UNIVERSIDAD NACIONAL DE SAN CRISTÓBAL DE HUAMANGA

FACULTAD DE INGENIERÍA DE MINAS, GEOLOGÍA Y CIVIL

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

"IMPLEMENTACIÓN DE UN SERVIDOR COMO GESTIÓN Y MONITOREO DE SERVICIOS PARA LA RED DE DATOS EN LA UGEL HUAMANGA, 2018"

Tesis Presentada por	: Bach. Omar Jesús Fernández Huaytalla
Para optar el título profesional de	: Ingeniero de Sistemas
Tipo de Investigación	: Observacional, Retrospectivo, Longitudinal, Analítico
Asesor	: Ing. Karel Peralta Sotomayor

Ayacucho – Perú

2019

DEDICATORIA

A mi esposa e hijos Matías y Angelina, que son la razón de todo mi esfuerzo y así alcanzar el éxito, además de recibir todo el amor, cariño, estímulo, apoyo constante, comprensión y paciencia.

A mi madre y tía por ser el pilar fundamental en todo lo que soy, en toda mi educación, tanto académica, como de la vida, por su incondicional apoyo.

AGRADECIMIENTO

A Dios quién supo guiarme por el buen camino, dándome la fuerza para seguir adelante y no desmayar en los problemas que se presentaban, enseñándome a encarar las adversidades sin perder nunca la dignidad ni desfallecer en el intento.

A todos los docentes de la Universidad Nacional de San Cristóbal de Huamanga especialmente de la carrera de Ingeniería de Sistemas por compartir sus conocimientos, por su esfuerzo en cada una de sus labores y por permitirme formarme como un gran profesional.

CONTENIDO

CAPÍTULO III

METODOLOGÍA DE LA INVESTIGACIÓN

CAPÍTULO IV

ANÁLISIS Y RESULTADOS DE LA INVESTIGACIÓN

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

Índice de Tablas

Índice de Figuras

RESUMEN

Las telecomunicaciones y en particular el campo de las redes de datos son áreas de constante desarrollo e innovación, en la actualidad la gran mayoría de empresas y entidades educativas utilizan redes de datos como base para sus comunicaciones y como plataforma para brindar servicios.

En la UGEL Huamanga a medida que va creciendo la red de datos la carga de información que viaja a través de la red va disminuyendo, lo cual produce una gran congestión en el tráfico de tal manera que satura el ancho de banda, haciendo que el servicio sea de calidad baja y poco satisfactoria para el uso de los trabajadores que requieren una conexión eficiente.

El objetivo de la presente investigación es implementar un servidor como gestión y monitoreo de dispositivos y servicios, mediante el protocolo SNMP, tecnologías de virtualización, Sistema Operativo CENTOS 7, Nethserver 7, herramientas Open Source como Ntopng, Suricata y Zabbix con la finalidad de monitorear el consumo de ancho de banda, análisis de todo el tráfico en el firewall en busca de ataques y anomalías conocidos y verificar el correcto funcionamiento de elementos de hardware y software para la red de datos.

El estudio se realizó en la UGEL Huamanga, el tipo de investigación es observacional, retrospectivo, longitudinal y analítico y el nivel de investigación es aplicada.

A partir de la implementación, el administrador de red podrá obtener la interfaz de graficas de la carga del CPU, el tráfico que atraviesa la red, que servicios son lo que más usan el CPU, monitorización de los recursos de un host (carga del procesador, uso de los discos, logs del sistema) en varios sistemas operativos como son los que utilizan los servidores, controlar el consumo del ancho de banda a través de túneles SSL cifrados o SSH, Chequeo de servicios paralizados. reportes y estadísticas del estado cronológico de disponibilidad de servicios y hosts.

PALABRAS CLAVE: Gestión y monitoreo, red de datos, UGEL Huamanga, dispositivos y servicios, Protocolo SNMP, host. tecnologías de virtualización, CENTOS 7, Nethserver 7, Open Source, Ntopng, Suricata y Zabbix.

INTRODUCCIÓN

Según (Ford & Lew, 1998) la gestión y monitoreo es el seguimiento, vigilancia y control permanente hacia los diferentes equipos de comunicación (router, switch, firewall, IPS, IDS, etc.) y servicios mediante el uso de un software especializado el cual censa constantemente la red en busca de componentes defectuosos o lentos, para luego notificar a los administradores de red a través de diferentes medios (SMS, correo electrónico, alertas pop-up, etc.). (p. 96)

"La gestión y administración de una red requiere de instrumentos adecuados tanto en hardware como en software, los mismos que deben ser los elementos de mayor eficiencia junto con toda la infraestructura de red especializada" (Becerra, 2016, pág.10).

La motivación que me impulsa a investigar e implementar un servidor desarrollado en software libre es que ofrece los mismos servicios que los que manejan licencia pagada; por otra parte, se cuenta con el soporte de muchos usuarios a nivel mundial que continuamente brindan su aporte para mejorar y actualizar las diversas herramientas y aplicaciones que ofrecen beneficios para una empresa.

Contar con un servidor como gestión y monitoreo de dispositivos y servicios basado en el protocolo SMNP, que permita monitorizar el estado de un enlace punto a punto y detectar cuando este congestionado, es decir hacer que el servidor envié una alerta cuando la carga sea demasiado elevada. SNMP también permite la modificación remota de la configuración de un ordenador a través de su agente SNMP, además se implementará herramientas para monitorear el ancho de banda, así como el control de intrusos no identificados a la red.

Los principales objetivos específicos son: a) Definir las variables que permita almacenar la Base de Información (MIB) usadas por el protocolo SNMP para supervisar y controlar los componentes en la red de datos. b) Establecer las configuraciones del protocolo SNMP en los dispositivos y servicios que permita el intercambio de información y así supervisar el correcto funcionamiento de la red. c) Implementar la estación de gestión (NMS) que muestra la interfaz web para el manejo de herramientas que extrae información de la base de datos de los dispositivos y servicios que maneja la red**.**

CAPÍTULO I
PLANTEAMIENTO DEL PROBLEMA

1.1 DIAGNÓSTICO Y ENUNCIADO DEL PROBLEMA

La estructura de la red de la UGEL Huamanga; a medida de los años se ha ido expandiendo y el consumo de los servicios de red e internet ha sido más frecuente, el cuál produce una gran congestión en el tráfico de tal manera que satura el ancho de banda, haciendo que el servicio sea de calidad baja y poco satisfactoria para el uso de los trabajadores que requieren una conexión eficiente.

