



# **Universidad Nacional Mayor de San Marcos**

**Universidad del Perú. Decana de América**

**Facultad de Ingeniería Electrónica y Eléctrica**

**Escuela Académico Profesional de Ingeniería Electrónica**

## **Diseño de un sistema de monitoreo de red LAN para una empresa Pyme, para mejorar la disponibilidad y la gestión de red, tomando como referencia el modelo de gestión de red en OSI**

### **TRABAJO DE SUFICIENCIA PROFESIONAL**

**Para optar el Título Profesional de Ingeniero Electrónico**

#### **AUTOR**

**Julio César FUERTE RUBIO**

#### **ASESOR**

**Rossina Isabel GONZALES CALIENES**

**Lima, Perú**

**2021**



Reconocimiento - No Comercial - Compartir Igual - Sin restricciones adicionales

<https://creativecommons.org/licenses/by-nc-sa/4.0/>

Usted puede distribuir, remezclar, retocar, y crear a partir del documento original de modo no comercial, siempre y cuando se dé crédito al autor del documento y se licencien las nuevas creaciones bajo las mismas condiciones. No se permite aplicar términos legales o medidas tecnológicas que restrinjan legalmente a otros a hacer cualquier cosa que permita esta licencia.

## Referencia bibliográfica

---

Fuerte, J. (2021). *Diseño de un sistema de monitoreo de red LAN para una empresa Pyme, para mejorar la disponibilidad y la gestión de red, tomando como referencia el modelo de gestión de red en OSI*. [Trabajo de suficiencia profesional de pregrado, Universidad Nacional Mayor de San Marcos, Facultad de Ingeniería Electrónica y Eléctrica, Escuela Académico Profesional de Ingeniería Electrónica]. Repositorio institucional Cybertesis UNMSM.

---

### Metadatos complementarios

<b>Datos de autor</b>	
Nombres y apellidos	Julio César Fuerte Rubio
Tipo de documento de identidad	DNI
Número de documento de identidad	47589919
URL de ORCID	No Aplica
<b>Datos de asesor</b>	
Nombres y apellidos	Rossina Isabel Gonzales Calienes
Tipo de documento de identidad	DNI
Número de documento de identidad	09389306
URL de ORCID	<a href="https://orcid.org/0000-0002-6353-2712">https://orcid.org/0000-0002-6353-2712</a>
<b>Datos del jurado</b>	
<b>Presidente del jurado</b>	
Nombres y apellidos	Teresa Esther Nuñez Zuñiga
Tipo de documento	DNI
Número de documento de identidad	08006778
<b>Miembro del jurado 1</b>	
Nombres y apellidos	Wilbert Chavez Irazabal
Tipo de documento	DNI
Número de documento de identidad	08121733
<b>Datos de investigación</b>	
Línea de investigación	C.0.6.3 Instrumentación Biomédica
Grupo de investigación	No Aplica
Agencia de financiamiento	No Aplica
Ubicación geográfica de la investigación	Edificio: Topsale S.A.C. País: Perú Departamento: Lima Provincia: Lima Distrito: San Isidro Calle: C. Los Halcones 242. Latitud: -12.09966 Longitud: -77.02067

Año o rango de años en que se realizó la investigación	Enero 2019 - Febrero 2020
URL de disciplinas OCDE	<p>Ingeniería eléctrica, Ingeniería Electrónica  <a href="https://purl.org/pe-repo/ocde/ford#2.02.01">https://purl.org/pe-repo/ocde/ford#2.02.01</a></p> <p>Telecomunicaciones  <a href="https://purl.org/pe-repo/ocde/ford#2.02.05">https://purl.org/pe-repo/ocde/ford#2.02.05</a></p>



UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS  
(Universidad del Perú, DECANA DE AMÉRICA)  
FACULTAD DE INGENIERIA ELECTRÓNICA Y ELÉCTRICA  
Teléfono 619-7000 Anexo 4226  
Calle Germán Amezaga 375 – Lima 1 – Perú



UNMSM

Firmado digitalmente por PAREDES  
PENAFIEL Rejis Renato FAU  
20148092282 hard  
Motivo: Soy el autor del documento  
Fecha: 29.12.2021 11:57:36 -05:00



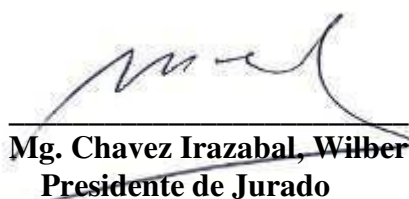
## ACTA DE SUSTENTACIÓN DE TRABAJO DE SUFICIENCIA PROFESIONAL Nº 055/FIEE-EPIE/2021


Los suscritos Miembros del Jurado, nombrados por la Comisión Ejecutiva del Programa de Perfeccionamiento Profesional de la Facultad de Ingeniería Electrónica y Eléctrica, reunidos en la fecha, bajo La Presidencia Del **Mg. Chavez Irazabal Wilbert** integrado por **Ing. Gonzales Calienes, Rossina Isabel** y **Dra. Nuñez Zuñiga, Teresa**.

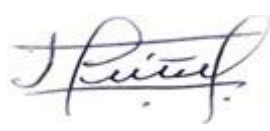
Después de escuchar la Sustentación de Trabajo de Suficiencia Profesional del **Bach. FUERTE RUBIO, JULIO CÉSAR** con código N° **12190150** que para optar el Título Profesional de Ingeniero Electrónico sustentó su Trabajo de Suficiencia Profesional titulado **DISEÑO DE UN SISTEMA DE MONITOREO DE RED LAN PARA UNA EMPRESA PYME, PARA MEJORAR LA DISPONIBILIDAD Y LA GESTIÓN DE RED, TOMANDO COMO REFERENCIA EL MODELO GESTIÓN DE RED EN OSI**.

El jurado examinador procedió a formular las preguntas reglamentarias y, luego de una deliberación en privado, decidió **aprobar** otorgándole el calificativo de dieciséis (16)

Ciudad Universitaria, 11 de diciembre del 2021

  
**Mg. Chavez Irazabal, Wilbert**  
Presidente de Jurado

  
**Ing. Gonzales Calienes, Rossina Isabel**  
Miembro de Jurado

  
**Dra. Nuñez Zuñiga, Teresa**  
Miembro Jurado

## RESUMEN

En la presente informe se da a conocer el proceso de implementación de un sistema de gestión y monitoreo para una empresa pyme usando herramientas de software libre u Open Source, con la finalidad de optimizar la red y mejorar la disponibilidad de los servicios y productos; asimismo, reducir el tiempo de solución de fallos que se dan día a día en la empresa, debido a que la empresa no cuenta con un sistema de monitoreo de gestión de incidencia y el tiempo de solución por cada fallo era de 4 horas hasta 1 día en red LAN de la empresa; asimismo solo el equipo router es monitoreado por el proveedor de servicio, lo que también ocasiona un retardo en el tiempo al diagnosticar la falla, por lo cual el tiempo de solución de cada incidencia se incrementa. Por consecuencia se propuso implementar un sistema de gestión y monitoreo usando herramientas de software libre, lo cual se quiere conseguir un mayor control del tráfico de datos a nivel LAN sin costear un software profesional con membresía. Con la finalidad de mejorar el SLA de las incidencias y la disponibilidad de la red; asimismo, facilitar el monitoreo al administrador de red.

**Palabras clave:** Ping, ICMP, Disponibilidad, SNMP, OSI.

## **ABSTRACT**

This report presents the implementation process of a management and monitoring system for a Pyme using free software tools or open source, in order to optimize the network and improve the availability of services and products; Also, reduce the time of solution of failures that occur every day in the company, because the company does not have a monitoring system for incident management and the solution time for each failure was 4 hours to 1 day in LAN network of the company; also only the router equipment is monitored by the service provider, which also causes a delay in time to diagnose the fault, so the solution time of each incident is increased. Consequently, it was proposed to implement a management and monitoring system using free software tools, in order to achieve greater control of data traffic at LAN level without the cost of professional software with membership. With the purpose of improving the SLA of the incidents and the availability of the network; also, to facilitate the monitoring to the network administrator.

**Keyboard:** Ping, ICMP, Availability, SNMP, OSI.



## TABLA DE CONTENIDO

RESUMEN .....	i
ABSTRACT .....	ii
TABLA DE CONTENIDO .....	iii
LISTA DE TABLAS .....	v
LISTA DE FIGURAS .....	vi
I. INTRODUCCIÓN .....	1
1.1. Objetivo del informe .....	1
1.2 Estructura del informe .....	1
II. INFORMACIÓN DEL LUGAR DONDE SE DESARROLLO LA ACTIVIDAD .....	2
2.1. Institución donde se desarrolló la actividad .....	2
2.2. Periodo de duración de la actividad .....	2
2.3. Finalidad y objetivos de la entidad .....	2
2.4. Razón social .....	3
2.5. Dirección postal .....	3
2.6. Correo electrónico del profesional a cargo .....	3
III. DESCRIPCIÓN DE LA ACTIVIDAD .....	4
3.1. Organización de la actividad .....	4
3.2. Finalidad y objetivos de la actividad .....	4
3.2.1. Finalidad .....	4
3.2.1. Objetivos .....	4
3.3. Problemática .....	5

	iv
3.3.1. Problema General .....	5
3.3.2. Problema Específicos.....	5
3.3.3. Justificación e Importancia de la Investigación.....	5
3.4. Metodología.....	6
3.4.1. Bases Teóricas .....	6
3.4.2. Marco Conceptual .....	13
3.5. Procedimiento.....	14
3.6. Resultados de la actividad.....	18
IV. CONCLUSIONES .....	43
4.1. Justificación .....	43
4.2. Metodología aplicada .....	44
4.2.1. Evaluación económica.....	44
4.2.2. Evaluación técnica .....	45
4.3. Descripción de la implementación .....	46
4.3.1. Requerimientos de hardware .....	46
4.3.2. Selección del hardware de sistema de monitoreo de red .....	48
4.4. Conclusiones .....	50
V. RECOMENDACIONES .....	52
VI. BIBLIOGRAFIA .....	53
VII. ANEXOS .....	55

## LISTA DE TABLAS

Tabla 1: Muestra de estudio.....	17
Tabla 2: Distribución de fallos en Cacti.....	27
Tabla 3: Límites de rendimiento.....	35
Tabla 4: Costo de software .....	44
Tabla 5: Presupuesto total .....	45
Tabla 6: Requerimientos de hardware para CentOS .....	47
Tabla 7: Requerimientos de hardware para Cacti.....	47
Tabla 8: Escalabilidad de equipos .....	48
Tabla 9: Evaluación de tres servidores .....	49

## LISTA DE FIGURAS

Figura 1: Simulación del diagrama de monitoreo .....	15
Figura 2: Elementos de Configuración .....	20
Figura 3: Inventario de Dispositivo .....	20
Figura 4: Documento Backup de Configuración.....	21
Figura 5: Prueba de conectividad mediante Ping .....	22
Figura 6: Prueba de Tracert hacia Google.com .....	22
Figura 7: Ciclo de vida de Incidencia .....	23
Figura 8: Captura de Monitor .....	24
Figura 9: Captura de Monitor.....	24
Figura 10: Alertas vía e-mail – Trafico Mayor 90%.....	25
Figura 11: Alerta del Dispositivo DOWN .....	26
Figura 12: Alerta del Dispositivo Activado.....	26
Figura 13: Panel de control para administración de incidente .....	28
Figura 14: Tickets de Incidencias y Solicitudes .....	28
Figura 15: Tráfico de Entrada y Salida SW_PISO13 .....	29
Figura 16: Tráfico de Entrada y Salida FWCISCO_ASA.....	30
Figura 17: Tráfico de Entrada y Salida SW_PISO2 .....	30
Figura 18: Tráfico de Entrada y Salida SW_PISO3.....	31
Figura 19: Tráfico de Entrada y Salida Router .....	31
Figura 20: Consumo de Memoria .....	36
Figura 21: Consumo de CPU de Servidor A.....	36
Figura 22: Consumo de CPU de AP_PISO3 .....	37
Figura 23: Configuración de una cuenta de usuario .....	38
Figura 24: Usuarios de Cacti .....	38
Figura 25: Los permisos que se puede asignar al usuario .....	39
Figura 26: Plantilla de Nessus .....	40
Figura 27: Escaneo del equipo por su IP .....	41

Figura 28: Escaneo del equipo .....	41
Figura 29: Vulnerabilidades existentes.....	42
Figura 30: Reporte de vulnerabilidad en Nessus.....	42
Figura 31: Diseño físico de sistema red de la empresa.....	46

## **I. INTRODUCCIÓN**

### **1.1. Objetivo del informe**

El presente informe tiene como objetivo gestionar y monitorear la red LAN de la empresa; asimismo, mejorar de disponibilidad de red y reducir los tiempos de SLA de las incidencias, por ello se realizó la implementación del modelo de gestión de red en OSI, y tomando como base sus áreas funcionales.

### **1.2 Estructura del informe**

La estructura del informe estará establecida de acuerdo al análisis realizado y guiada por un profundo estudio entre factores económicos y técnicos propios del diseño de sistema de monitoreo.

- Análisis técnico, se realizará en función a los dispositivos conectados a la red LAN y que estarán monitoreados debidamente.
- Análisis económico, se tomará utilizando la información de la implementación del diseño y del costo del dispositivo donde se instalarán las herramientas.

## **II. INFORMACIÓN DEL LUGAR DONDE SE DESARROLLO LA ACTIVIDAD**

### **2.1. Institución donde se desarrolló la actividad**

TOPSALE IT Solutions

### **2.2. Periodo de duración de la actividad**

El periodo de duración de las actividades fue desarrollado durante los años 2019 - 2020.

### **2.3. Finalidad y objetivos de la entidad**

- **Objetivos**

Ser una empresa innovadora y líder preocupada siempre por aportar a nuestro país, desde su crecimiento en el mundo de las tecnologías de la información y la inteligencia artificial, convencidos de que nuestra perseverancia y sentido de responsabilidad social empresarial lo harán posible de la mano de nuestro equipo de colaboradores y socios de negocios.

- **Finalidad**

Ser una empresa flexible e innovadora con la solvencia necesaria en todos los proyectos que decide participar, rediseñada e inspirada en ti y en nuestros

colaboradores en este nuevo comenzar al mundo que enfrentamos juntos contra el COVID19, a través de la calidad de nuestras soluciones inteligentes, dotadas de infraestructura y servicios TI innovadores, con alto sentido de responsabilidad social.

## **2.4. Razón social**

TOPSALE S.A.C

## **2.5. Dirección postal**

Cale los Halcones Nro. 242.

## **2.6. Correo electrónico del profesional a cargo**

Correo: [hpintor@topsale.pe](mailto:hpintor@topsale.pe)



### **III. DESCRIPCIÓN DE LA ACTIVIDAD**

#### **3.1. Organización de la actividad**

El profesional a cargo durante los análisis realizados fue Julio C. Fuerte Rubio y la organización de las actividades que se desarrollaron en el presente trabajo, se consideró las diferentes realidades tomadas en distintos escenarios nacionales e internacionales. De acuerdo a ello, se desarrolló un diseño de sistema de monitoreo y gestión de red LAN, donde abarca no solo el control del flujo de tráfico sino también tener una mayor disponibilidad y documentaciones de todos los dispositivos gestionados; asimismo, abarcando un gran control de seguridad informática de la misma. Finalmente, esto conlleva un monitoreo más efectivo y propicio para su sistema de red LAN de la empresa.

