.* Chicago.

Brad, H. (2003). *Network Management – Back to the Basics.*

Carlos, M. (2011). *METODOLOGIA DE LA INVESTIGACION CUANTITATIVA Y CUALITATIVA.* Bogota.

Case, Fedor, Shhhoffstall, & Davin. (1990). *A Simple Network Management Protocol.*

Chunkyun, Y. (2012). *A study for decrease of SNMP messages through an efficient processing of trend analysis information.* Kwangju.

Cisco Systems. (2003). *Internetworking Technologies Handbook.* Indianapolis: Cisco Press.

Clemm, A. (2007). *Network Management Fundamentals.* Indianapolis: Cisco Press.

Crawley, E., Nair, R., Rajagopalan, B., & Sandick, H. (Agosto de 1998). *RFC Editor*. Obtenido de https://www.rfc-editor.org/rfc/rfc2386.txt

Diccionario panhispánico de dudas. (2005). *Real Academia Española* . Obtenido de http://lema.rae.es/dpd/srv/search?id=79HjiY8E1D68S0oGfe

Drake, P. (s.f.). *Unisis SNMP to manage networks.*

Edelsys, H. (2006). *Sistema de Biblioteca Pontifie Universidad Catolica del Valparaios.* Obtenido de http://biblioteca.ucv.cl/: http://biblioteca.ucv.cl/site/servicios/documentos/como_escribir_tesis.pdf

IBM. (16 de Enero de 2014). *IBM Argentina*. Obtenido de https://www-935.ibm.com/industries/ar-es/telecom-media-entertainment/case-studies/vodafone.html

Jiang, W.-H., Li, W.-H., & Du, J. (2003). *The Application of ICMP Protocol in Network Scanning.* Chengdu.

Jurgen, S., Aiko, P., Matus, H., Jorrit, S., & Remco, V. d. (2007). *SNMP Traffic Analysis: Approaches, Tools, and First Results.* Bremen.

Kwang, S., Jin, H., & Jin, Y. (2007). *Real-time network monitoring shceme based on SNMP for dynamic information.* Republic of Korea.

Lago, A., Mera, D., & Medina, W. (s.f.). *Implementacion virtual de redes LAN, enfocadas en el analisis comparativo de las ventajas del uso y aplicacion de las diferentes versiones del protocolo SNMP.* Guayaquil.

Lamberto, V. (s.f.). *Universidad Interamericana de Puerto Rico*. Obtenido de www.ponce.inter.edu: http://www.ponce.inter.edu/cai/Comite-investigacion/investigacion-cualitativa.html

Liang, L., Weifeng, W., & Wang, Z. (2013). *Design and Implementation of Network Devices Monitoring System Based on SNMP* . Paris.

Liu, A., Torng, E., & Meiners, C. (2012). Compressing Network Access Control Lists. *TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS*, 1969.1977.

Lopera, J., Ramírez, C., Zuluga, M., & Ortiz, J. (2010). EL MÉTODO ANALÍTICO COMO MÉTODO NATURAL. *Revista Crítica de Ciencias Sociales y Jurídicas*, 5-27.

Luque, P. (Septiembre de 2015). *Ministerio Publico.* Obtenido de Misnisterio Publico Fiscalia de la Nacion: http://www.mpfn.gob.pe/escuela/contenido/actividades/docs/4090_diapo_curso_itil.pdf

Mifsud, E., & Lerma , R. (2013). *Servicio en red.* Madrid: McGraw-Hill.

Min, L., Zhiheng, G., & Weiping, L. (2011). *Case Study on IT Service Management Process valuation Framework Based on ITIL.* China.

Mogu, J. C. (1990). *Efficient use of workstations for passive monitoring of local area networks.* Palo Alto, California.

Newman, G. (2006). El razonamiento inductivo y deductivo dentro del proceso investigativo en ciencias experimentales y sociales. *Laurus Revista de Educación*, 180-205.

Pagurek, B. (2001). *Communications Network Management.*

Patcharee, T., & Finn, A. (2010). *An Adaptable Capability Monitoring System* .

Pras, A., Van de Meent, R., & Quartel, D. (2004). *Comparing the Performancie od SNMP and Wev Services-Based Management.*

Pugazendi, & Duraiswamy. (2009). *Mobile Agents-A Solution for Network Monitoring.* Kottayam.