Es así que surge el problema en las redes LAN y WLAN que mientras mayor es el tamaño de consumo se vuelve más compleja y complica el mantenimiento de los enlaces de comunicación, la administración de los dispositivos que conectan las diferentes áreas en la institución y monitorear los servicios de la red.

Para la Oficina de Informática y Sistemas desconoce la información acerca del tráfico que atraviesa la red, el enlace que satura el ancho de banda y los servicios que hacen que la carga de servidores sea elevada hace imposible tener una red de telecomunicaciones en buen estado. Actualmente se tienen servidores instalados y configurados que controlan la salida hacia páginas de radio, música, televisión, vídeo, descargas, sin embargo, el esquema de administración de estos servidores se basa en listas de control de acceso y verificación de urls fáciles de vulnerar utilizando programas como puente que vulneran la seguridad, ocasionando el incremento de tráfico de red, afectando la distribución del ancho de banda disponible.

Por otra parte, la Oficina de Informática y Sistemas no cuenta con un sistema que le permita gestionar y monitorear los diferentes componentes y servicios que conforman la red, solamente se hace uso de un aplicativo “Wireless Network Watcher” que es una pequeña utilidad que escanea la red y muestra la lista de todas las computadoras y dispositivos que están actualmente conectados a la red. Estas limitaciones traen como resultado el no poder llevar a cabo las acciones necesarias y así no poder actuar de manera oportuna ante la presencia de un corte en

los servicios y consumo de banda ancha. De esta manera el no tener la posibilidad de mantener el control de una manera remota de toda la red provoca la pérdida de tiempo y molestias en las labores del personal que labora en la UGEL Huamanga.