#### **3.2. Finalidad y objetivos de la actividad**

##### ***3.2.1. Finalidad***

Optimizar la red LAN y reducir el tiempo de SLA.

##### ***3.2.1. Objetivos***

Analizar el impacto del funcionamiento de un sistema de monitoreo para mejorar la disponibilidad de la red interna de una empresa pyme en Perú, en base al modelo de gestión de red OSI.

### **3.3. Problemática**

#### **3.3.1. Problema General**

¿Cuál será el impacto de la implementación de un sistema de monitoreo para una Pyme con la finalidad de mejorar la disponibilidad de sus equipos conectados a la red?

#### **3.3.2. Problema Específicos**

¿En qué medida se reduce los tiempos de SLA que se da por cada incidencia que se presenta, con un sistema de gestión y monitoreo en la red LAN?

¿En qué medida afectará la productividad de los usuarios finales una vez ya implementado el sistema de gestión y monitoreo en la red LAN?

¿En qué medida es viable las herramientas Open Source pueden ser tan factible para su uso en un sistema de gestión y monitoreo para una red LAN?

#### **3.3.3. Justificación e Importancia de la Investigación**

En la actualidad, el rubro de las telecomunicaciones viene creciendo progresivamente en conjunto a ello, las prestaciones de servicio por parte de los proveedores de servicio de internet (ISP) cada vez se acopla hacia las medianas y pequeñas empresas, dado que algunos proveedores de servicio adicionalmente brinda herramientas de monitoreo a sus clientes que son

gestionados por sus propios ingenieros asignados por parte del mismo proveedor de servicio, cabe explicar que, las empresas pymes que adquieren los servicios no tienen acceso directo a estas herramientas o no por completo, a partir de entonces los administradores de red de dicha empresa se ve sujeta a solicitar información sobre sus enlaces a ingeniero de nivel 1 a cargo de la gestión de la herramienta, como consecuencia a lo anterior se trabaja en la investigación de herramientas de monitoreo Open Source que puede ser instalado sin necesidad de comprar alguna licencia o permisos en cualquier equipo de red, con ello el administrador de red de la empresa tendrá la total libertad de poder controlar y gestionar sus propios enlaces, en caso que se presente una alerta, saturación o alguna falla en el enlace de sus sedes remotas, con esta información poder reportarlo lo más breve posible al proveedor de servicio de internet y así obtener una respuesta de solución más rápida, con la finalidad de mejorar la disponibilidad de sus enlaces.

El monitoreo y el control de fallos de la red es uno de los puntos más relevantes que tiene esta herramienta de red. Dicha herramienta de monitoreo nos permite analizar y validar el estado de cada dispositivo conectado a la red; es decir, se le representa al tráfico de la red con gráficas, estadísticas y diagramas en bloques entre otros, facilitando una mejor información para el administrador de red. Seleccionar una herramienta de monitoreo de red apropiada nos ayudará a identificar los posibles fallos antes de que suceda o se presente la alerta o caída del servicio.

### **3.4. Metodología**

#### **3.4.1. Bases Teóricas**

- Antecedentes internacionales

Baéz (2017), en su tesis “Diseño e implementación de un modelo de gestión de red para la red de área local del edificio central de la universidad técnica

del norte en base al modelo de gestión OSI con el protocolo SNMP.”, tuvo como objetivo mejorar la disponibilidad en la operación de la red con herramientas adecuadas de control y monitoreo, con la finalidad del uso eficiente del sistema de red y así poder utilizar mejor los recursos del sistema.

Lo cual los factores principales para este diseño era disponibilidad de la red, que no tengan interrupciones y mayor rendimiento adecuado para la red, ya que el más mínimo problema de red puede traer efectos adversos. Del Edificio Central de la Universidad Técnica del Norte su red área local, dado que presentaba un gran número de dispositivos conectados a la red, está dependía de variantes e inconvenientes que se presentaban.

La labor más engorrosa de un sistema de red es conservar el uso correcto de la misma, lo cual esto hace que es más compleja el control. Cada vez que se presentaba alguna falla en algunos de los componentes de la red, este no se notificaba de una manera automatizada; asimismo, es fundamental que el administrador de red TI y su soporte técnico validen presencialmente el funcionamiento de los equipos conectados para verificar alguna falla. Otra desventaja es que tener un log acerca de los eventos que se producen en el sistema de red, por ello no se pueden aplicar ciertas medidas y ofrecer una respuesta más rápida a la incidencia.

Se desarrollo un modelo de monitoreo y gestión de red en el Edificio Central de la Universidad, en base a las 5 áreas funcionales del modelo de gestión de red OSI, los cuales son las siguientes: Gestión de contabilidad, gestión de fallos, gestión de configuraciones, gestión de seguridad y gestión de prestaciones.

En base al desarrollo y diseño de la herramienta de distribución Open Source, se logró obtener un sistema de monitoreo de red que abarca las 5 áreas funcionales mencionadas, ofreciendo así un sistema de red con alta disponibilidad monitoreada, en donde las incidencias que ocurren en el día a día pueda ser detectadas en el menor tiempo posible, en comparación si no se tuviera este control. Al finalizar este proyecto se desarrollaron manuales y políticas de procedimientos en base a las cinco áreas funcionales del modelo

de gestión de red OSI, para que ayude como guía para el uso adecuado del sistema de monitoreo y sus componentes.

Inuca (2015), en su tesis “Administración y gestión de la red de área local del gobierno autónomo descentralizado municipal del Cantón Cayambe, basado en el modelo funcional de gestión de red ISO/OSI con el protocolo SNMP y uso de herramientas de software libre.”, el presente trabajo, se realizó con el propósito de optimizar el rendimiento de la red interna, del GADIP Municipio de Cayambe, en referencia al modelo de gestión de red OSI, y tomando en base a sus 5 áreas funcionales de gestión de fallos, gestión de contabilidad, gestión configuración, gestión de seguridad y gestión de rendimiento, la cual ejerce un monitoreo y control de la red de forma más adecuada, e organizada las funciones que se debe monitorear.

Para el monitoreo y gestión del sistema de red, se propuso las herramientas de software libre, los cuales fueron Zenoss y Zentyal, esto mejoro el control de las áreas funcionales de gestión OSI, la herramienta Zenos tenía la función de ser la estación gestora, esto permitía recopilar información de los equipos conectados en la red; asimismo, el rendimiento de sus recursos, inventarios, así como también el empleo de notificación de eventos y fallas producidas mediante correo electrónico o mensajes de texto, por otra parte, la herramienta Zentyal propone una plataforma con múltiples servicios en un solo sistema operativo, lo que también cumplía funciones como control de usuarios, IDS/IPS, firewall mediante OPEN LDAP, en un ambiente de portal cautivo.

En la presente tesis se desarrolló el significado de los protocolos de gestión de red simple, SNMP versión 2, por ende, dicho protocolo se debía habilitar a todos los dispositivos conectados a la red, este protocolo nos permitía recibir la información requerida de cada equipo conectado para ser monitoreado y validar su funcionamiento, con la finalidad que el administrador pueda monitorear los registros de la red. Esta estructura del sistema monitoreo de red, que trabaja en el NOC de administración y monitoreo de red, que se encuentra en el departamento de TIC de la institución, por ende, se aplica en base a procedimientos y políticas propuestas para administrar la red.

Como alternativa para mejorar la gestión de la red, también se ha propuesto un diseño de segmentación de la red. Finalmente, la implementación de este proyecto ha facilitado al administrador la gestión y control de la información del tráfico de la red y su funcionamiento, lo que ya no es necesario realizar un inventario manual de las direcciones IP utilizadas, registrándose las propiedades de los dispositivos y el nombre del usuario como la información del dispositivo se obtiene a través del monitoreo y se pueden ver los usuarios que están usando la red a través de la plataforma.

Cuchala (2016), en su tesis “Gestión y monitoreo de la red interna del Gobierno Provincial de Imbabura mediante el modelo de gestión ISO y software libre”, este proyecto final se llevó a cabo con el objetivo de optimizar el servicio de la población asegurando la disponibilidad de la red de la Prefectura de Imbabura basada en el modelo de gestión de red OSI con sus cinco áreas funcionales: configuración, errores, facturación, beneficios y seguridad. En el desarrollo de este diseño, se examinaron las definiciones de administración y monitoreo de la red, así como el protocolo SNMP y sus funcionalidades, se desarrolló una auditoría lógica y de comunicación para determinar el estado actual de la red y sus componentes y los servicios de la red.

El diseño de las áreas funcionales del estándar OSI / ISO partió de la información almacenada, ya que para la gestión de la configuración se utilizó el estándar IEEE 291 8 con el fin de especificar los requisitos del software a implementar en la red de la prefectura de Imbabura. La elección recayó en la herramienta FMS Pandora, que facilita la gestión y el seguimiento de los dispositivos conectados a la red.

Para la gestión de errores se desarrolló un proceso de solución de las alarmas que ocurren en la red y una base de datos para la documentación de los errores y su eliminación.

La herramienta de Pandora FMS permite la creación de Alertas y Alertas Críticas a enviar a través del correo electrónico del administrador de la red para que el administrador de la red pueda identificar los errores que se puedan ocasionar y encontrar una solución de manera efectiva y rápida.

Como parte de la gestión de prestaciones, se ha desarrollado el control del rendimiento del flujo del tráfico de la red, en base al uso de la herramienta que permite la visualizar y registrar los eventos en la red a partir de gráficos e informes realizados de acuerdo a los requerimientos del administrador de la red para tener una mejor visualización del flujo. del tráfico de la red.

En referencia a la gestión de la contabilidad, se registraron los parámetros de los dispositivos, el nivel de las interfaces del equipo, la cantidad de usuarios conectados, la disposición del disco, el uso de la memoria y el procesador, las fases de conexión. En la gestión de la seguridad, se tomó como una contraseña principal para el usuario administrador y se han establecido políticas y lineamientos de seguridad para conectarse a los dispositivos conectados a la red. Finalmente, se establecieron normas de gestión, una guía procedimental para el correcto uso de las cinco áreas funcionales del modelo de gestión ISO; asimismo, se desarrolló un manual general con las configuraciones realizadas, y estos son brindados al director del Departamento de Tecnología de la Información de la Prefectura de Imbabura. Por último, en referencia al análisis de viabilidad técnica, se logró apreciar que el software y hardware de la Prefectura de Imbabura y se concluyó que el desarrollo del proyecto es de gran importancia para una adecuada gestión de la red, asegurando su disponibilidad, en situaciones críticas.

- Antecedentes nacionales

Peralta (2019), en la investigación titulada “Implementación de un servidor como gestión y monitoreo de servicios para la red de datos en la Ugel Huamanga, 2018”, se propuso que: Desarrollar un servidor para administrar y monitorear los equipos y servicios a través del protocolo SNMP, usando como base al sistema operativo CentOS7, Nethserver7, softwares de virtualización, herramientas Open Sources como Ntopng, Zabbix y Suricata, lo cual se utilizó como guía básica para la gestión de proyectos (PMBOK) para monitorear el consumo del flujo de tráfico de red, y evaluar el ancho de banda en el firewall, con la finalidad de detectar archivos maliciosos y vulnerabilidades, analizar el correcto funcionamiento de los elementos del software y hardware del sistema de red.

El estudio se desarrolló según los parámetros del método hipotético inductivo y de análisis, tipo observacional, la tesis arribó la siguiente conclusión: la propuesta de un servidor para administrar y monitorear de los equipos conectados a la red y servicios, utilizando como base la guía de Fundamentos de Gestión de Proyectos (PMBOK) fue reconocida como uno de los resultados de la evaluación del consumo del tráfico de red usado por IPS o equipos referenciales, puertos y a su vez los más utilizados. Protocolos de red identificados en términos de tráfico de red en tiempo real.

Casas (2017), en la investigación titulada “Implementación de un Sistema de Monitoreo y Supervisión de la infraestructura y servicios de red para optimizar la gestión de TI en la Universidad Nacional Pedro Ruiz Gallo”, planteó como objetivo general: Desarrollar un sistema de control y monitoreo para optimizar la gestión de la red de datos y la gestión continua de los equipos que se encuentran conectados a la red, y los servicios que se ejecutan en la Universidad Nacional Pedro Ruiz Gallo.

La presente investigación es de tipo aplicada, de diseño experimental. La tesis arribo a la siguiente conclusión: Mediante el estudio del estado actual de la Infraestructura y Servicios de red de la Universidad Nacional Pedro Ruiz Gallo se puede asegurar que el área TI de la Red Telemática no tiene un buen monitoreo de los equipos y servicios de TI ya que no se cuenta con la información centralizada ocasionando retardos al tomar conocimiento de las caídas de red de los equipos y servicios.

Quispe (2018), en su tesis “Implementación de un sistema de monitoreo y control de red, para un canal de televisión, basado en herramientas Open Source y Software Libre, Lima - 2017”, en esta investigación se desarrolló un estudio basado en la tecnología y monitoreo de soporte de la red del canal de televisión WILLAX TV, con el objetivo principal de diseñar un sistema de monitoreo y control de red del área local, basado en herramientas OPEN SOURCE (plugins). y Software Libre (CENTOS 7). Dado que este canal no cuenta con un sistema de gestión y monitoreo, esto fue visto como un problema principal para el canal, en su mayor parte para el área de redes, ya



que las transmisiones en vivo se realizan en líneas arrendadas. Por este motivo, se desarrolló un análisis del diseño descriptivo cuasiexperimental y eso nos dio un muestreo probabilístico, simplemente aleatorio, desarrollado y realizado en la oficina de apoyo y red de la emisora de televisión en la ciudad de Lima. Se utilizó la herramienta de seguimiento CentOs, que es una herramienta de código abierto.

Con el desarrollo del sistema de gestión y monitoreo de una red, usando la herramienta Centosv6, se logró un chequeo efectivo y análisis de los equipos de red (host, procesador, RAM, enrutador, fibra óptica, punto de acceso, servidor) y servicios del canal de televisión; mejorar y optimizar una respuesta oportuna para corregir los errores que se produzcan en la misma, mejorando así la gestión de los servicios y dispositivos de red para el personal. Centosv6 monitorea y monitorea la red para detectar problemas ocasionados por conexiones de datos sobrecargadas o conexiones de red, así como por monitorear el disco duro, RAM, conmutadores.

Al comenzar la implementación, se dio por el monitoreo de los equipos conectados a la red lo cual se implementó la configuración e instalación del sistema operativo en este caso Linux. A esto siguió la instalación de la herramienta de código abierto CentOS6, los complementos y el software de monitoreo de red.

El sistema operativo CentOS6 para este proyecto fue de gran importancia para las organizaciones, para identificar problemas de sus sistemas de red y resolverlas antes que se vean afectados los servicios tanto comunes como críticos. Se considero dos puntos fundamentales para el diseño, que son la flexibilidad y la escalabilidad de la red, es un software poderoso que ayuda a controlar y detectar la falla, evitando incidencias a futuro antes de que impacten al usuario final y a los clientes. Luego se agregaron los equipos y servicios de red, posterior se implementó la configuración de la herramienta para cada equipo conectada a la red. Por último, se llevaron a cabo validaciones funcionales para corroborar la efectividad del ancho de banda, la gestión de dispositivos y los servicios.