Ritchie, G. (s.f.). *Serio.* Obtenido de Serio: http://www.seriosoft.com/sites/default/files/file-service/Introducci%C3%B3n%20a%20la%20Gesti%C3%B3n%20de%20Disponibilidad%20ITIL%C2%AE.pdf

Robert, L. (2009). *Configuracion y monitoreo de servidores.*

Romero, M. (2010). *Departamento de tecnología Electrónica Universidad de Sevilla.* Obtenido de Departamento de tecnología Electrónica: http://www.dte.us.es/personal/mcromero/masredes/docs/SMARD.0910.qos.pdf

Sahibudin, S., Sharifi, M., & Ayat, M. (2008). *Combining ITIL, COBIT and ISO/IEC 27002 in Order to Design a Comprehensive IT Framework in Organizations.* Malaysia.

Vargas, V. (7 de Agosto de 2016). *Calidad de software*. Obtenido de Calidad de software: https://vanevargas.jimdo.com/m%C3%B3dulos/modelos/modelo-iso-9126/

Yongqi, H., Yun, Z., Yaihao, L., & Liying, C. (2013). *Research of Network Monitoring Based on SSNMP*. Changchun .

ANEXOS

Anexo 1

ENTREVISTA JEFE DE DEPARTAMENTO DE TIC

1. ¿Cuáles son las principales funciones del departamento de TIC’s?
2. ¿Existe algún sistema de monitoreo de la red de datos en la organización?
3. Describa los componentes de la infraestructura de la red de la organización
4. ¿Qué tipo de problemas tiene el administrador al monitorear la red de datos?
5. ¿Qué servidores, dispositivos y servicios se requiere monitorizar?
6. A nivel de aplicación y usuario ¿Cuáles son los requerimientos que el sistema de monitoreo debe poseer?

Anexo 2

Tabla 9 Descripción de la matriz para evaluación ISO 9126

Característica	**Sub-característica**	**Escenario**
Funcionalidad	Interoperabilidad	El sistema posee componentes capaces de leer datos provenientes de otros sistemas
		El sistema posee componentes capaces de producir datos para otro sistema
	Precisión	Los resultados ofrecidos por los componentes sistema son exactos
		La comunicación entre los componentes no altera la exactitud de los datos.
	Seguridad	El sistema detecta la actuación de un intruso e impide acceso a los componentes que manejen información sensible
		El sistema asegura que los componentes no pierdan datos ante un ataque (interno o externo)
	Obediencia (Complinace)	Los componentes respetan un estándar de fiabilidad.
		La comunicación entre los componentes no viola los estándares de fiabilidad
Fiabilidad	Madurez	Los componentes del sistema manejan entradas de datos de datos incorrectos.
	Tolerancia a fallas	Todas las operaciones ejecutadas por los componentes se realizan correctamente bajo condiciones adversas.
	Capacidad de restablecimiento o recuperación	Los componentes del sistema no fallan bajo ciertas condiciones especificadas.
		Ante problemas con el ambiente un subconjunto determinado de los componentes

		puede continuar prestando sus servicios.
Eficiencia	Tiempo de comportamiento	El sistema debe recibir los servicios de sus componentes en el transcurso de un tiempo indicado.
	Recursos utilizados	Los componentes pueden compartir recursos adecuadamente.
		El sistema controla que ningún componente se quede sin recursos cuando los necesita.
Mantenibilidad	Habilidad de cambio, estabilidad, prueba	Es posible verificar el estado de los componentes del sistema.
		El sistema brinda facilidad para adaptar un componente.
		El sistema debe facilitar la sustitución/adaptación de un componente.
Portabilidad	Adaptabilidad	El sistema debe continuar funcionando correctamente aun cuando los servicios de los componentes provistos por el ambiente varíen
	Capacidad de Instalación	Los componentes pueden instalarse fácilmente en todos los ambientes donde debe funcionar
	Co-existencia	Los componentes manejan adecuadamente recursos compartidos del sistema.