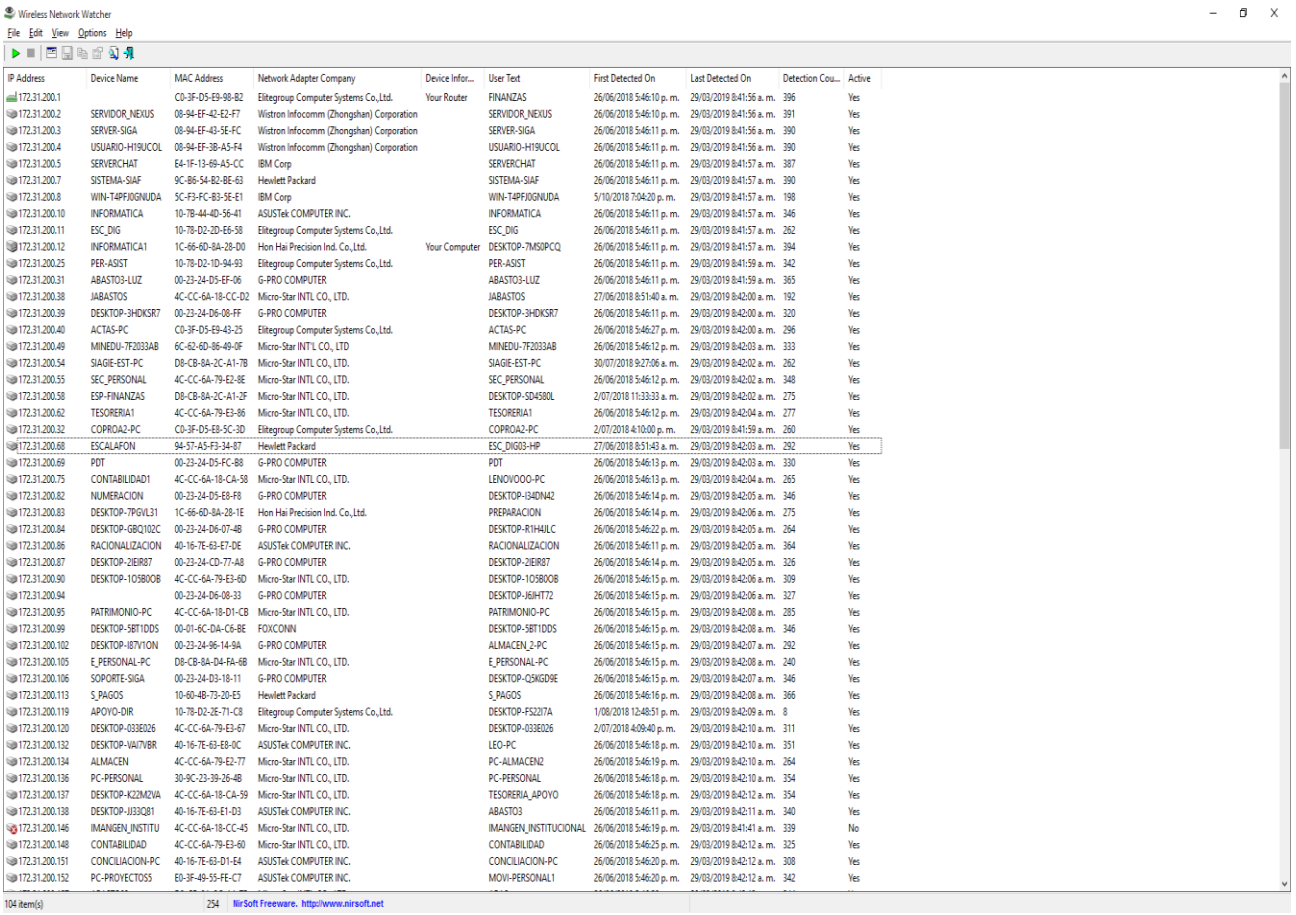


Figura N° 1. Escaneo de la red en la UGEL Huamanga

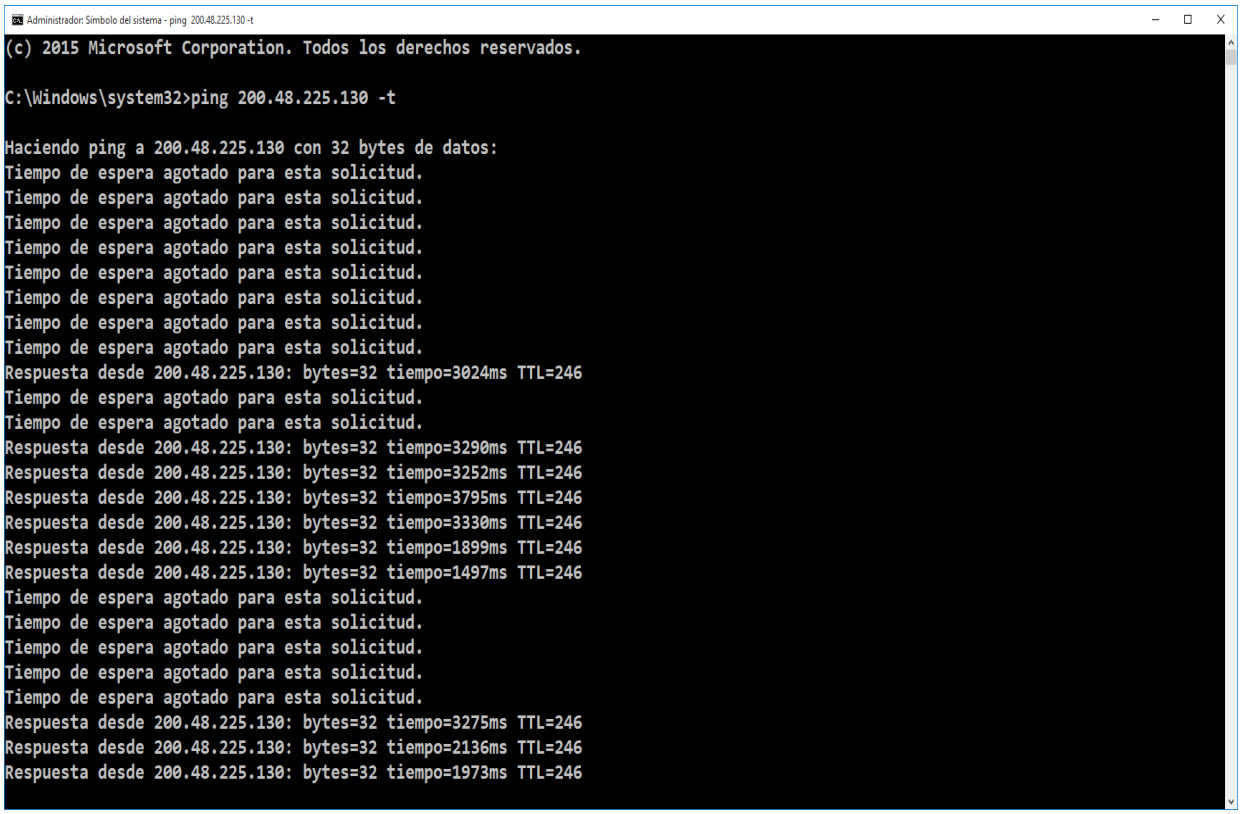


Figura N° 2. Ping a la Dirección IP del servicio de internet (200.48.225.130)