### **3.4.2. Marco Conceptual**

- SNMP: Es un protocolo que establece una conexión para compartir información de administración entre los dispositivos de red, dicho protocolo pertenece a la capa de aplicación.
- DHCP: Es un protocolo que tiene la función principal asignar una dirección IP y parámetros de configuración a los dispositivos conectados en la red, este tipo de protocolo es de cliente/servidor.
- DNS: En sus siglas en ingles Domain Name System, es un sistema o servicio que habilita una conexión entre nombres de dominio y direcciones IP con las que están relacionado.
- API: En sus siglas en ingles Application Programming Interfaces, API es un conjunto de protocolos y reglas que se usa para integrar y desarrollar el software de las aplicaciones.
- IP dinámica: Es una IP asignada a un equipo de red mediante un servidor DHCP de forma aleatoria, lo cual dicha IP tiene una duración temporal, posteriormente hasta que caduque este tiempo se le asigna otra IP aleatoria.
- ISO: Representa las siglas de la organización que desarrolla los estándares, International Standard Organization, dentro de esta organización ISO existen ciertos comités encargados de desarrollar los estándares.
- ITU: Unión Internacional de Telecomunicaciones es el organismo especializado en telecomunicaciones de las Naciones Unidas, encargado de regular las telecomunicaciones a nivel internacional entre distintas empresas y ordenadoras.
- MIB: En sus siglas en ingles Management Information Base, es una base de datos que representa las características de cada componente en un dispositivo de red.
- TCP/IP: En sus siglas en ingles Transmission Control Protocol/Internet Protocol, es un conjunto de normas estandarizadas que establecen una comunicación entre equipos de red mediante ciertos protocolos.

- UDP: Es sus siglas en ingles User Datagram Protocol, UDP es un protocolo que establece una comunicación entre equipos de red sin conexión de datagramas de redes.
- Cisco: Es una empresa global y líder mundial en TI, que está dedicada a la fabricación, comercialización y venta de equipos de red, como por ejemplo router, switch, firewall entre otros.
- CMIP: El protocolo de administración de información común es un protocolo de administración de red que define la comunicación entre las aplicaciones de administración de red.
- ICMP: Es el protocolo de notificación y control de errores e información operativa de Internet.
- NMA: Es una aplicación de administración de red es el software que se encuentra en la instalación de administración de red y recuperar datos.
- NMS: Es la estación encargada de la monitorización en un sistema de gestión.
- OSI: Es un modelo de referencia para los protocolos de la red de arquitectura en capas.

### **3.5. Procedimiento**

Para la implementación de la propuesta del presente trabajo se desarrolló en base al modelo de gestión OSI, donde se diseñó un sistema red similar a la red de la empresa para tener una perspectiva del diagrama de monitoreo, lo cual se simulo en la herramienta GNS3. En la siguiente Figura 1, podremos visualizar la simulación del diagrama de monitoreo en GNS3, donde se propondrá la implementación de sistema de monitoreo de red. Los equipos que estuvieron en monitoreo fueron los servidores, los switches, el access point, firewall y el router; todos los equipos de red que están en monitoreo se le tuvo que configurar el protocolo SNMP.

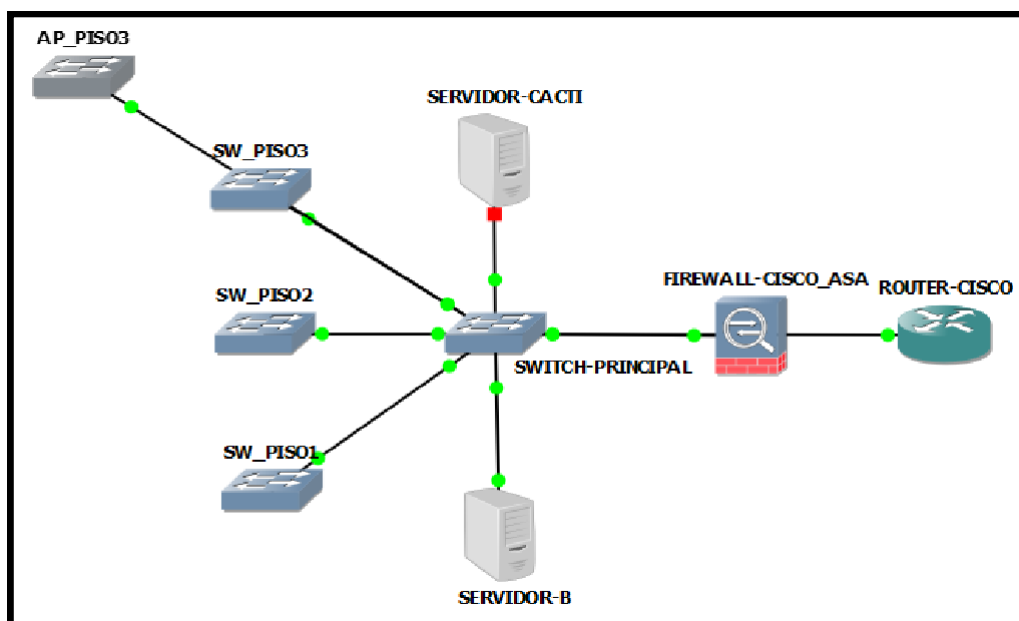


Figura 1: Simulación del diagrama de monitoreo. Fuente: Captura de GNS3

El diseño es no experimental ya que se basa en la observación con la ayuda de los datos obtenidos.

En el Servidor-Cacti se instaló el Windows Server 2012, lo cual este servidor será nuestro servidor de monitoreo, así mismo se instaló Nessus 8.14.0 para los análisis de vulnerabilidad, la herramienta iTOP para gestionar los tickets, y por último se levantó una máquina virtual en Centos v6 para instalar el Cacti que será nuestra herramienta de gestión y monitoreo.

Los equipos de red que se usaron en la simulación en GNS3 entre router y switches se tendrán que habilitar el protocolo SNMP, con la finalidad de ser gestionados por la herramienta de monitoreo Cacti.

Cacti permite monitorear los dispositivos mediante el protocolo SNMPv1, SNMPv2, SNMPv3, la versión con la que se habilitó a los dispositivos fue con SNMPv2, debido que esta versión es mucho más simple y más sencilla su configuración. Lo cual no se optó la habilitación de SNMPv3, a pesar de que sea la versión más robusta en seguridad lo que produce un aumento de carga de CPU, ocasionando que la herramienta tenga un performance más lento.

Para que el router pueda enviar datos al software de gestión se tuvo que realizar la siguiente configuración con el protocolo SNMPv2.

```
snmp-server community public RO
```

Donde RO indica que la función será Read-Only, además se configuró la comunidad con el nombre de public, lo cual se recomienda cambiar de nombre por otra.

Esta configuración sirve tanto para el router como los switches.

Se consideró como población en estudio es de cuarenta y dos (42) equipos de comunicación, red de ordenadores, es un conjunto de dispositivos conectados en la misma red, mediante de señales, cables o cualquier otro medio de transporte de datos, y así establecer una conexión para compartir información y servicios.

Estos equipos red hacen posible las comunicaciones entre distintos puntos de red, estos equipos por ejemplo son: computadora, laptop, impresora, router, switch y etc.

Toda red tiene el propósito de conectar computadoras, teléfonos y celulares mediante equipos que administra el flujo de tráfico como son los switches y routers. Estos dos equipos son fundamentales para mantener a todos los equipos de red conectados con los demás y con otras redes. A pesar que estos dos equipos de red son muy similares, los switches y routers tienen funciones muy diferentes en el sistema de red.

Por el lado con los switches, estas son usadas para conectar varios dispositivos que se encuentren conectados en la misma red de un edificio u oficina. De esta manera se podría decir, un switch nos permite conectar las computadoras, teléfonos IP, impresoras, access point y servidores, y así construyendo un ambiente de red donde comparte información entre ellas. El switch también actuaría como un gestor y controlador del flujo de tráfico de red, permitiendo así clasificar el tráfico de acuerdo a las áreas de la empresa.

En cambio, los routers tiene la función de conectar varias redes distintas. Es decir, esto nos permite que las computadoras puedan conectarse a internet y compartir información entre varios usuarios. El router se comportará como un

distribuidor, y tomando la mejor ruta para que la información enviada llegue al destino en un tiempo menor. Este dispositivo también analiza los datos que se van a compartir mediante la red, los empaquetan de acuerdo a su tipo y los envía a cada red correspondiente. Finalmente, el router nos permite conectar nuestra empresa al mundo exterior, y proteger nuestra información privada de amenazas de ciberseguridad, incluso, puede priorizar los tipos de tráfico que llegan a la red interna sobre los demás.

*Tabla 1:* Muestra de estudio

Equipos de comunicación	Cantidad
Router	1
Switch	3
Access Point	1
Servidores	2
Firewall	1
<b>Total</b>	<b>9</b>

Fuente: Autor

En las siguientes líneas explicaremos las funciones de los softwares que utilizaremos para el monitoreo y gestión.

- Cacti: Esta herramienta nos permite medir el flujo de tráfico en la red, lo cual eso nos ayuda a verificar si hay una alta saturación en la red o si no se observa tráfico se podría considerar ya como una incidencia. Así mismo, esto nos ayuda a tener un mayor control proactivo de la red que nos ayuda a combatir la incidencia en un menor tiempo posible, mejorando nuestro tiempo de SLA.
- iTop: Esta herramienta nos sirvió para medir las cantidades incidencias por un intervalo de tiempo y haciendo un cálculo por estadística podemos

verificar alguna falla repetitiva y así tratar de solucionar alguna problemática en la red.

- Nessus: Esta herramienta nos permitió medir el nivel de vulnerabilidades de los servicios que utilizamos en nuestra red. (Crítica, Alto, medio, bajo, información.)

### **3.6. Resultados de la actividad**

En este campo se detalló los resultados obtenidos de la simulación del modelo de gestión de monitoreo, donde se desarrolló la implementación para cada una de las áreas funcionales mencionadas del sistema de gestión de red OSI.

#### ***3.6.1. Implementación de gestión de configuración***

Para implementación de la gestión de configuración se realizó un registro las configuraciones e inventario de los equipos de red, guardando dicha configuración en la nube privada como en el servidor principal.

***3.6.1.1. Registro de configuración.*** Se planteó una plantilla en formato Excel para registrar todas las configuraciones realizadas sobre los dispositivos que se viene gestionando.

La plantilla en mención contiene la siguiente información:

- Fecha y hora de ingreso y salida

Se refiere al registro de horario de trabajo que se realizó la configuración.

- Responsable de trabajo a realizar

Registrar el nombre del personal responsable de la configuración.

- Responsable que autoriza

Hace referencia al jefe directo o alguien de rango superior que apruebe la configuración.

- Tipo de dispositivo

Consta de registrar que dispositivo se va a configurar, sea un switch, router o servidores.

- Nombre de dispositivo

Es el nombre del equipo que se ha de configurar.

- Motivo de configuración

Es el por qué a realizar la configuración.

- Configuración realizada.

Es lo que el responsable de la configuración realizó

- Observaciones

Son los detalles que tienen que ser analizados.

La plantilla del registro de trabajo se encuentra en el ANEXO A

**3.6.1.2. Registro de configuración de dispositivos.** Tener un registro de los dispositivos en monitoreo es tan fundamental como tener un backup de la configuración de los mismo, ya que por buenas prácticas se lo recomienda, en caso ocurra un incidente donde se pierde la configuración del dispositivo y no se pueda recuperar. Por ellos la herramienta iTop nos permite tener un registro de cada equipo en monitoreo, de los usuarios por cada área, nos permite crear notas y documentos donde podemos guardar la configuración backup de cada dispositivo en monitoreo. En las figuras 2, 3 y 4 se muestra los elementos de configuración.



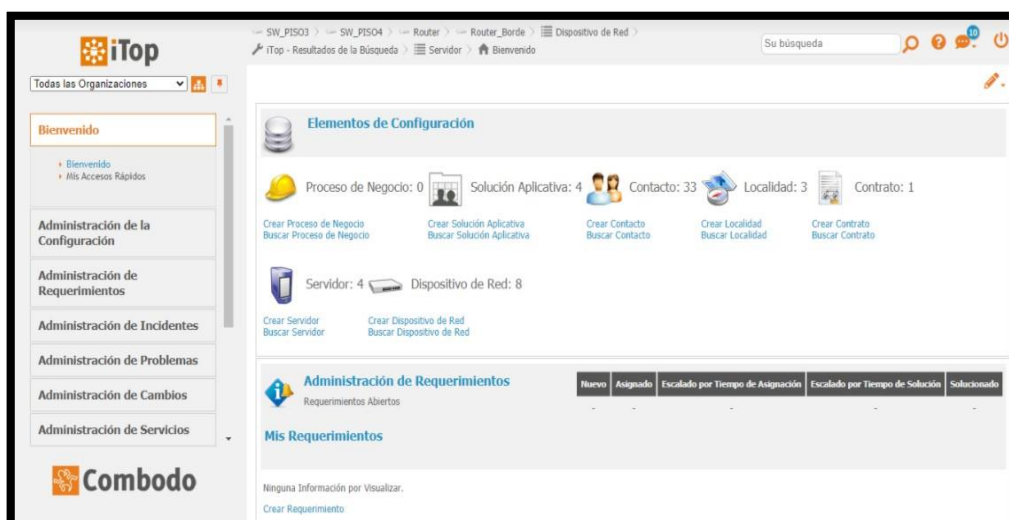


Figura 2: Elementos de Configuración. Fuente: Captura de iTOP

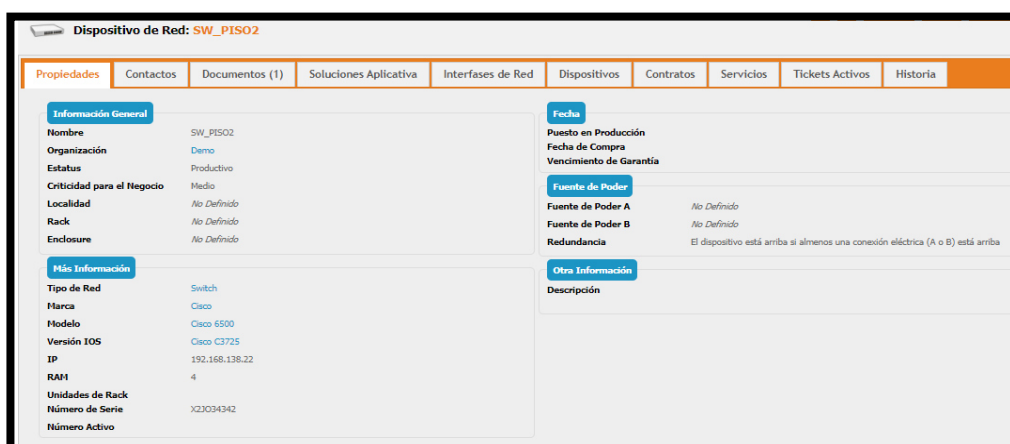


Figura 3: Inventario de Dispositivo. Fuente: Captura de iTOP

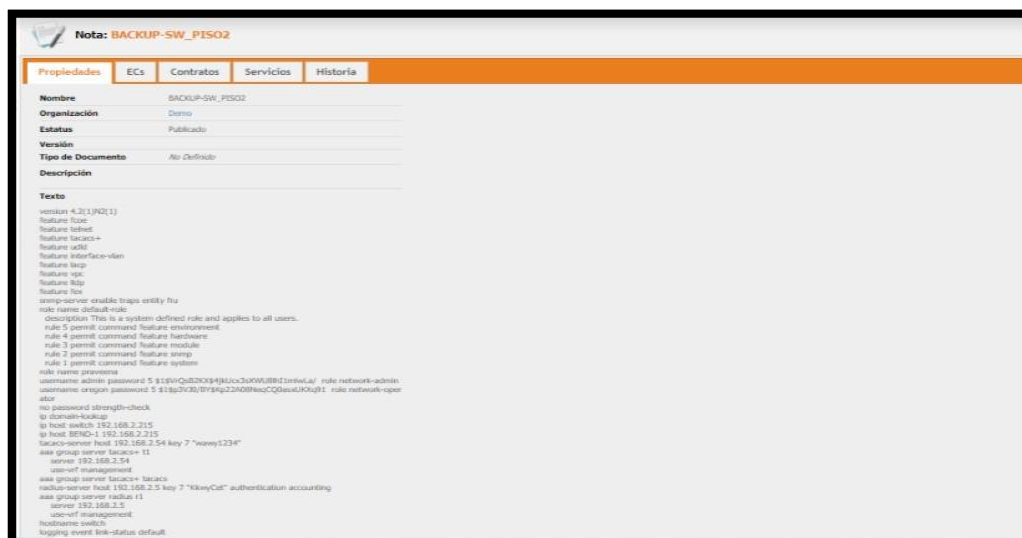


Figura 4: Documento Backup de Configuración.  
Fuente: Captura de iTop

### 3.6.2. Implementación de gestión de fallos

Para la implementación de gestión de fallos se utilizó los siguientes softwares, CACTI. Lo cual en la gestión de fallos se puede clasificar en gestión proactiva y reactiva.