Anexo 1

Tabla 10 Matriz de evaluación de Software bajo ISO 9126

12	CARACTERÍSTICA	SUB-CARACTERÍSTICA	MÁX. PONDERACIÓN	Pandora FMS		Nagios		Zabbix		Icinga		Paessler	
				EVALUADO	PUNTAJE	EVALUADO	PUNTAJE	EVALUADO	PUNTAJE	EVALUADO	PUNTAJE	EVALUADO	PUNTAJE
Calidad Interna y Externa	Funcionablidad	Adecuación	5	SI	5,00	SI	5,00	SI	5,00	SI	5,00	SI	5,00
		Exactitud	5	SI	4,00	SI	4,00	SI	5,00	SI	4,00	SI	5,00
		Interoperabilidad	5	SI	5,00	SI	5,00	SI	5,00	SI	5,00	SI	5,00
		Seguridad	5	SI	2,00	SI	3,00	SI	4,00	SI	3,00	SI	4,00
	Usabilidad	Documentación	5	SI	5,00	SI	5,00	SI	5,00	SI	5,00	SI	5,00
		Soporte y Entrenamiento	5	SI	3,00	SI	3,00	SI	4,00	SI	4,00	SI	3,00
		Interfaz Gráfica	5	SI	4,00	SI	4,00	SI	4,00	SI	4,00	SI	4,00
	Fiabilidad	Recuperabilidad	5	SI	4,00	SI	3,00	SI	4,00	SI	4,00	SI	4,00
		Tolerancia a Fallas	5	SI	3,00	SI	3,00	SI	4,00	SI	3,00	SI	3,00
	Eficiencia	Desempeño	5	SI	4,00	SI	5,00	SI	5,00	SI	4,00	SI	4,00
		Utilizacion de Recursos	5	SI	3,00	SI	3,00	SI	4,00	SI	3,00	SI	4,00
	Manteniabilidad	Acoplamiento	5	SI	5,00	SI	3,00	SI	5,00	SI	3,00	SI	4,00
		Modularidad	5	SI	5,00	SI	4,00	SI	4,00	SI	3,00	SI	5,00
	Portabilidad	Adaptabilidad	5	SI	5,00	SI	4,00	SI	5,00	SI	4,00	SI	4,00
		Instalabilidad	5	SI	4,00	SI	3,00	SI	4,00	SI	4,00	SI	5,00
		Coexistencia	5	SI	4,00	SI	4,00	SI	5,00	SI	4,00	SI	4,00
		Reemplazabilidad	5	SI	3,00	SI	3,00	SI	4,00	SI	3,00	SI	4,00
Calidad en uso		Poductividad	5	SI	4,00	SI	4,00	SI	5,00	SI	4,00	SI	4,00
		Seguridad	5	SI	3,00	SI	3,00	SI	4,00	SI	4,00	SI	4,00
		Satisfacción	**5**	SI	4,00	SI	3,00	SI	5,00	SI	4,00	SI	4,00
		TOTAL	**100**		**79**		**74**		**90**		**77**		**84**

Anexo 4

Tabla 11 Revisión de Funcionalidades

FUNCIONALIDAD	Pandora FMS	Nagios	Icinga	Zabbix	Paessler
Alertas	SI	SI	SI	SI	SI
Traps	SI	SI	SI*	SI	SI
ACL	NO	SI†	NO	SI	SI
Ancho de banda	SI	SI	SI	SI	SI
Histórico	SI	SI	SI	SI	SI
Reportes	SI	SI	SI	SI	SI
Detección de intrusos	SI†	SI†	SI	SI	SI
Graficas	SI	SI	SI	SI	SI