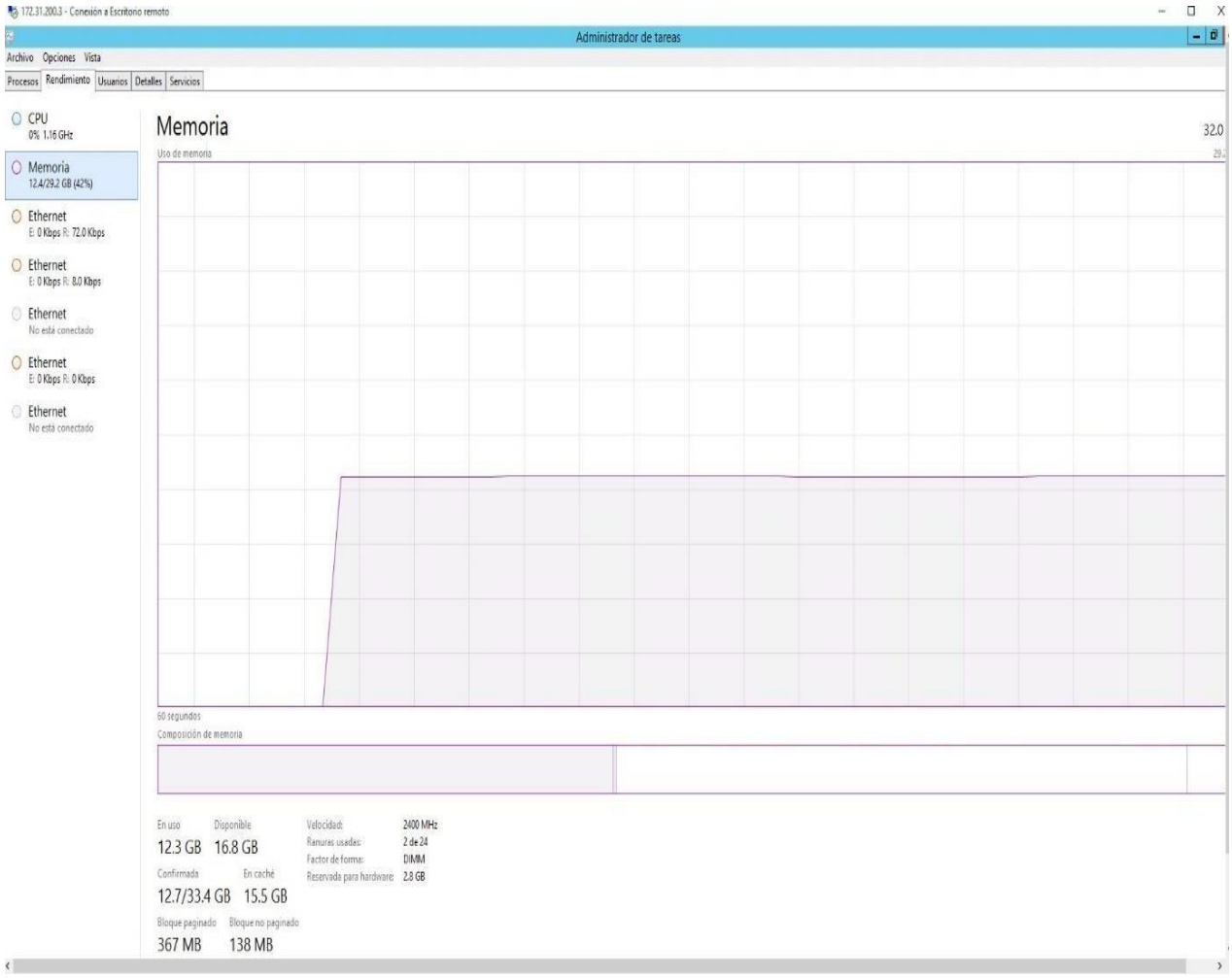


Figura N° 3. Rendimiento de Recursos de Memoria del Servidor

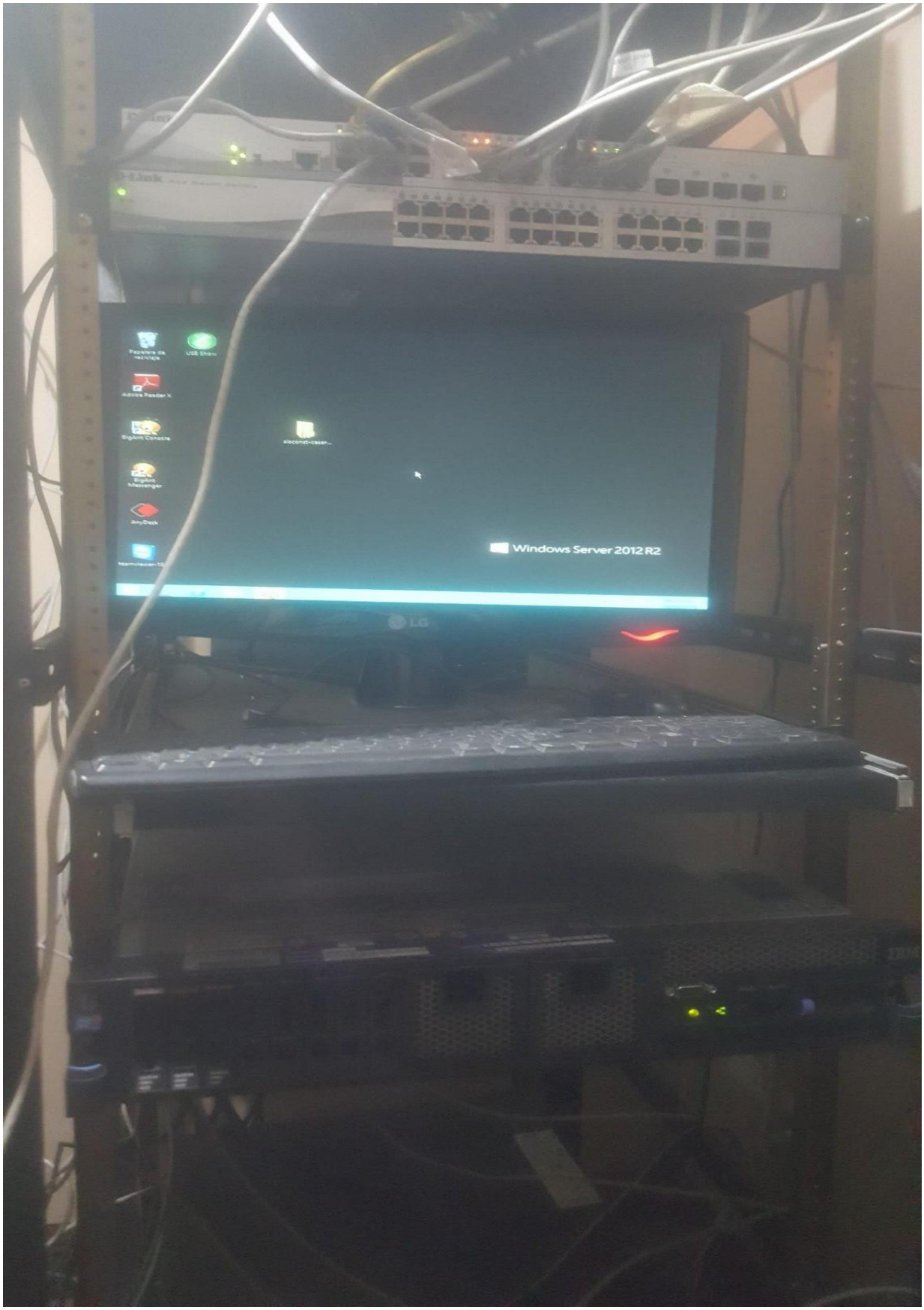


Figura N° 4. Equipos y Servidores de la red de datos

1.2 FORMULACIÓN DEL PROBLEMA DE INVESTIGACIÓN

1.2.1 PROBLEMA PRINCIPAL

¿De qué manera, la implementación del servidor realizará la gestión y monitoreo de servicios y dispositivos de modo que pueda el rastrear todos los dispositivos conectados, recursos y consumo de ancho de banda en la red de datos de la UGEL Huamanga, 2018?

1.2.2 PROBLEMAS SECUNDARIOS

a) ¿De qué manera la base de información (MIB) podrá gestionar los recursos respecto a la red de datos?

b) ¿Cómo podrá intervenir el protocolo SNMP, de tal manera que se ajuste a las necesidades de monitoreo de los servicios y dispositivos de la red de datos?

c) ¿De qué manera la estación de gestión (NMS) podrá determinar el resultado de monitorear e identificar los problemas en los dispositivos y servicios, control de ancho de banda y detección de intrusos a la red de datos?

1.3 OBJETIVOS DE LA INVESTIGACIÓN

1.3.1 OBJETIVO GENERAL

Implementar un servidor como gestión y monitoreo de dispositivos y servicios, mediante el protocolo SNMP, tecnologías de virtualización, Sistema Operativo CENTOS 7, Nethserver 7, herramientas Open Source como Ntopng, Suricata y Zabbix y como instrumento de buenas prácticas la guía de fundamentos para la dirección de proyectos (PMBOK) con la finalidad de monitorear el consumo de ancho de banda, análisis de todo el tráfico en el firewall en busca de ataques y anomalías conocidos y verificar el correcto funcionamiento de elementos de hardware y software para la red de datos.