**3.6.2.1. Gestión proactiva.** La gestión proactiva consiste en anticiparse un fallo que va suceder o ya sucedió, como también se puede contrarrestar antes que el usuario sea consciente de la falla. Una de las formas de realizar las pruebas cuando se tenga una alerta o una alta latencia se puede utilizar las siguientes herramientas:

- Ping: es un comando o una herramienta de diagnóstico que permite hacer una verificación del estado de una determinada conexión de un host local con al menos un equipo remoto contemplado en una red de tipo TCP/IP. En la siguiente Figura 5, se muestra un ping continuo hacia google.

```

C:\Users\Administrador>ping google.com -t

Haciendo ping a google.com [172.217.3.78] con 32 bytes de datos:
Respuesta desde 172.217.3.78: bytes=32 tiempo=79ms TTL=116
Respuesta desde 172.217.3.78: bytes=32 tiempo=77ms TTL=116
Respuesta desde 172.217.3.78: bytes=32 tiempo=77ms TTL=116
Respuesta desde 172.217.3.78: bytes=32 tiempo=78ms TTL=116
Respuesta desde 172.217.3.78: bytes=32 tiempo=88ms TTL=116
Respuesta desde 172.217.3.78: bytes=32 tiempo=76ms TTL=116
Respuesta desde 172.217.3.78: bytes=32 tiempo=78ms TTL=116
Respuesta desde 172.217.3.78: bytes=32 tiempo=77ms TTL=116
Respuesta desde 172.217.3.78: bytes=32 tiempo=77ms TTL=116
Respuesta desde 172.217.3.78: bytes=32 tiempo=79ms TTL=116

Estadísticas de ping para 172.217.3.78:
    Paquetes: enviados = 10, recibidos = 10, perdidos = 0
        (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 76ms, Máximo = 88ms, Media = 78ms

```

Figura 5: Prueba de conectividad mediante Ping.  
Fuente: Captura desde el Servidor Monitoreo

- Traceroute: es un comando o una herramienta que permite seguir la ruta que toma los paquetes que vienen desde un host. Figura 6, nos muestra el camino que recorre el paquete hasta llegar al destino establecido.

```

C:\Users\Administrador>tracert google.com

Traza a la dirección google.com [172.217.3.78]
sobre un máximo de 30 saltos:

  1    1 ms     2 ms     <1 ms  192.168.0.1
  2   10 ms    11 ms     8 ms  10.142.64.1
  3   11 ms    14 ms    12 ms  10.150.144.41
  4   12 ms    11 ms    10 ms  10.95.156.34
  5   82 ms    76 ms    77 ms  209.85.173.137
  6   86 ms    80 ms    93 ms  108.170.249.1
  7   78 ms    79 ms    80 ms  142.250.58.103
  8   83 ms    83 ms    78 ms  mia07s54-in-f14.1e100.net [172.217.3.78]

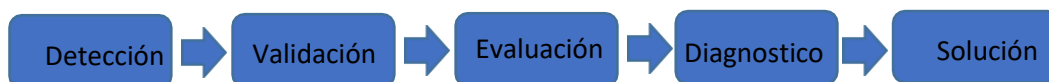
Traza completa.

```

Figura 6: Prueba de Tracert hacia Google.com.  
Fuente: Captura desde el Servidor

**3.6.2.2. Gestión reactiva.** La gestión reactiva consiste en el monitoreo constante tanto como el aplicativo Cacti. Cuando hablamos de gestión

reactiva nos referíamos que se realiza un monitoreo constante de los dispositivos que se encuentre dentro de la red LAN de la empresa, con la finalidad de detectar las incidencias que ocurren día a día. Esta gestión cumple con un ciclo de vida de incidencia a fallo, lo cual se visualiza en la Figura 7.



**Figura 7:** Fuente: Autor

- Detección: Es cuando se visualiza la alerta de un dispositivo de red.
- Validación: Se refiere al descarte de energía o trabajo programado que se realizó en el área.
- Evaluación: En esta etapa es cuando se realizan las pruebas y descartes de conectividad y configuración.
- Diagnóstico: De acuerdo a lo realizado en la etapa de evaluación se diagnostica el fallo o error de la incidencia.
- Solución: Una vez ya obtenido el diagnóstico se aplica las soluciones para dar por concluido el fallo en el menor tiempo posible.

En base a ello, desde el Cacti tenemos una interfaz de monitoreo donde podremos ver el estado de los dispositivos conectados al aplicativo. En la figura 8, podemos visualizar todos los dispositivos activos; en cambio, en la figura 9, podemos visualizar algunos equipos que se encuentra sin servicios.

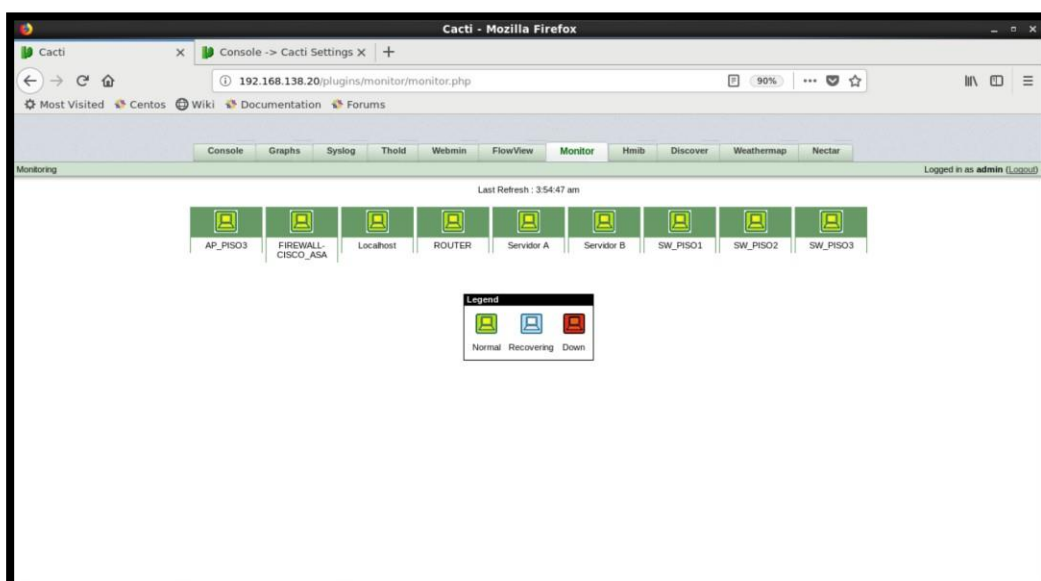


Figura 8: Captura de Monitor. Fuente: Captura Desde Cacti

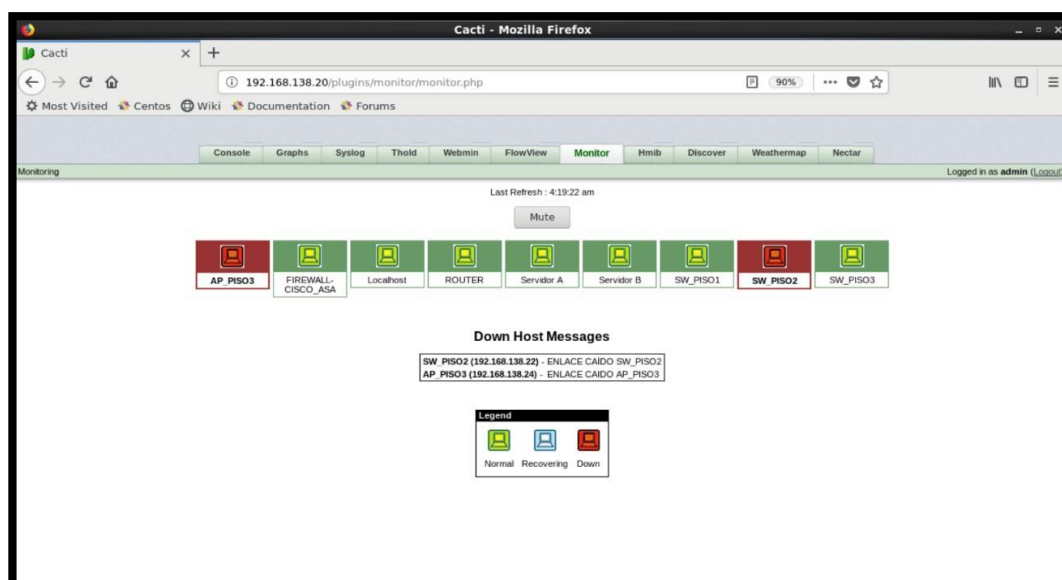


Figura 9: Captura de Monitor. Fuente: Captura Desde Cacti

- Alerta Vía e-mail

La herramienta Cacti nos la opción de configurar las alertas vía e-mail, las cuales estas se envían automáticamente cuando acontece algún evento en cualquier dispositivo monitoreado. Para el envío alertas se ha

configurado en Cacti desde un correo de Gmail, donde se enviarán las alertas. En la siguiente figura se puede visualizar la configuración de Cacti para el envío de correo vía e-mail a base del protocolo SMTP.

Las alertas de fallos se envían desde el correo de [monitorcactijf@gmail.com](mailto:monitorcactijf@gmail.com) hacia el correo empresarial de los administradores de red. La siguiente figura 10 nos muestra un correo de alerta por una notificación que el tráfico paso el 90% de su capacidad de transferencia.

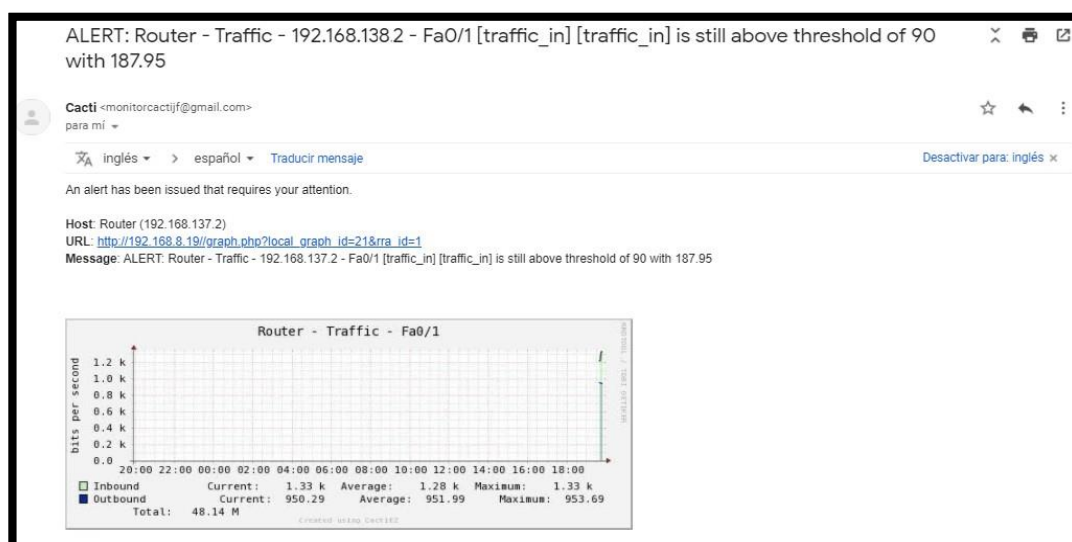


Figura 10: Alertas vía e-mail – Trafico Mayor 90%  
Fuente: Captura de Correo del Administrador de Red

En la figura 11, se visualiza el correo que es enviado desde Cacti, donde nos alerta que el servicio del dispositivo SW\_PISO2 se ha caído, lo cual también nos detalla el tiempo que se encuentra sin servicio.



Figura 11: Alerta del dispositivo down.  
Fuente: Captura de Correo del Administrador de Red

En la Figura 12, podemos ver de igual manera que Cacti envía la Alerta cuando el servicio del dispositivo 192.168.138.22 se volvió activar, lo cual también nos indica cual fue el tiempo que estuvo sin servicio.

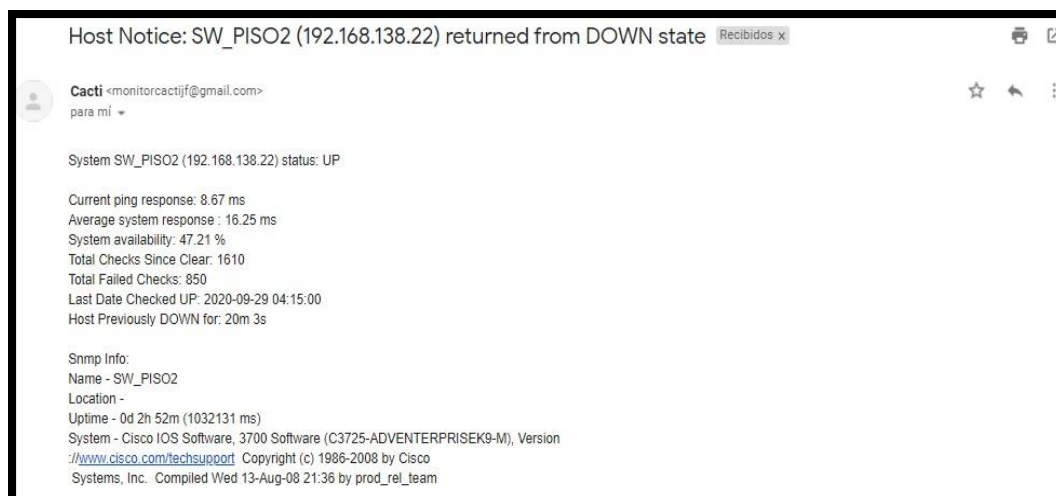


Figura 12: Alerta del dispositivo activado.  
Fuente: Captura de Correo del Administrador de Red

- Clasificación de Fallos

La clasificación de fallos depende de la gravedad de la incidencia, se tiene diferentes grados de alertas que son clasificados por colores, en la

siguiente tabla 2 se podrá visualizar los niveles de clasificación de fallos que se puede asignar libremente de acuerdo al criterio del área TI.