† Solo disponible en versión pagada

* Requiere de configuraciones adicionales

Anexo 5

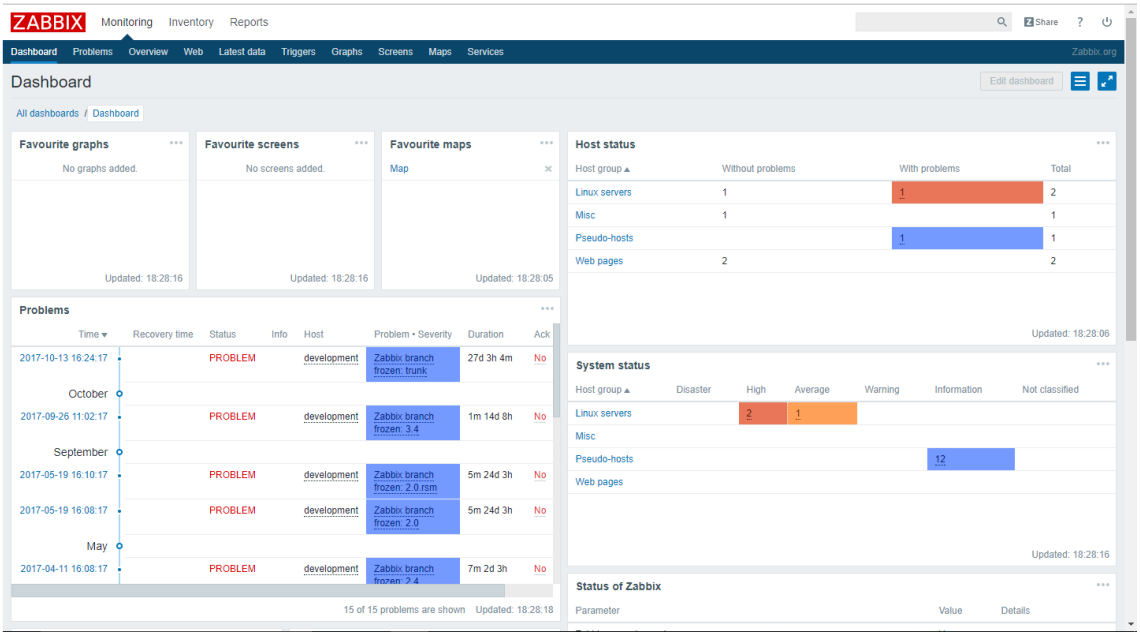


Ilustración 7 Dashboard de Zabbix

Anexo 6