1.3.2 OBJETIVOS ESPECÍFICOS

a) Definir las variables que permita almacenar la Base de Información (MIB) usadas por el protocolo SNMP para supervisar y controlar los componentes en la red de datos.

b) Establecer las configuraciones del protocolo SNMP en los dispositivos y servicios que permita el intercambio de información y así supervisar el correcto funcionamiento de la red de datos.

c) Implementar la estación de gestión (NMS) que muestra la interfaz web para el manejo de herramientas que extrae información de la base de datos de los dispositivos, servicios y el tráfico que maneja la red de datos.

1.4 JUSTIFICACIÓN Y DELIMITACIÓN DE LA INVESTIGACIÓN

1.4.1 IMPORTANCIA DEL TEMA

IMPORTANCIA TÉCNICA

Dentro del aspecto técnico contar con un servidor de gestión y monitoreo, conllevará a una labor muy importante y con características pro-activas que buscarán evitar problemas a los administradores y encargados ya que podrá mejorar la actual realidad de la red de datos de la UGEL Huamanga y optimizar la infraestructura, pues además el uso de software libre le dan aún más factibilidad, de tal manera que puedan tener el control del estado y conocimiento de los recursos de la red en los equipos de comunicación todo el tiempo y los usuarios dispondrán de ellos de mejor manera.

IMPORTANCIA ECONÓMICA

Para el aspecto económico la implementación del servidor y la utilización de herramientas Open Source permitirá agilizar la atención de los posibles incidentes, debido al monitoreo permanente y a la funcionalidad de las alarmas, que realicen notificaciones en línea y ejecuciones de planes de contingencia o prevención en tiempo real, de esta manera se evita gastos innecesarios al hacer contrataciones con otras empresas que brindan el mismo servicio, pero con costos elevados por las licencias.

1.4.2 JUSTIFICACIÓN

La UGEL Huamanga necesita tener un servidor que gestione y monitoree los dispositivos y servicios de la red de datos, controlar el estado de todos los enlaces conectados y detectar cuando este congestionado, es decir hacer que el servidor envié una alerta cuando este saturado los recursos, el ancho de banda y los servicios que hacen que la carga de servidores sea elevada. Es así que se obtiene una visión amplia de lo que se puede hacer con el

funcionamiento del protocolo SNMP de monitoreo de red, realizar una auditoría de sistemas según las necesidades que tiene la UGEL Huamanga.

1.4.3 DELIMITACIÓN

La investigación se realizará en la UGEL Huamanga, abarcando los diferentes dispositivos y servicios que tiene la infraestructura de la red de datos de la UGEL Huamanga en el año 2018.

CAPÍTULO II
REVISIÓN DE LA LITERATURA

2.1 ANTECEDENTES DE LA INVESTIGACIÓN

Según, (Arias Figueroa, 1999) “Herramientas de Gestión basada en Web” trabajo de tesis para la obtención de Magister en Informática de la Universidad Nacional de La Plata, La Plata Argentina; indica que el principal beneficio de los mecanismos de Gestión basados en Web es que se tiene que conocer a detalles los protocolos de gestión para manejar dispositivos remotos. Adicionalmente esto permite abstraer los diferentes protocolos y unificarlos con una única visión. Por otra parte, hace un énfasis en muchas características como seguridad, eficiencia, costo, interfaz amigable, etc. Del mismo modo intenta desarrollar un conjunto de herramientas que sean rápidamente implementables y permitan al Ingeniero de red realizar algunas operaciones de administración en agentes del tipo pc/routers, ver estadísticas, estado y evolución de estos dispositivos.

Según (Becerra Orrala, 2016) “Implementación de monitoreo de red utilizando los Protocolos ICMP y SNMP” proyecto de tesis para la obtención del título de Ingeniería en Electrónica y Telecomunicaciones de la Universidad Estatal Península de Santa Elena de La Libertad, Ecuador; concluye que se establecieron los requerimientos del sistema de monitoreo para la generación y recolección de información, implantando así el monitoreo del tráfico de red interno y externo, realizando las respectivas pruebas de monitoreo de interfaces de red consumo de procesador y memoria en equipos compatibles con el protocolo SNMP; y por último se comprobó el monitoreo ICMP hacia equipos principales de la red.

Para (Botero Arana, 2005) “Modelo de gestión de seguridad con soporte a SNMP” proyecto de grado presentado para optar el título de Ingeniero de Sistemas de la Pontificia Universidad Javeriana, Bogotá Colombia; menciona que para asegurar que el sistema de gestión y monitoreo funcione de una manera eficiente y garantizada debe tener los siguientes componentes NMS (Network management station), NMA (Network management Aplication), MIB (Management information Base), NE (Network Element), MA (Management Agent), estos componentes interactúan entre sí para lograr tener un eficiente envió e interpretación de traps (interrupciones) y así que administrador de red puede tomar decisiones acertadas.

Por otra parte (Bonilla, Iván, & Lozada, 2013) “Herramienta OpenSource De Administración Y Monitoreo Basado En SNMP Para El Mejoramiento Del Funcionamiento De La Red En Speedy Com Cia Ltda” proyecto de tesis para obtener el título de Ingeniero Electrónico de la Universidad Técnica de Ambato, Ambato Ecuador; concluye lo siguiente. La implementación de la herramienta Zenoss para la administración y monitoreo de la red mediante el protocolo SMNP, resultó de gran utilidad ya que se optimizó la gestión del administrador en cuanto a detección y solución de problemas presentados en la red, reduciendo de esta forma tiempo hombre y recursos, que se usaban antes de la implementación de la herramienta, además la productividad de la red de datos mejoró haciendo que las aplicaciones no presenten problemas.

Según (Saldarriaga & Huila, 2015) “Implementación de un Sistema de Gestión y Administración de Redes Basados en el Protocolo Simple de Monitoreo de Redes SNMP en la Red ESPOL- FIEC” trabajo de tesis para la obtención de título de Ingeniero Electrónico de la Escuela Superior Politécnica del Litoral, Guayaquil Ecuador; menciona que con el Protocolo SNMP se crea un agente especialmente diseñado para administrar la red que se encarga de recorrer el Árbol MIB que posee la Información detallada de cada equipo. Es decir que para realizar una administración de redes basados en el protocolo SNMP se puede realizar mediante software que implemente este protocolo, o mediante hardware con equipo que especialmente son diseñados para determinadas funciones.