Tabla 2: Distribución de fallos en Cacti

<i>N°</i>	<i>SEVERIDAD</i>	<i>DESCRIPCION</i>
0	Emergencia	El sistema sin servicio
1	Alerta	Se deben tomar medidas de inmediato
2	Crítico	Estado críticas
3	Error	Estado de error
4	Peligro	Estado de peligro
5	Información	Condiciones normales pero notables
6	Aviso	Mensajes informativos
7	Depuración	Mensajes de bajo nivel

Fuente: Elaboración propia basada en la herramienta Cacti

- Registro de Incidencia - Ticket

Cada vez que ocurre un incidente en la red o una solicitud de usuario que se encuentra teniendo algún inconveniente con su conexión, todos estos requerimientos van registrado en la herramienta iTOP, donde el personal de HelpDesk apertura un ticket de acuerdo al área que se encuentre presentando la falla y luego se procede a asignar al personal quien atenderá el ticket. En la figura 13, se puede visualizar un resumen global, como también la cantidad de ticket que tienen asignado cada personal de HelpDesk y un diagrama circular dividido por prioridad.



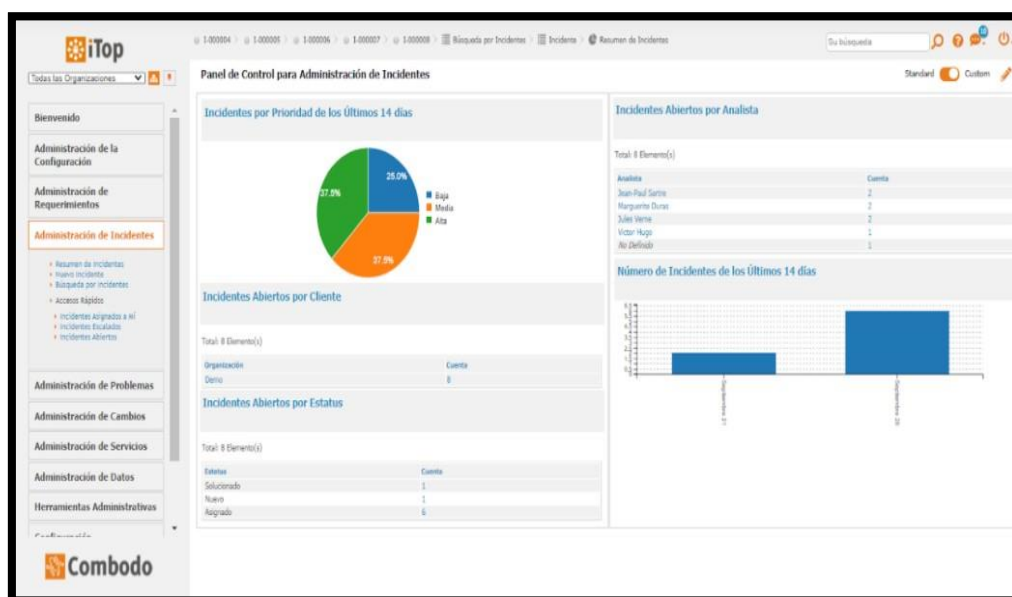


Figura 13: Panel de control para administración de incidente.  
Fuente: Captura del portal iTop

En la figura 14, podemos observar los tickets de incidencias o fallo como también las solicitudes de los usuarios que van reportando en el día a día para ser atendidas.

The screenshot displays the iTop 'Buscar Incidente' page. It shows a search bar and a table of incident tickets. The table has columns for Incidente, Asunto, Organización, Reportado por, Fecha de Inicio, Estatus, and Analista.

Incidente	Asunto	Organización	Reportado por	Fecha de Inicio	Estatus	Analista
1-000006	Sin Conexión a Internet	Demo	Eugene Delacroix	2020-09-28 08:03:20	Asignado	Julius Verne
1-000007	Sin Acceso	Demo	Agatha Christie	2020-09-28 08:02:13	Asignado	Julius Verne
1-000006	Sin Conexión a Internet	Demo	René Descartes	2020-09-28 08:00:21	Asignado	Marguerite Duras
1-000005	Saturación	Demo	Pablo Picasso	2020-09-28 07:58:16	Asignado	Victor Hugo
1-000004	SIN ACCESO A RED	Demo	Frida Kahlo	2020-09-28 07:55:41	Nuevo	No Definido
1-000003	Saturación	Demo	Eugene Delacroix	2020-09-28 07:47:37	Asignado	Marguerite Duras
1-000002	Sin Acceso A La Base Datos	Demo	Eugene Delacroix	2020-09-21 08:30:41	Asignado	Jean-Paul Sartre
1-000001	Sin Conexión a Internet	Demo	Agatha Christie	2020-09-21 08:03:13	Solucionado	Jean-Paul Sartre

Figura 14: Tickets de Incidencias y Solicitudes  
Fuente: Captura del portal iTop

### 3.6.3. Implementación de gestión de prestaciones

Para la implementación de la gestión de prestaciones tenemos una variedad de informes sobre el rendimiento del flujo red mediante estadísticas y gráficas.

**3.6.3.1. Monitoreo de las interfaces de los dispositivos.** En la interfaz gráfica del Cacti, se configuran las interfaces de los dispositivos en monitoreo, donde se pudo visualizar el flujo de tráfico de datos que pasa por cada interfaz de red, cabe resaltar, que el administrador de red puede configurar las interfaces que cree conveniente monitorear y cuáles no, teniendo en claro las buenas prácticas de monitoreo de gestión de red, se tuvo que configurar de manera estratégica sólo las interfaces que eran necesario a monitorear, para así evitar un consumo de memoria y CPU del equipo donde está instalado el software de monitoreo.

En la figura 15, figura 16 y figura 17, se puede visualizar el tráfico de los puertos Fa0/0 que están en monitoreo, con esto podemos tener un mayor control sobre el tráfico que pasa por cada interface de los dispositivos, tanto como el tráfico de entrada como el tráfico que sale de la interface, y así poder tener una mejor evaluación si en casa ocurra alguna saturación del enlace.

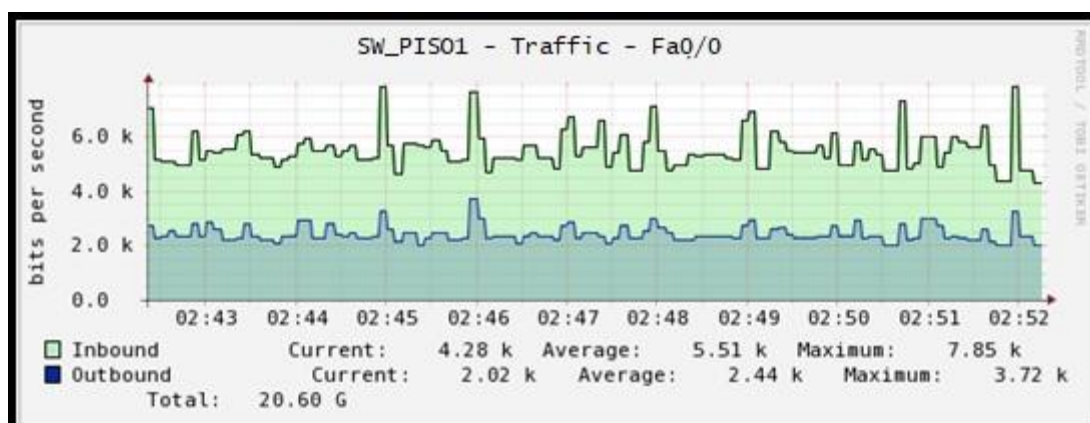


Figura 15: Tráfico de Entrada y Salida SW\_PISO1.  
Fuente: Captura Cacti Web

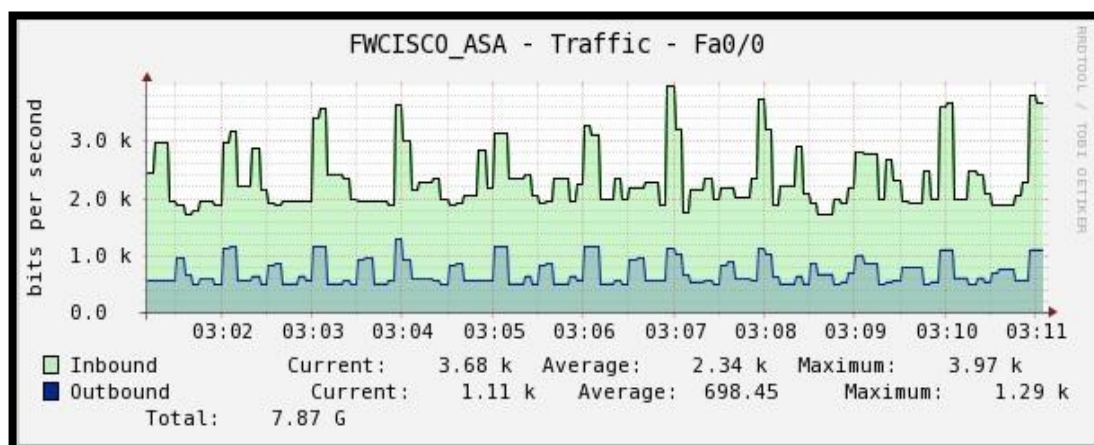


Figura 16: Tráfico de Entrada y Salida FWCISCO\_ASA.  
Fuente: Captura Cacti Web

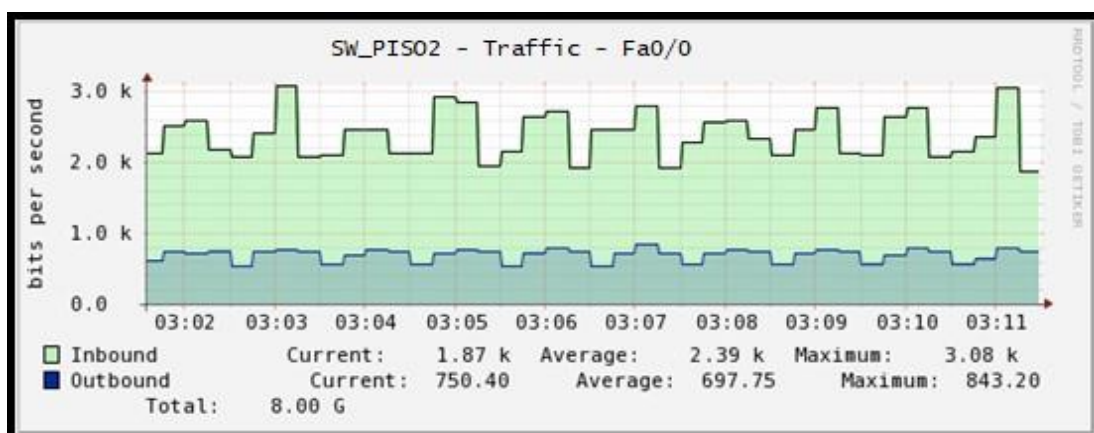


Figura 17: Tráfico de Entrada y Salida SW\_PISO2  
Fuente: Captura Cacti Web

#### - Switches

De acuerdo al esquema que se implementó, en base al diseño de red que se tiene en la empresa, se habilitó en el puerto FastEthernet 0/0 por el protocolo SNMP, para validar el tráfico de entrada y salida, y por buenas prácticas no se habilitó a los demás puertos ya que ellos iban conectado a otro equipo que están en monitoreo, donde tenían también

habilitado sus puertos por el protocolo SNMP. En la figura 18, podemos ver el tráfico de entrada y salida del dispositivo SW\_PISO3.

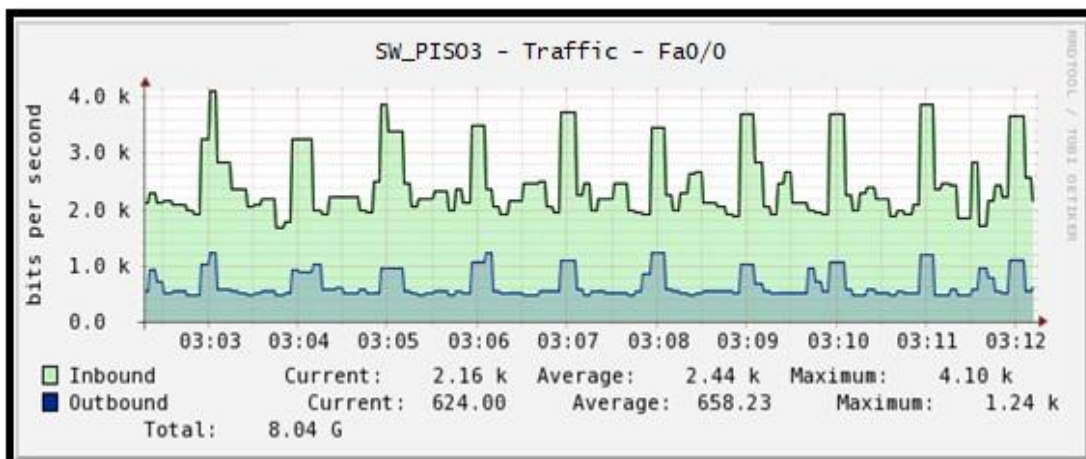


Figura 18: Tráfico de Entrada y Salida SW\_PISO3.  
Fuente: Captura Cacti Web

#### - Router

De acuerdo al esquema que se implementó, de igual manera que en el switch, en el router se habilitó en la interfaz g0/0 y en la g0/1, para tener un mayor control tanto en la interfaz LAN como en la WAN.

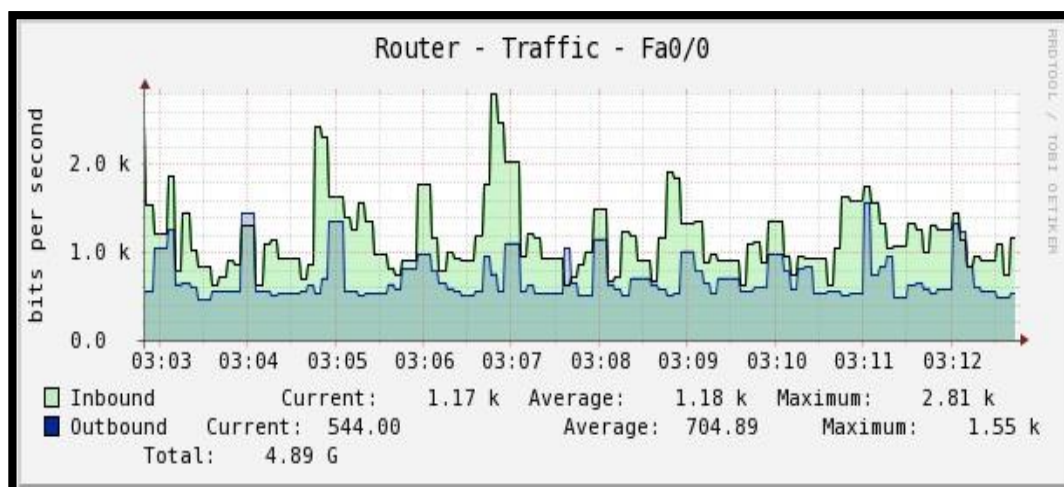


Figura 19: Tráfico de Entrada y Salida Router  
Fuente: Captura Cacti Web

De tal manera cuando algún usuario de la empresa presenta lentitud en su navegación web, se podría hacer un descarte visualizando la gráfica que haya estado ocurriendo alguna saturación en la red, así se podrá tener un reporte más eficiente y preciso del problema que está ocurriendo.

**3.6.3.2. Límites de rendimiento de los equipos en monitoreo.** Aquí establecimos las bases de rendimiento de acuerdo al tipo de equipo de red que se encuentre en monitoreo.

- Switch

En un dispositivo switch se consideró que menos del 60% de utilización del CPU es admisible para ser considerado que el switch está trabajando de manera óptima. En caso que este más del 50% de utilización del CPU, es considerado como un problema.