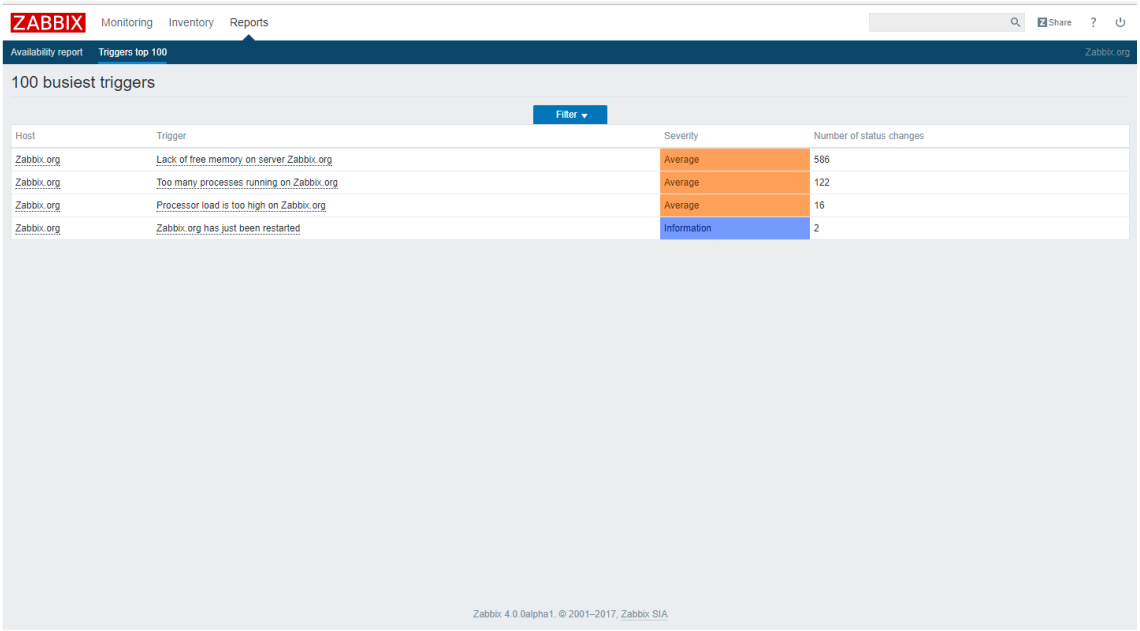


Ilustración 8 Reportes Zabbix

Anexo 7

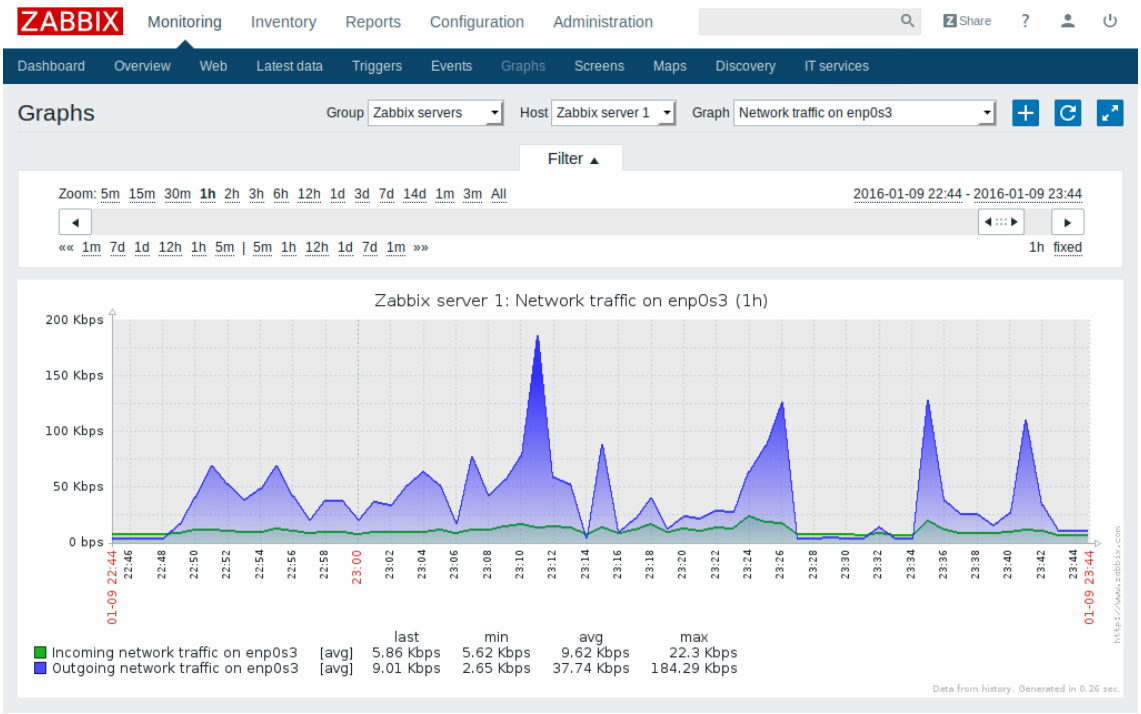


Ilustración 9 Zabbix Grtafico tráfico de red