Según (Jardinez & Ruiz, 2012) “Propuesta de un Sistema de Monitoreo para la Red ESIME ZACATENCO utilizando el Protocolo SNMP y Software Libre” proyecto de tesis para obtener el título de Ingeniero en Comunicaciones y Electrónica del Instituto Politécnico Nacional México D.F. México; concluye que al usar la herramienta Nagios se obtienen las capacidades necesarias para poder llevar a cabo el monitoreo de una red de área local utilizando el protocolo SNMP. La ventaja de esta herramienta de monitoreo es el poder visualizar los estados y gráficas de los diferentes objetos administrados desde cualquier punto de la red utilizando un navegador web teniendo precaución en asignar un nombre de usuario y contraseñas que siguieran las políticas de la escuela, con esto los administradores de la red no tendrían que estar siempre al lado del servidor Nagios para poder acceder a la información.

2.2 MARCO TEÓRICO

2.2.1 GESTIÓN Y MONITOREO

En la gestión y monitoreo de (Saydam & Magedanz, 1996) definen lo siguiente:

> La gestión y monitoreo incluye el despliegue, integración y coordinación del hardware, software y los elementos humanos para controlar, probar, sondear, configurar, analizar, evaluar y controlar los recursos de la red para conseguir los requerimientos de tiempo real, desempeño operacional y calidad de servicio a un precio razonable. (p. 345)

La gestión y monitoreo es la faceta que se ocupa de controlar el funcionamiento y el mantenimiento de una red de datos. Para ello se utiliza un conjunto de protocolos y técnicas que conjuntamente pueden garantizar el funcionamiento del sistema y el acoplamiento del mismo a las necesidades de funcionamiento diario de los organismos que las utilizan**.** (Sanchez, 2015, pág. 34)

2.2.2 COMPONENTES DE MONITOREO DE RED

Las redes soportan aplicaciones y servicios estratégicos de las organizaciones y requieren de una permanente supervisión de todos sus componentes, a fin de conocer oportunamente situaciones críticas como son las interrupciones de servicios, ataques a dispositivos, tráficos anómalos o comportamientos dentro de la red que requieren de la intervención del encargado para evitar colapsos o saturaciones que puedan poner en riesgo la continuidad de la operación. (Magnini & Cavaglia, 2000, pág. 1413)

Monitorear un servidor de red significa que el administrador conocerá si uno o todos sus servicios están caídos. La monitorización del servidor puede ser interna (el software del servidor se verifica y notifica de los problemas al administrador) o externa. (Donde se verifica manualmente). Durante el monitoreo se verifican características como el uso de CPU, uso de memoria, rendimiento de red y el espacio libre en disco e incluso las aplicaciones instaladas (como Apache, MySQL, entre otros). (Magnini & Cavaglia, 2000, pág. 1415)

2.2.3 MONITOREO ACTIVO

Para (Magnini & Cavaglia, 2000) define lo siguiente:

Este tipo de monitoreo se realiza introduciendo paquetes de pruebas en la red, o enviando paquetes a determinadas aplicaciones y midiendo sus tiempos de respuesta. Este enfoque tiene la característica de agregar tráfico en la red y es empleado para medir el rendimiento de la misma. Puede ser basado mediante protocolo ICMP, obteniendo los siguientes beneficios: (p.1418)

a. Diagnosticar problemas en la red.
b. Detectar retardo, pérdida de paquetes.
c. RTT
d. Disponibilidad de host y redes.

2.2.4 MONITOREO PASIVO:

Este enfoque se basa en la obtención de datos a partir de recolectar y analizar el tráfico que circula por la red. Se emplean diversos dispositivos como routers, computadoras con software de análisis de tráfico y en general dispositivos con soporte para SNMP. Este enfoque no agrega tráfico a la red como lo hace el activo y es utilizado para caracterizar el tráfico en la red y para contabilizar su uso real. Entonces una red monitoreada está compuesta por los siguientes componentes: (Magnini & Cavaglia, 2000, pág. 1419)

a. Dispositivos
b. Interconexión
c. Servidores
d. Red de administración

Figura N° 5 Estación de Monitoreo del Pasado

Fuente: (Magnini & Cavaglia, 2000, pág. 1420)

2.2.5 ESTACIÓN DE GESTIÓN (NMS)

"Un gestor o una estación de gestión, es una estación que ejecuta un cliente de SNMP. Una estación gestionada, denominada agente, es un dispositivo que ejecuta un servidor de SNMP. La gestión se realiza a través de una sencilla interacción entre el gestor y el agente" (Laporta, 2006, pág. 343).

Para (Morris, 2003) respecto a la estación gestión (NMS) menciona lo siguiente:

> Que el gestor es una estación de trabajo donde se ejecutan las aplicaciones de gestión de red, que disponen de interfaces gráficas para presentar información al usuario y para facilitarle la invocación de operaciones de gestión. Es la parte de la aplicación que emite las directivas de operaciones de gestión y recibe notificaciones y respuestas. Este se implementa en una estación de gestión. Integran la información asociada con varios sistemas gestores de elementos, usualmente ejecuta una correlación de alarmas entre los diversos gestores de elementos. En estos sistemas se debe recolectar la información necesaria acerca de la fuente (objeto gestionado), reducirla a algo significativo y presentarla en la consola central para su análisis. (p.78)

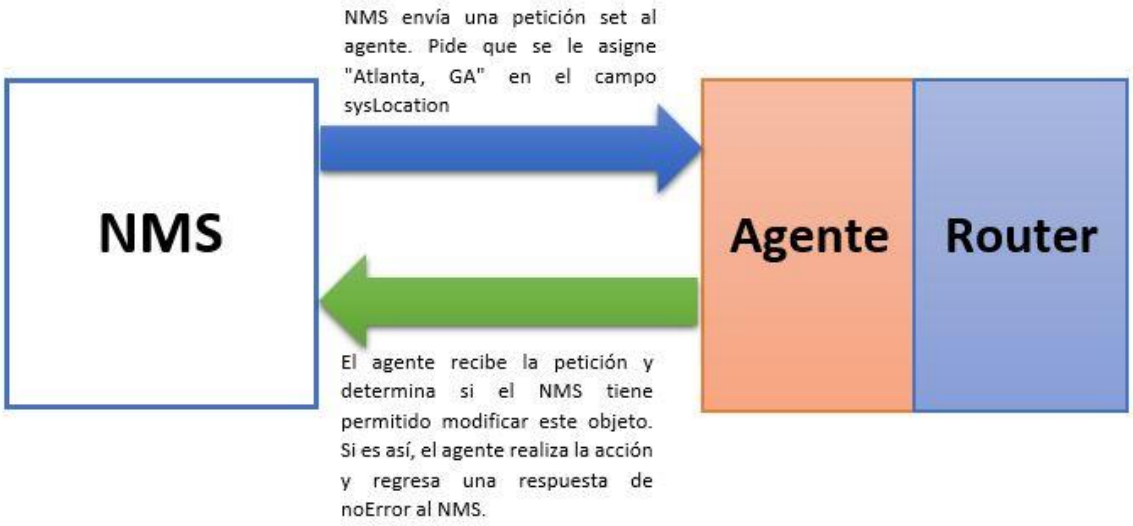


Figura N° 6. Petición NMS- Agente

Fuente: (Morris, 2003, pág. 82)