Debido a este parámetro establecido, el switch puede parecer que está funcionando con normalidad a esta capacidad de utilización de CPU, pero su comportamiento a distintos eventos de red se puede ver comprometida. En función al parámetro establecido definimos el 50% de utilización para el umbral de advertencia y un 70% para el umbral de criticidad.

Podemos decir que, en algunos escenarios de sistema de red, el uso de CPU con un alto consumo de su capacidad es común. Por lo que podemos decir que, mientras mayor es la red de Capa 3 o Capa 2, mayor se consume el CPU para procesar el tráfico en función a la red. En las siguientes líneas detallamos operaciones que producen alto nivel de uso del CPU:

- Comandos de Cisco IOS
- Actualizaciones de la tabla de enrutamiento IP
- Spanning Tree
- Protocolos de enrutamiento dinámico

La alta utilización del CPU en estas operaciones mencionadas es normal, como no puede causar ningún problema a la red. Cuando el alto consumo de CPU se transforma en un gran problema, el switch empieza a presentar anomalías y alta latencia.

De acuerdo a Cisco (2016) el uso de memoria debe estar por lo menos 30% de su capacidad de memoria libre. En función de esta pauta se definió los siguientes umbrales para el uso de memoria para la notificación, cuando llegue al nivel de utilidad del 50% es una notificación de advertencia y si llega a un nivel de utilidad del 70% es una notificación de criticidad.

- Firewall

De la misma manera en el CISCO ASA que se tiene en la data center, cuando llegue a un nivel de utilidad del 70% de uso de la CPU, esto puede llegar afectar el flujo de tráfico de red a través del Cisco ASA aumentando considerablemente. En el momento que el nivel de utilidad del CPU sobrepasa el 80%, Cisco ASA empieza a perder paquetes (Cisco, 2016). Por ello se estableció, cuando el umbral llega al 70% se notifica como una advertencia y de la misma manera cuando el umbral llega al 80% se notifica como crítica.

De acuerdo al uso de la memoria es similar a lo establecido en el Switch, siendo que cuando el umbral llegue a un 70% es considerado como una notificación de advertencia y si sobrepasa el 80% se considera como notificación crítica.

- Servidores

En la simulación que se tomó como ejemplo un Windows Server, de acuerdo a Microsoft (2005), el nivel de uso del procesador del servidor depende de la hora de actividad máxima, lo cual se debe considerar mantener una carga hasta el 60%. Por otro lado, si el procesador está por encima de los 70% de manera constante, se puede decir que el funcionamiento del procesador se vuelve un cuello de botella, para el tráfico de red.

En las siguientes líneas, se detalla algunos factores por los cuales el CPU de un servidor afectaría el rendimiento:

- El tipo de procesador
- El número de procesadores.
- La velocidad de reloj del procesador.

De acuerdo al uso de memoria, cuando el nivel de utilización se acerque al 100%, el servidor empezará a rechazar las aplicaciones que consuma la memoria o como también tendrá un periodo más largo en ejecutar algunas herramientas que ya están corriendo, con lo dicho en lo anterior el umbral de su capacidad para un servidor no debe exceder el 70% que se utiliza. Según lo mencionado, establecimos que el umbral cuando llegue al 60% se notificará como advertencia

- Access Point

De la misma manera que en el caso del switch cisco, se tomó como referencia el nivel de utilización del CPU, por lo que podría afectar de manera considerable al flujo de tráfico, debido a esto se estableció se estableció de la misma manera al 50% del uso de CPU se considera notificación de advertencia, y cuando esté por encima de los 70% del uso de CPU se considera una notificación crítica.

**3.6.3.3. Tabla de límites de rendimientos.** De acuerdo a lo anunciado en las líneas anteriores se procedió a establecer los límites de rendimientos de los equipos de red en monitoreo. Los cuales se expresan en la siguiente tabla 3.

Tabla 3: Límites de rendimientos

DISPOSITIVO	PARAMETRO	UMBRAL DE ADVERTENCIA	UMBRAL DE CRITICIDAD
Servidor	Uso de CPU	55%	65%
	Uso de Memoria	55%	65%
Firewall	Uso de CPU	65%	75%
	Uso de Memoria	65%	75%
Switch	Uso de CPU	50%	70%
	Uso de Memoria	50%	70%
Access Point	Uso de CPU	50%	70%
	Uso de Memoria	50%	70%

Fuente: Autor

### 3.6.4. Implementación de gestión de contabilidad

La implementación de la Gestión de Contabilidad es de mucha importancia debido a que recolectamos datos muy relevantes de la utilización de los componentes del hardware que se viene a usar, dado que luego se pueda alcanzar registros sobre los recursos que se tiene en el sistema red.

**3.6.4.1. Monitoreo de uso de memoria.** El uso de memoria de un dispositivo es un medio muy fundamental, ya que, si no se monitorea, en un caso donde se sobrepase sobre el límite permitido de uso de memoria perjudica el rendimiento del dispositivo.

Cacti te permite tener un mayor control de uso de memoria del dispositivo de manera gráfica, mostrándote así la memoria disponible como la memoria que está siendo consumida.

En la figura 20, se puede visualizar el uso del Switch, donde la parte roja es la memoria que está siendo utilizada y la porción azul es la memoria que se tiene libre.



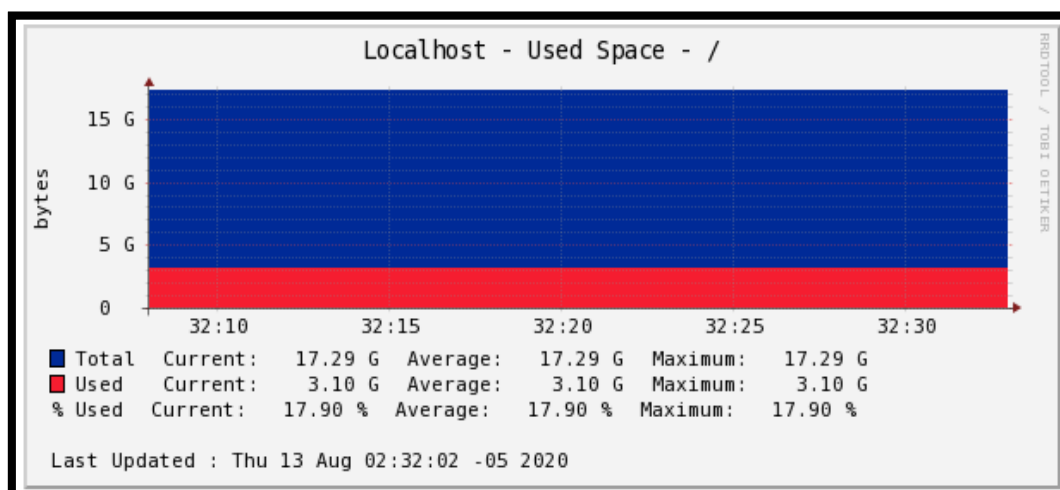


Figura 20: Consumo de Memoria.  
Fuente: Captura Cacti Web

**3.6.4.2. Monitoreo de uso de CPU.** En un dispositivo el monitoreo del uso de CPU es tan fundamental para tener un mayor control del consumo que se tiene. En cacti te muestra el uso del CPU en porcentajes, en la figura 21 te muestra el consumo por debajo de los límites permitidos, dado a eso no envié ninguna alerta. Figura 22, nos muestra el uso de CPU de un Access Point en porcentajes.

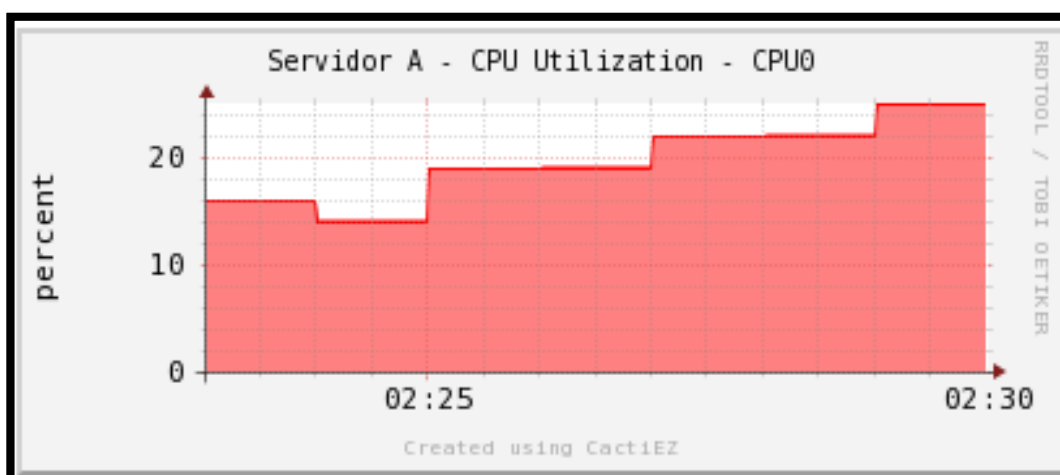


Figura 21: Consumo de CPU de Servidor A.  
Fuente: Captura Cacti Web

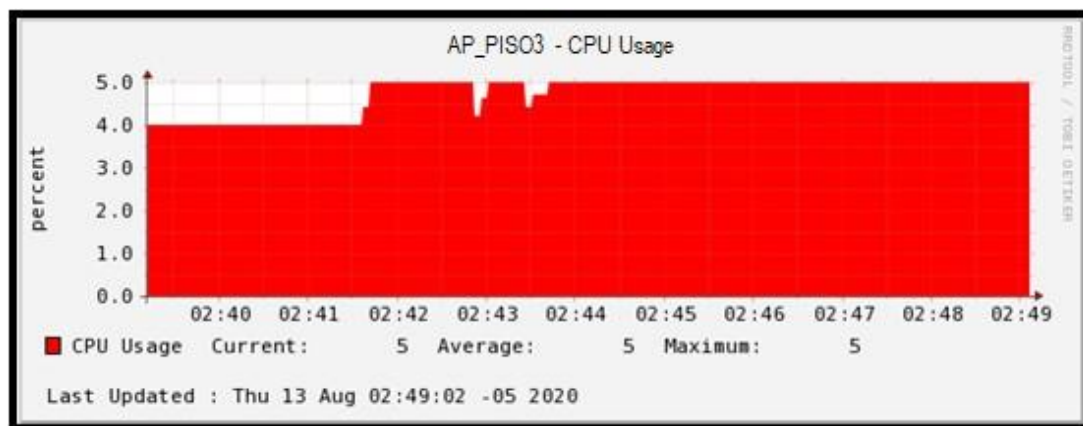


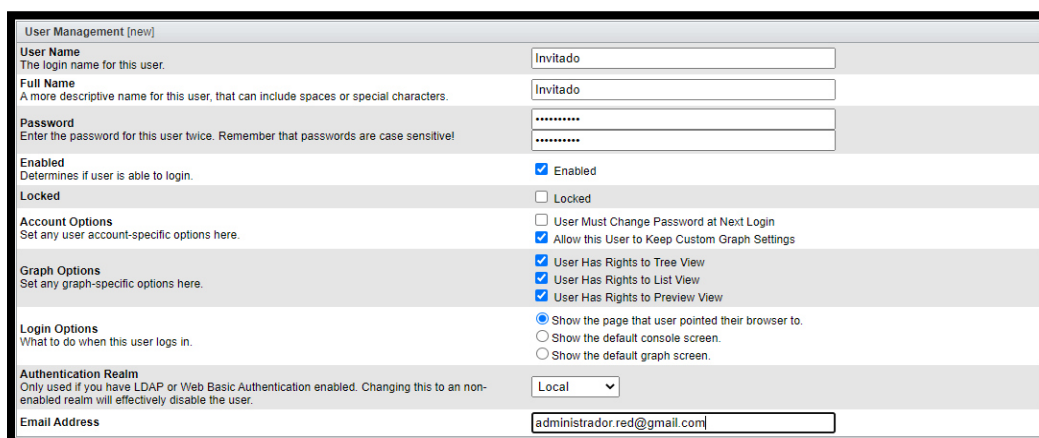
Figura 22: Consumo de CPU de AP\_PISO3.  
Fuente: Captura Cacti Web

### 3.6.5. Implantación de gestión de seguridad

**3.6.5.1. Acceso a la web de gestión de monitoreo.** El control hacia la Web del Cacti, se hizo por medio una PC que se encuentra conectada en la misma red e ingresando por un navegador y colocando la IP del servidor del Cacti.

En primer momento cuando ingresas a la interfaz web te solicita cambiar la contraseña, así mismo, se cambió la contraseña en base a las políticas de seguridad de la empresa, donde se solicita que la contraseña tenga un mínimo de 20 caracteres con una combinación en alfanuméricos entre mayúsculas y minúsculas.

En la figura 24, nos muestra la configuración de la contraseña del usuario “admin”, debido que por defecto la contraseña es “admin”. Así mismo en la figura 23, podemos crear otros usuarios administradores con ciertos privilegios o como también usuarios invitados que solo tienen permitido poder visualizar el flujo de tráfico de los dispositivos en monitoreo.



User Management [new]

**User Name**  
The login name for this user.

**Full Name**  
A more descriptive name for this user, that can include spaces or special characters.

**Password**  
Enter the password for this user twice. Remember that passwords are case sensitive!

**Enabled**  
Determines if user is able to login. ☒ Enabled

**Locked**  
☐ Locked

**Account Options**  
Set any user account-specific options here.

- ☐ User Must Change Password at Next Login
- ☒ Allow this User to Keep Custom Graph Settings

**Graph Options**  
Set any graph-specific options here.

- ☒ User Has Rights to Tree View
- ☒ User Has Rights to List View
- ☒ User Has Rights to Preview View

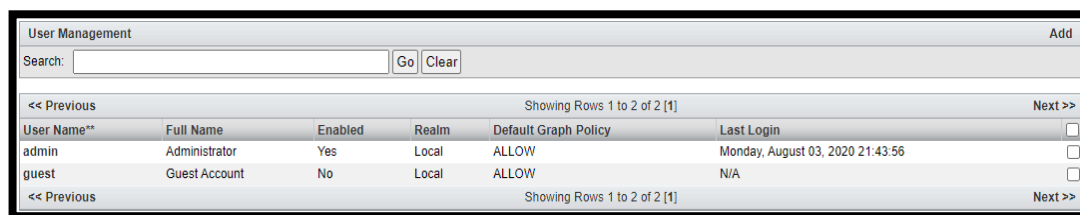
**Login Options**  
What to do when this user logs in.

- ☒ Show the page that user pointed their browser to.
- ☐ Show the default console screen.
- ☐ Show the default graph screen.

**Authentication Realm**  
Only used if you have LDAP or Web Basic Authentication enabled. Changing this to a non-enabled realm will effectively disable the user.

**Email Address**

Figura 23: Configuración de una cuenta de usuario  
Fuente: Captura Cacti Web



User Name**	Full Name	Enabled	Realm	Default Graph Policy	Last Login
admin	Administrator	Yes	Local	ALLOW	Monday, August 03, 2020 21:43:56
guest	Guest Account	No	Local	ALLOW	N/A

Figura 24: Usuarios de Cacti. Fuente: Captura Cacti Web

En la Figura 25, observamos todos los permisos que se le puede otorgar a un usuario, para tener una mejor gestión y un uso correcto del servidor de gestión.

Realm permissions control which sections of Cacti this user will have access to.