Anexo 8

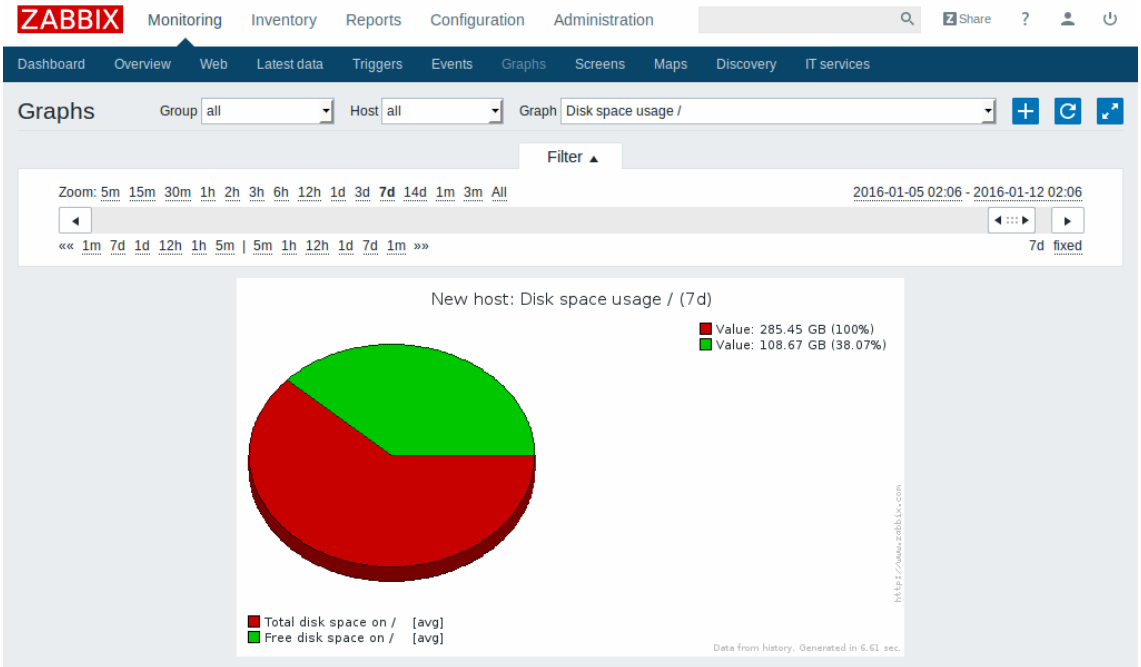


Ilustración 9 Zabbix Grafica uso de disco

Anexo 9

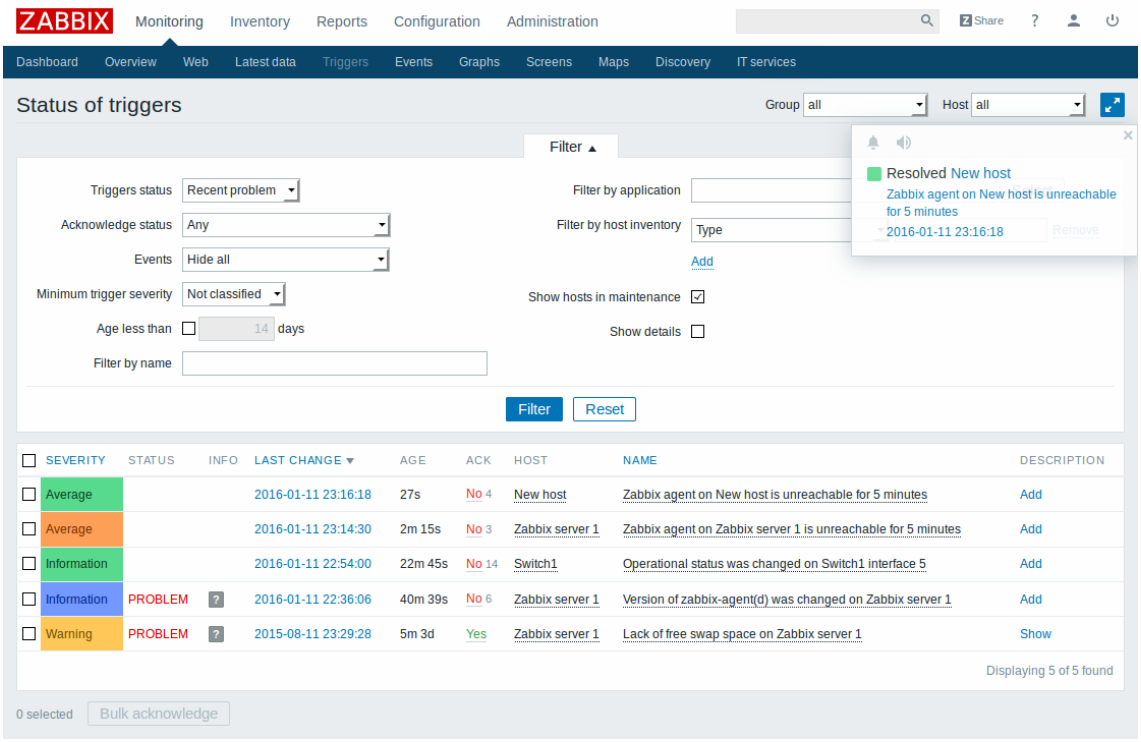


Ilustración 10 Zabbix Alertas