2.2.6 AGENTE

El agente almacena información sobre prestaciones en una base de datos MIB (Management Information Base). El agente tiene acceso a los valores de esta base de datos, la cual puede leer y comparar los valores de estas dos variables para actualizar los datos a mostrar. Cada agente crea su propia MIB con base en el dispositivo en el que esté instalado. Los objetos en la MIB se clasificarán en ocho grupos: sistema, interfaz, traducción de direcciones, ip, icmp, tcp, udp, y egp. Estos grupos se encuentran bajo el objeto MIB en el árbol de identificadores de objetos. Cada grupo tiene variables definidas y/o tablas. (Verón, 2010, pág. 74)

El agente es el equipamiento lógico alojado en un dispositivo gestionable de la red. Almacena datos de gestión y responde a las peticiones sobre sobre dichos datos. Cuya función es, por un lado, recoger información de los eventos que se producen en el dispositivo, y por otro comunicarse con el gestor. (Lopez, 2017, pág. 36)

Para (Sanz, 2006) considera que: “El agente es otro elemento activo del sistema que responde las solicitudes de acción desde la estación de gestión, pudiendo proporcionar información de una manera síncrona o también asíncrona de información importante y no solicitada. Este agente está alojado en los dispositivos gestionados” (p.5).

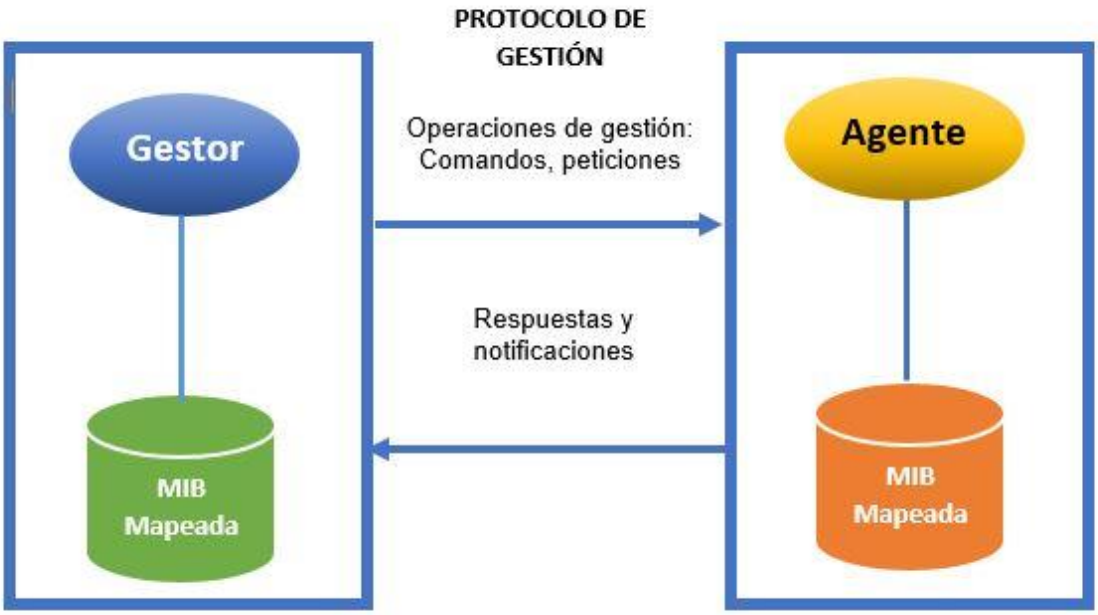


Figura N° 7. Relación Gestor - Agente

Fuente: (Sanz, 2006, pág. 7)

2.2.7 GESTIÓN DE FALLAS

La gestión de fallas no se limita al monitoreo, incluye también el ciclo de vida de la falla de un componente de la infraestructura de TIC, lo que hace posible dar seguimiento a la falla (el estado del equipo, del segmento, de la red completa o del sistema) desde que se recibe la alarma o incluso desde antes, y hasta que el problema se solucione por completo. La gestión de fallas puede interactuar y complementarse con información proveniente de otros dominios de gestión (como desempeño, inventario, u otro) y puede, a su vez, proveer información para complementar otros dominios de gestión**.** (Abricot, 2017)

2.2.8 GESTIÓN DE CONFIGURACIONES

Para (Abricot, 2017) define que: “El objetivo de la gestión de configuraciones es tener información sobre cada dispositivo de la red en lo que respecta a sus capacidades y a su actual configuración, así como llevar un control de los cambios que ocurran”.

2.2.9 GESTIÓN DE PERFOMANCES

Dentro de lo que es la performance, se debe poder observar y analizar la utilización de la red, de manera que se pueda determinar el estado y eficiencia de la misma, así como el poder definir tendencias y poder preparar los requerimientos de la red en un futuro. Además del ancho de banda utilizado puede ser conveniente analizar parámetros tales como tasas de error, paquetes eliminados, tiempos de latencia, entre otros. Deber ser posible definir límites, que de ser sobrepasados generen una alerta. (Abricot, 2017)

2.2.10 BASE DE INFORMACIÓN (MIB)

La Base de Información, también conocida como MIB es una colección de objetos almacenados por el agente. Los objetos son parámetros que identifican cada componente del dispositivo mediante un valor numérico denominado OID (Object Identifier), que puede ser actualizado por el agente o pedido por una fuente externa, como un gestor. (Hucaby, 2002, pág. 87)