**Realm Permissions**

<input type="checkbox"/> User Administration	<input type="checkbox"/> Plugin -> Host MIB Admin
<input type="checkbox"/> Data Input	<input type="checkbox"/> Plugin -> Host MIB Viewer
<input type="checkbox"/> Update Data Sources	<input type="checkbox"/> Plugin Management
<input type="checkbox"/> Update Graph Trees	<input type="checkbox"/> MacTrack Viewer
<input type="checkbox"/> Update Graphs	<input type="checkbox"/> Plugin -> MacTrack Administrator
<input type="checkbox"/> View Graphs	<input type="checkbox"/> Maintenance Schedules
<input type="checkbox"/> Console Access	<input type="checkbox"/> View Monitoring
<input type="checkbox"/> Update Round Robin Archives	<input type="checkbox"/> Plugin -> Nectar Reports Admin
<input type="checkbox"/> Update Graph Templates	<input type="checkbox"/> Plugin -> Nectar Reports User
<input type="checkbox"/> Update Data Templates	<input type="checkbox"/> Plugin -> Realtime
<input type="checkbox"/> Update Host Templates	<input type="checkbox"/> Send Test Email
<input type="checkbox"/> Data Queries	<input type="checkbox"/> Plugin -> Syslog Administration
<input type="checkbox"/> Update CDEF's	<input type="checkbox"/> Plugin -> Syslog User
<input type="checkbox"/> Global Settings	<input type="checkbox"/> Plugin -> Configure Threshold Templates
<input type="checkbox"/> Export Data	<input type="checkbox"/> Plugin -> Configure Thresholds
<input type="checkbox"/> Import Data	<input type="checkbox"/> Plugin -> Manage Notification Lists
<input type="checkbox"/> Plugin -> Aggregate Administrator	<input type="checkbox"/> Plugin -> View Thresholds
<input type="checkbox"/> Plugin Automate -> Maintain Automation Rules	<input type="checkbox"/> Plugin -> Weathermap: Configure/Manage
<input type="checkbox"/> View Host Auto-Discovery	<input type="checkbox"/> Plugin -> Weathermap: View
<input type="checkbox"/> Plugin -> Flow Admin	<input type="checkbox"/> Access Webmin
<input type="checkbox"/> Plugin -> Flow Viewer	

Figura 25: Los Permisos Que se Puede Asignar al Usuario  
Fuente: Captura Cacti Web

**3.6.5.2. Seguridad en los dispositivos monitoreado.** Para tener una mejor seguridad en los equipos de red, se propuso usar la solución Nessus, esta herramienta se utilizó con el fin de realizar análisis de vulnerabilidades.

La herramienta Nessus home es un software Opensource que tiene la funcionalidad de escanear la red donde se encuentre mediante el uso de ciertas aplicaciones, donde en la figura 26 se muestra sus funcionalidades, solo las plantillas donde se encuentra el anuncio UPGRADE no está disponible para la versión home.

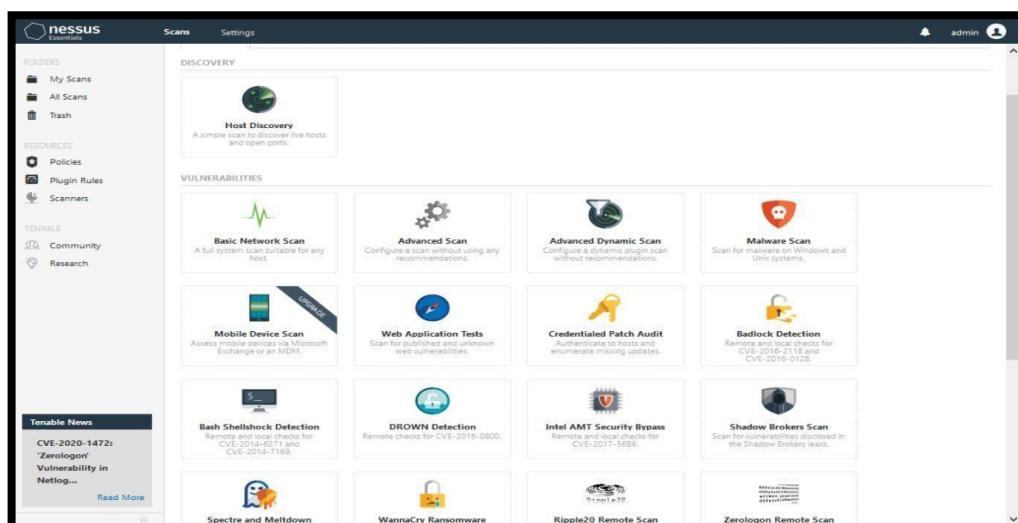


Figura 26: Plantilla de Nessus. Fuente: Captura Nessus

Para ejecutar la función de escaneo se selecciona la opción Advanced Scan, y luego proceder a configurar los parámetros de acuerdo a lo que se requiere como la dirección IP que se quiere escanear. Esta herramienta también te permite programar o ejecutar manualmente. La figura 27 se visualiza un escaneo simple de la red, como también de las vulnerabilidades que cuenta el dispositivo, lo cual se representan por colores.

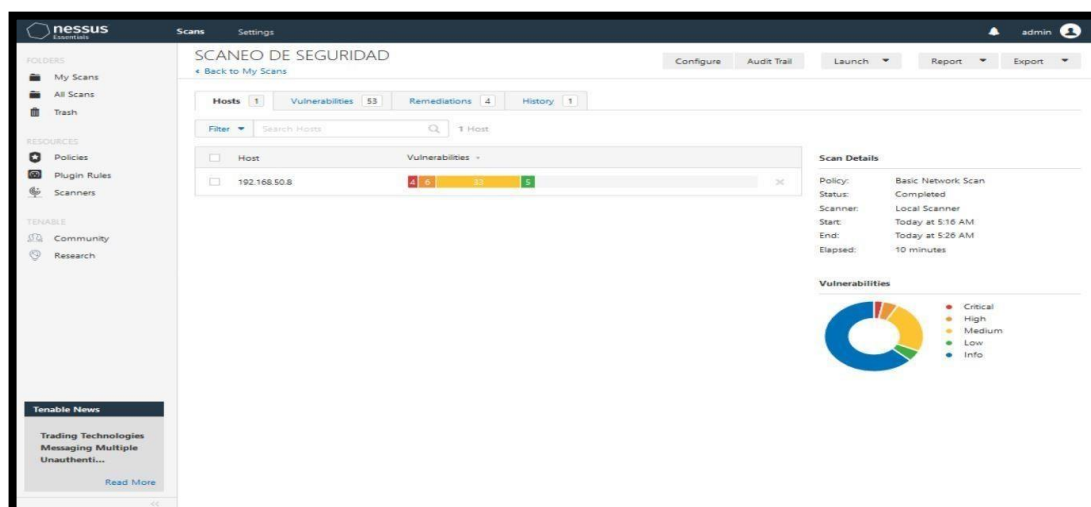


Figura 27: Escaneo del Equipo Por Su IP.  
Fuente: Captura Nessus

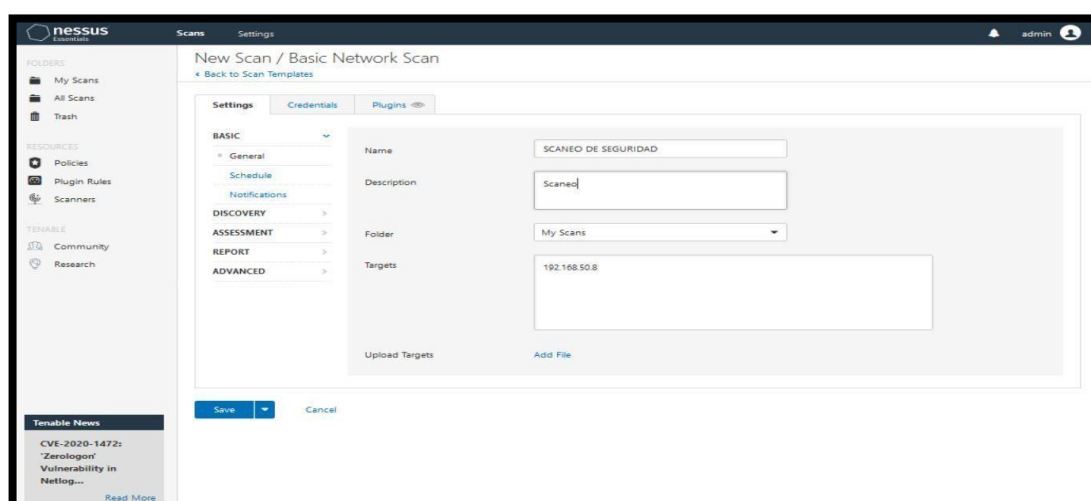


Figura 28: Escaneo del Equipo. Fuente: Captura Nessus

Cuando se ingresa a más detalles de las vulnerabilidades encontradas, esta herramienta presenta una descripción detallada por cada vulnerabilidad, así mismo, con la solución. En la figura 30, se tiene un informe de los puertos abiertos del equipo evaluado, los cuales son el 22, 80 y 443.

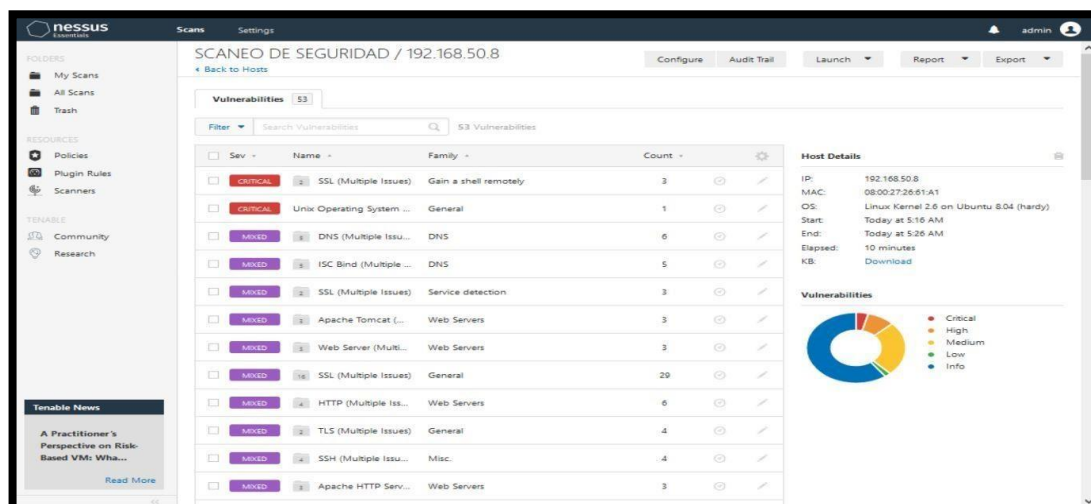


Figura 29: Vulnerabilidades Existentes. Fuente: Captura Nessus

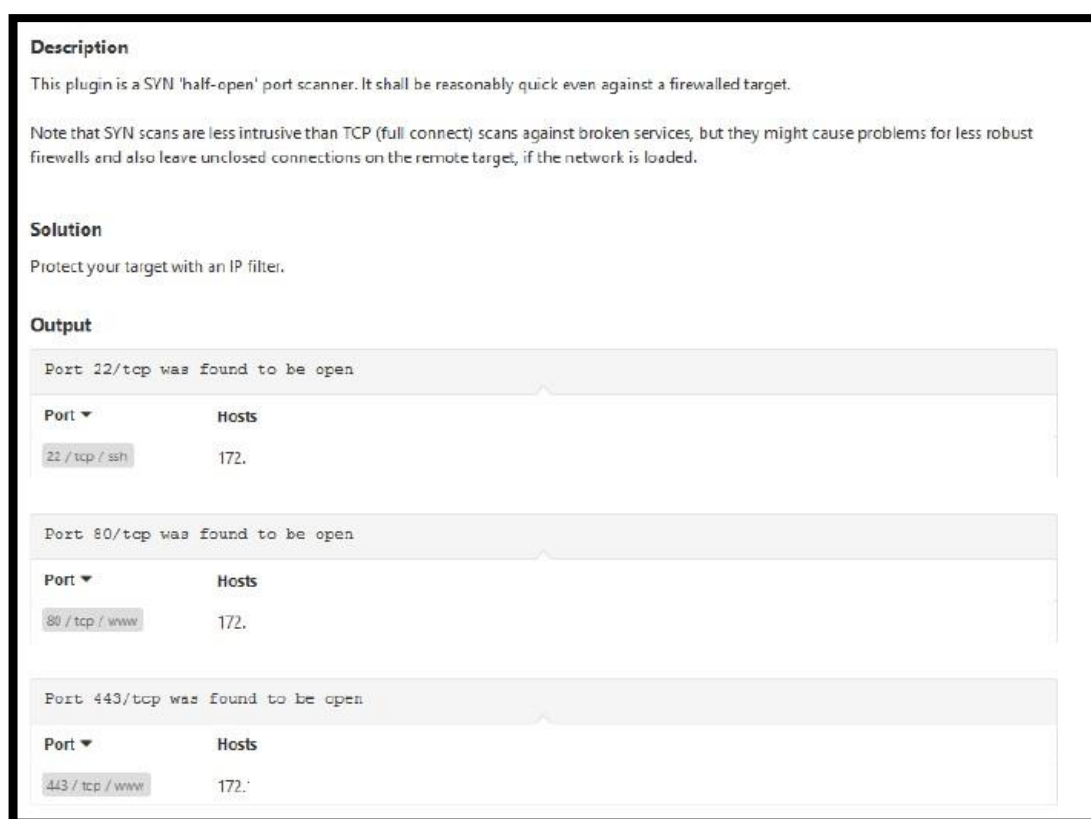


Figura 30: Reporte de Vulnerabilidad en Nessus.  
Fuente: Captura Nessus

## **IV. CONCLUSIONES**

### **4.1. Justificación**

En la actualidad, el rubro de las telecomunicaciones viene creciendo progresivamente en conjunto a ello, las prestaciones de servicio por parte de los proveedores de servicio de internet (ISP) cada vez se acopla hacia las medianas y pequeñas empresas, dado que algunos proveedores de servicio adicionalmente brinda herramientas de monitoreo a sus clientes que son gestionados por sus propios ingenieros asignados por parte del mismo proveedor de servicio, cabe explicar que, las empresas pymes que adquieren los servicios no tienen acceso directo a estas herramientas o no por completo, a partir de entonces los administradores de red de dicha empresa se ve sujeta a solicitar información sobre sus enlaces a ingeniero de nivel 1 a cargo de la gestión de la herramienta, como consecuencia a lo anterior se trabaja en la investigación de herramientas de monitoreo Open Source que puede ser instalado sin necesidad de comprar alguna licencia o permisos en cualquier equipo de red, con ello el administrador de red de la empresa tendrá la total libertad de poder controlar y gestionar sus propios enlaces, en caso que se presente una alerta, saturación o alguna falla en el enlace de sus sedes remotas, con esta información poder reportarlo lo más breve posible al proveedor de servicio de internet y así obtener una respuesta de solución más rápida, con la finalidad de mejorar la disponibilidad de sus enlaces.

La monitorización de redes es una parte fundamentales en las soluciones de red. Las herramientas de gestión le permiten evaluar y verificar la condición de su sistema de redes a un nivel simple y entendible; es decir, se le representa al tráfico de la red con gráficas, estadísticas y diagramas en



bloques entre otros, facilitando una mejor información para el administrador de red. Elegir una herramienta de monitoreo de red adecuada nos ayudara a detectar posibles problemas antes de que se produzca un colapso o una caída de las redes.

## 4.2. Metodología aplicada

### 4.2.1. Evaluación económica

En este apartado se evaluó un estudio del costo beneficio de la propuesta con la finalidad de obtener los costos y rentabilidad que obtendrá a la implementación del presente informe. Se evaluaron tanto el costo del hardware como el de software.