Anexo 10

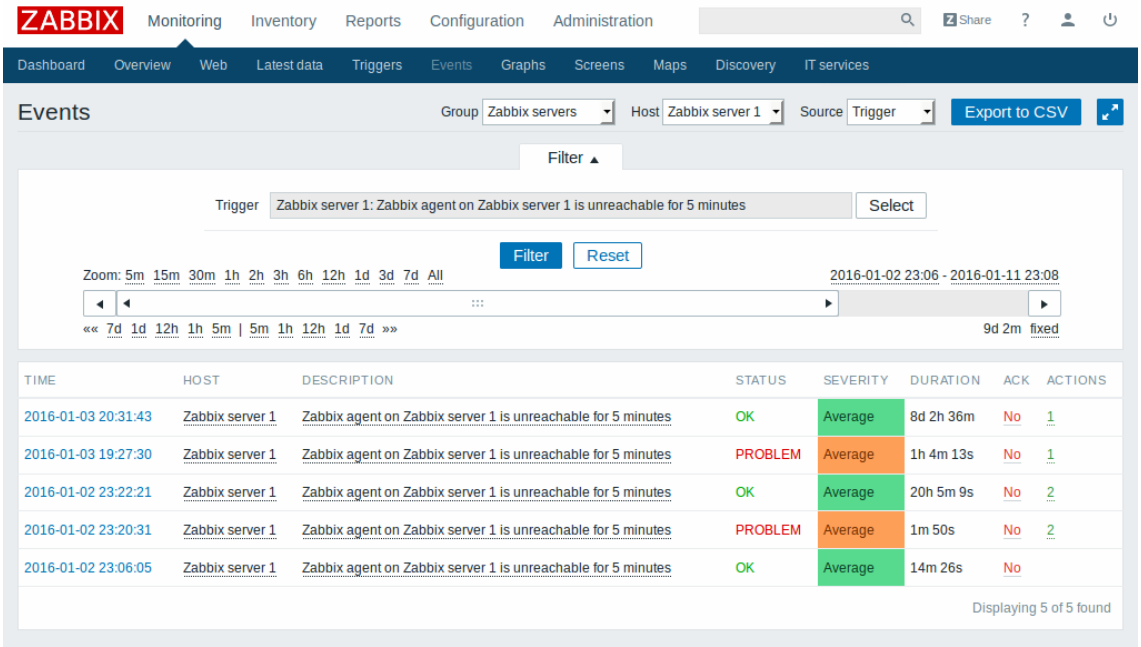


Ilustración 11 Zabbix Reportes

Anexo 11

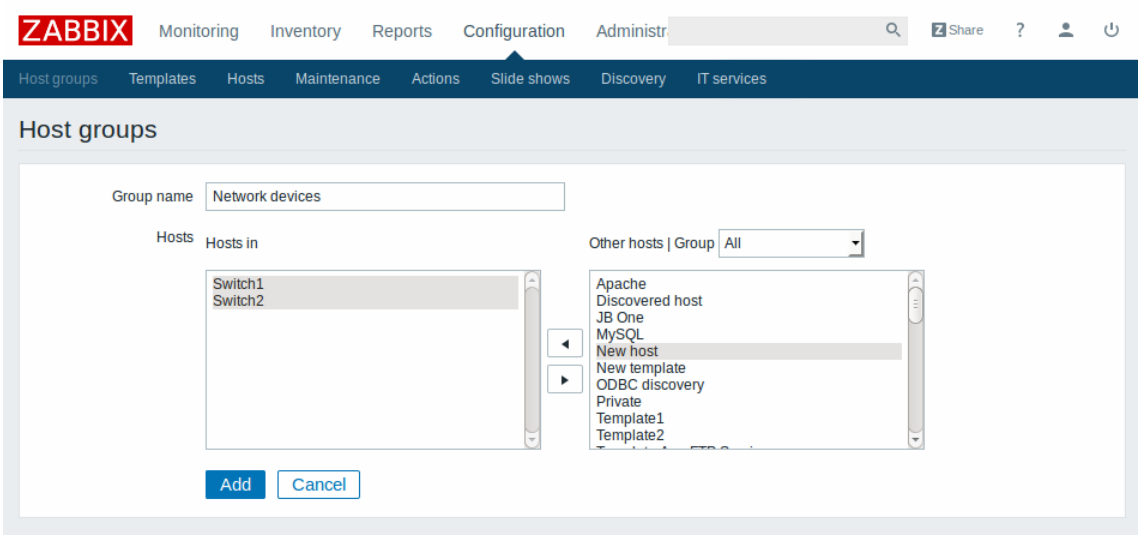


Ilustración 12 Zabbix Grupos