**4.2.1.1. Evaluación económica del software.** El costo del software se establece en base a las herramientas utilizadas en la implementación, que son el Cacti como herramienta de gestión y monitoreo de la red, el iTop como software de gestión de fallos y Nessus como software para la gestión de seguridad. Asimismo, se consideró el costo de la implementación y capacitación del software, lo cual se tiene un costo aproximado de \$200. En la siguiente tabla 4 se detallará el costo total del software.

Tabla 4: Costo de software

Software	Costo
<b>Licencia Cacti</b>	\$ 0,00
<b>Licencia iTop (free)</b>	\$ 0,00
<b>Licencia Nessus (Free)</b>	\$ 0,00
<b>Implementación y Capacitación en Software Libre</b>	\$ 200
<b>Total</b>	\$ 200

Fuente: Autor

**4.2.1.2. Evaluación económica del hardware.** Para el costo del hardware se determina tomando como referencia el servidor seleccionado donde se instalarán los softwares para la gestión de red, lo cual tiene un valor de \$862,31.

**4.2.1.3. Presupuesto final.** Se determinó que el presupuesto final para implementar este proyecto en la empresa, tomando en consideración los precios de software y hardware mencionados, se detalla en la siguiente tabla 5.

Tabla 5: Presupuesto final

Descripción	Presupuesto
Costo de Hardware	\$862,31
Costo de Software	\$200.00
Total	\$1062,31

Fuente: Autor

#### **4.2.2. Evaluación técnica**

En base al enfoque técnico, se puede obtener muchas mejoras en función a la disponibilidad de la red y al flujo del tráfico de datos. Las mejoras técnicas que se podrían obtener al ser implementada serían:

- Lleva un registro de los equipos gestionados de forma más ordenada.
- Permite detectar fallas o problemas con la red en un menor tiempo.
- Mejorar la disponibilidad del sistema de red.
- Tener una red más estable.
- El tiempo de solución de las incidencias sería mucho menor, lo cual aumentaría el tiempo de productividad de la empresa.

### 4.3. Descripción de la implementación

En este apartado se detallará los requerimientos de hardware donde sería optimo la implementación de los softwares de monitoreo, tomando como escenario la empresa donde se realizó el análisis para desarrollar el diseño propuesto. En la siguiente Figura 31 se representa el diseño físico del sistema red similar de la empresa.

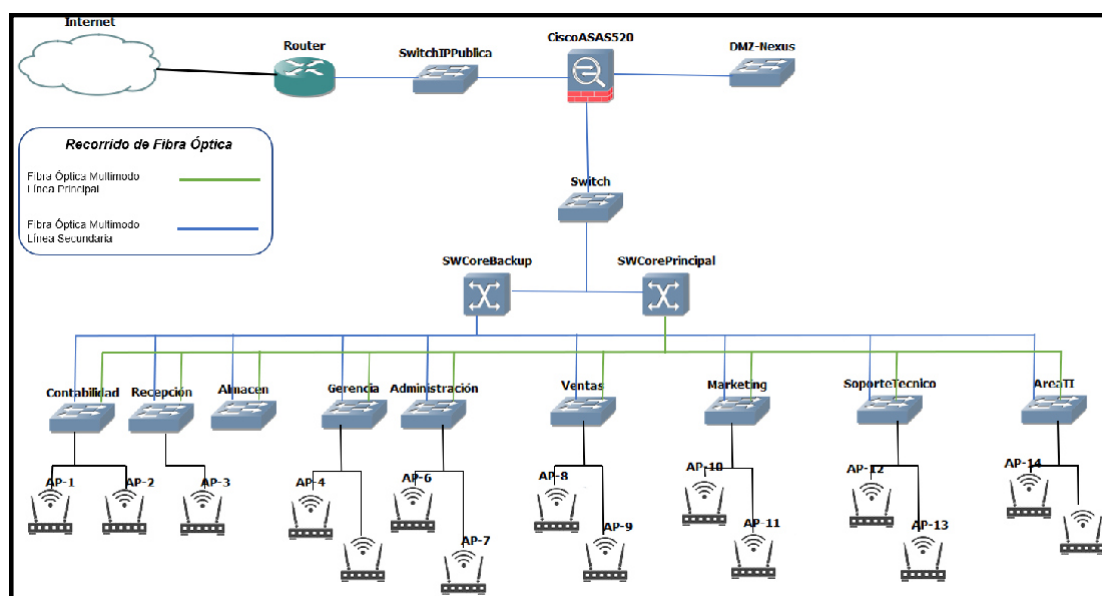


Figura 31: Diseño físico de sistema red de la empresa.

Fuente: Empresa

#### 4.3.1. Requerimientos de hardware

En base a la herramienta de monitoreo Cacti, que será implementado en un servidor que contenga como sistema operativo CentOS7. Las características del hardware deben contar con la arquitectura x86, donde se define en la siguiente tabla 6.

*Tabla 6:* Requerimientos de hardware para CentOS

Requerimiento	Mínimo	Recomendado
Procesador	1.1 GHz	1.1 GHz
Espacio de disco	20GB	40GB
Memoria	1GB	2GB

Fuente: Documentación de Cpanel

La herramienta Cacti suele demandar demasiado la capacidad del CPU, de acuerdo especialmente del número de parámetros utilizados y del motor de base de datos elegidos.

Los requerimientos básicos que debe tener el hardware es en función al tipo de empresa donde se implementará, en la siguiente tabla 7 se detalla los recursos de acuerdo al tipo de empresa.

*Tabla 7:* Requerimientos de hardware para Cacti

Empresa	CPU	Memoria	Disco duro	Hosts Gestionados
Pequeña	2 CPU Cores	2GB	40GB	100
Mediana	2 CPU Cores	2GB	80GB	500

Fuente: Autor

En base al número de equipos a gestionar, lo cual para este escenario es menor a 100, por ello la configuración recomendada donde se desarrolla el presente proyecto es pequeño.

#### 4.3.2. Selección del hardware de sistema de monitoreo de red

En este apartado evaluamos los recursos para el hardware del sistema de gestión red y precisa el dispositivo adecuado para su uso.

**4.3.2.1. Análisis de escalabilidad.** Actualmente se tiene una cantidad de 45 equipos considerando los router, switch, firewall, AP, servidores entre otros; no obstante, considerando la escalabilidad que tendrá la infraestructura de la red de la empresa, se determinó la tasa de crecimiento aplicando la ecuación (1). La Tabla 8 detalla el incremento de equipos de conmutación en los últimos 5 años.

Tabla 8: Escalabilidad de equipos

Año	Equipos de monitoreo
2016	34
2017	38
2018	38
2019	40
2020	45

Fuente: Empresa de referencia

$$Tasa\ de\ crecimiento = \frac{Preente-Pasado}{Pasado} \times 100 \quad (1)$$

$$Tasa\ de\ crecimiento\ 5\ años = \frac{45 - 34}{34} \times 100$$

$$Tasa\ de\ crecimiento\ 5\ años = 32.35\%$$

Lo cual se obtiene una escalabilidad del 32.35% de equipos en monitoreo en el periodo de los últimos cinco años. Con este análisis podemos llegar a concluir que la suma de dispositivos monitoreados para los próximos 5 años será de 59.




**4.3.2.2. Requerimientos del servidor.** Para definir las características básicas del servidor, primero identificamos los requerimientos de la

herramienta Cacti, lo cual requiere de un hardware con las siguientes características mínimas.

- CPU de 2 cores
- Permitir la instalación de distribuciones Linux
- Memoria RAM de 2GB
- Contar con un interfaz GigabitEthernet
- Disco duro de 40GB

Se realizó una tabla para contrastar entre ciertos servidores de diferentes fabricantes, considerando que cumplan con todas las características mencionadas en líneas anteriores. Dicha comparación se realiza con la finalidad de encontrar el equipo apropiado para la implementación de la herramienta de monitoreo Cacti.

*Tabla 9:* Evaluación de tres servidores

	<b>Dell PowerEdge T20</b> 	<b>IBM System x3100</b> 	<b>HP ProLiant ML110</b> 
<b>Fabricante</b>	DELL	IBM	HP
<b>Memoria instalada</b>	4GB	8GB	2GB
<b>Número de cores</b>	Quad-Core	Dual-Core	Dual-Core
<b>CPU</b>	Intel Xeon E3-1225 v3	Intel Xeon	Intel Xeon 3065
<b>Máximo tamaño de memoria</b>	32GB	8GB	8GB
<b>Memoria Cache</b>	8MB	4 MB	4 MB
<b>Disco duro</b>	1TB HDD	1 TB HDD	1 TB HDD
<b>Precio</b>	\$862,31	\$1223,60	\$1392,38

Fuente: HP, IBM y DELL

Según las características de los tres servidores de la tabla 9, el equipo más adecuado es el servidor Dell PowerEdge T20, debido a que cumple y supera con las características mínimas de CPU, memoria RAM y disco duro, por lo cual podemos decir que se estaría cumpliendo con la escalabilidad del sistema de monitoreo de gestión de red.

#### **4.4. Conclusiones**

El presente trabajo se llegó a demostrar la importancia de tener un sistema de herramienta de monitoreo para una empresa, sin la necesidad de costear ninguna licencia y usando solo herramientas open sources, así cualquier pequeña o media empresa debería gestionar el suyo propio

La gestión y monitoreo de la red LAN de la empresa es fundamental debido que permite al área TI como el administrador de red tener mayor control de los recursos, así mismo poder supervisar el rendimiento de los equipos de red, de manera que se pueda analizar y evaluar de una forma más temprana algún fallo o incidente que se esté presentando y pueda ser resuelto en un tiempo menor.

El análisis de información con referencia al modelo de gestión OSI se puede implementar de manera correcta, lo que nos permite dar a conocer ciertos criterios que deben cumplirse para la implementación, en función de sus cinco áreas funciones: gestión de rendimiento, gestión de contabilidad, gestión de configuración, gestión de fallos y gestión de seguridad.

Con esta implementación la empresa estaría cumpliendo los términos y cláusulas de la ISO 9001, la cual es velar por un sistema de gestión de calidad para aumentar la productividad, reducir los costos innecesarios y garantizar la calidad de los procesos y productos.

Con esta implementación la empresa estaría cumpliendo ciertos términos y cláusulas de la ISO 27001, dado que con esta propuesta estaríamos cumpliendo con disponibilidad de la información de los sistemas y aplicaciones de una organización.

La presente propuesta es de gran valor para todo negocio o empresa PYME, debido que permite una gestión y monitoreo adecuada para la toma de acciones preventivas y/o correctivas en la monitorización de los equipos que se encuentran conectados a la red.

Así mismo, el costo de lo adquirido es lo mínimo a lo que podría ser si se implementa un software con licencia, por lo que estas herramientas de gestión Open Source permite tomar las acciones preventivas necesarias para poder evitar pérdidas de dinero generadas en el intervalo de tiempo donde se queda sin acceso a la red y además tomar acciones correctivas de una forma más adecuada teniendo como visión la herramienta de gestión y poder tomar una mejor decisión correctiva, por lo tanto, todo esto tiene como finalidad brindar una mejor atención para el cliente y no tener pérdidas de dinero.



## **V. RECOMENDACIONES**

El personal encargado de monitorear la red con la herramienta propuesta, debe revisar y analizar de manera constante las fallas que pueden presentar y evaluar las alertas producidas por la herramienta de monitoreo, y así evitar que la incidencia se convierta en un problema crítico.

Para el servidor Cacti, se recomienda brindar los recursos necesarios de memoria, con la finalidad que el software de monitoreo contenga un nivel de productividad óptimo a pesar que se adicionen nuevos dispositivos en el futuro.

De ser necesario, asignar plantillas adicionales para la notificación de fallas, ya sea por saturación, alta latencia, con el fin de obtener registros que puedan ayudar a prevenir o identificar una posible incidencia que pueda ocurrir durante el horario de trabajo.

Si el administrador de red implementa un nuevo equipo de red a su sistema, se recomienda, validar que el nuevo equipo soporte el protocolo SNMP por lo menos la versión 2, para que pueda ser adicionado sin ningún inconveniente y pueda estar sujeto a la monitorización constante.

Se recomienda que el personal de TI encargado del monitoreo y control de la red, debe capacitarse constantemente en las futuras aplicaciones que viene saliendo así aprovechando los beneficios que trae la nueva tecnología.

## VI. BIBLIOGRAFIA

Barba Martí, Antoni (1999) *Gestión de Red*, Barcelona - España

Recuperado de: [https://es.scribd.com/document/106303438/Gestion-](https://es.scribd.com/document/106303438/Gestion-De-Red-Antoni-)

[De-Red-Antoni-](#)

[Barba-Marti-UPC #logout](#)

Stallings, William (1999) *SNMP, SNMPv2, SNMPv3, and RMON 1 and2*.  
3ra Edición. Recuperado de:

<http://www.gbv.de/dms/ilmenau/toc/572061714.PDF>

Berry, Ian (2017) *The Cacti Manual*. Recuperado de:

<https://cacti.net/downloads/docs/pdf/manual.pdf>

Cisco (2016) Recuperado de:

[https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750/software/troubleshooting/cpu\\_util.html](https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750/software/troubleshooting/cpu_util.html)

[http://www.uelbosque.edu.co/sites/default/files/publicaciones/revistas/revista\\_tecnologia/volumen2\\_numero1/gestion\\_integrada\\_telecomunicaciones2-1.pdf](http://www.uelbosque.edu.co/sites/default/files/publicaciones/revistas/revista_tecnologia/volumen2_numero1/gestion_integrada_telecomunicaciones2-1.pdf)

Cisco (2016) recuperado de:

<https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/113185-asaperformance.html>

Marcos Jorquera, Diego (2010) *Difusión masiva de información en los modelos de gestión de redes*. Alicante – España. Recuperado de:

[https://rua.ua.es/dspace/bitstream/10045/20061/1/Tesis\\_Marcos.pdf](https://rua.ua.es/dspace/bitstream/10045/20061/1/Tesis_Marcos.pdf)

Microsoft (2013) recuperado de:

[https://docs.microsoft.com/es-es/previous-versions/exchange-server/exchange-server-2000//bb124583\(v=exchg.65\)?redirectedfrom=MSDN](https://docs.microsoft.com/es-es/previous-versions/exchange-server/exchange-server-2000//bb124583(v=exchg.65)?redirectedfrom=MSDN)

Molero, Luis (2010) Planificación y Gestión de Red. Recuperado de:  
<https://www.urbe.edu/info-consultas/web-profesor/12697883/archivos/planificacion-gestion-red/Unidad-I.pdf>

Padilla Benítez, René Damian (2015) Propuesta de modelo de gestión de infraestructura de red, basado en las mejores prácticas de gestión de TI y los modelos estándar de gestión red – caso de estudio EP Petroecuador, Quito – Ecuador. Recuperado de:

<https://bibdigital.epn.edu.ec/bitstream/15000/15092/1/CD-6904.pdf>

Valera, C. (2003). Gestión integrada de telecomunicaciones y el modelo TMN de la UTI. Recuperado de:

[http://www.uelbosque.edu.co/sites/default/files/publicaciones/revistas/revista\\_tecnologia/volumen2\\_numero1/gestion\\_integrada\\_telecomunicaciones2-1.pdf](http://www.uelbosque.edu.co/sites/default/files/publicaciones/revistas/revista_tecnologia/volumen2_numero1/gestion_integrada_telecomunicaciones2-1.pdf)