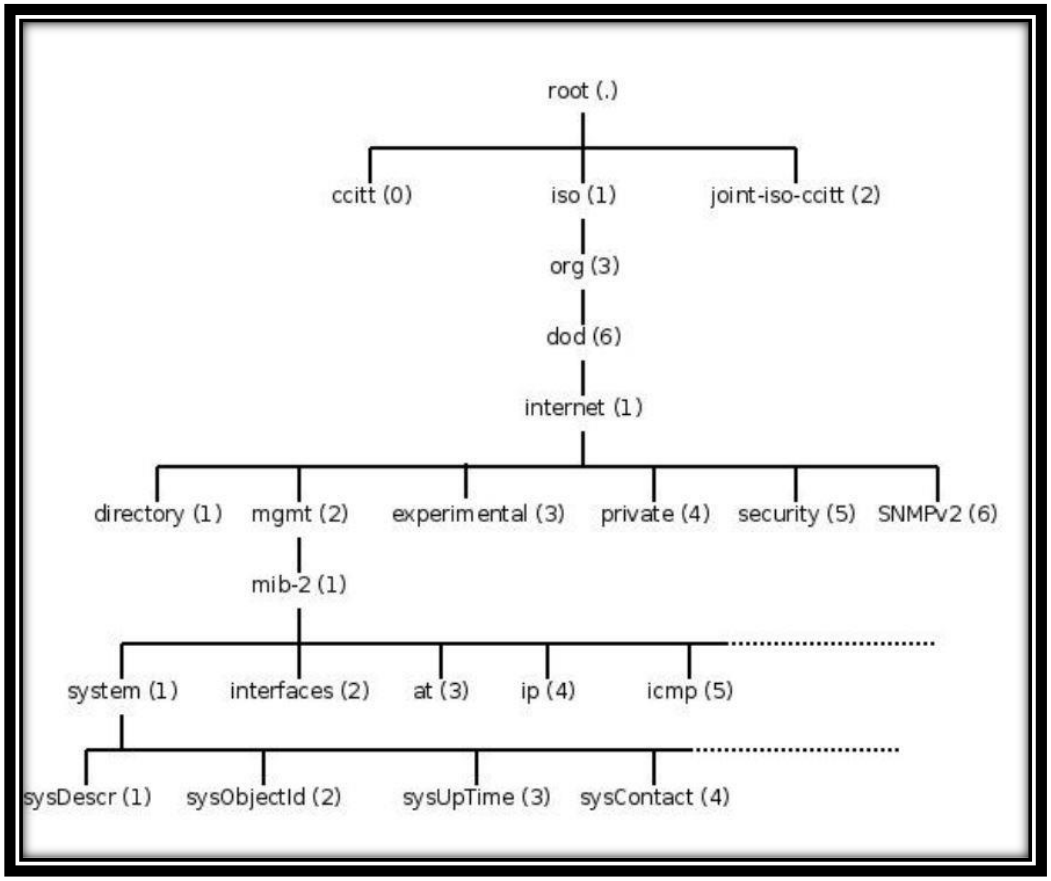


Figura N° 8. Estructura de una MIB

Fuente: (Hucaby, 2002, pág. 87)

Los objetos administrados están compuestos de una o más instancias de objeto, que son esencialmente variables. Existen dos tipos de objetos administrados: escalares y tabulares. Los objetos escalares definen una simple instancia de objeto. Los objetos tabulares definen múltiples instancias de objeto relacionadas que están agrupadas conjuntamente en tablas MIB. (Rose & McCloghrie, 1991, pág. 137)

2.2.11 SNMP (Simple Network Management Protocol)

Para (Mauro, 2008) el protocolo SNMP lo define como:

El Protocolo Simple de Administración de Red (Simple Network Management Protocol) es un protocolo de internet para el manejo de dispositivos dentro de redes IP y pertenece a la capa de aplicación. Existen muchos tipos de dispositivos que soportan SNMP, como por ejemplo están los ruteadores, switches, servidores, estaciones de trabajo, impresoras, así como UPS ("Uninterruptible Power Supply: Suministro de Energía Ininterrumpible").

Por otra parte, (Ford & Lew, 1998) considera lo siguiente:

El protocolo SNMP para manejar y monitorear dispositivos y servicios de redes, se basa en paquetes UDP, protocolo de la capa de transporte, basado en IP, compatible con SMNP. UDP es un protocolo sin conexión que no garantiza la entrega del paquete, por lo tanto, SMNP es un protocolo no orientado a la conexión y utiliza los puertos 161 y 162. El protocolo SNMP corresponde a la capa de aplicación del modelo de referencia OSI. El utilizar UDP implica que no se establece una sesión entre el NMS y los agentes, lo cual hace que las transmisiones sean más rápidas y que la red no se sobrecargue, pero también implica que el que envía los mensajes debe, por algún medio, asegurar que este ha sido recibido, en el caso del sondeo el NMS puede esperar un tipo por la respuesta y, en caso no está reciba, se puede reenviar el paquete. (p.63)

A. VERSIONES SNMP

a) **SNMP VERSIÓN 1 (SNMPV1):** Es la versión estándar del protocolo SNMP, la seguridad de SNMPv1 está basada en comunidades, que no son más que contraseñas: cadenas en texto plano que permiten a cualquier aplicación basada en SNMP tener

acceso a la información de esos dispositivos con tan sólo poseer la cadena. (Ford & Lew, 1998, pág. 562)

b) **SNMP VERSIÓN 2 (SNMPV2):** Tiene características en común con la versión 1 pero ofrece mejoras, como, por ejemplo, operaciones adicionales. Utiliza el mismo modelo administrativo que la primera versión del protocolo SNMP, y como tal no incluye mecanismos de seguridad. Las únicas mejoras introducidas en la nueva versión consisten en una mayor flexibilidad de los mecanismos de control de acceso, ya que se permite la definición de políticas de acceso consistentes en asociar un nombre de comunidad con un perfil de comunidad formado por una vista MIB y unos derechos de acceso a dicha vista (read-only o read-write). (Ford & Lew, 1998, pág. 562)

c) **SNMP VERSIÓN 3 (SNMPV3):** Éste agrega soporte para una autenticación fuerte y comunicación privada entre entidades administradas. Es un protocolo de manejo de red interoperable, que proporciona seguridad de acceso a los dispositivos por medio de una combinación de autenticación y cifrado de paquetes que trafican por la red. (Ford & Lew, 1998, pág. 562)

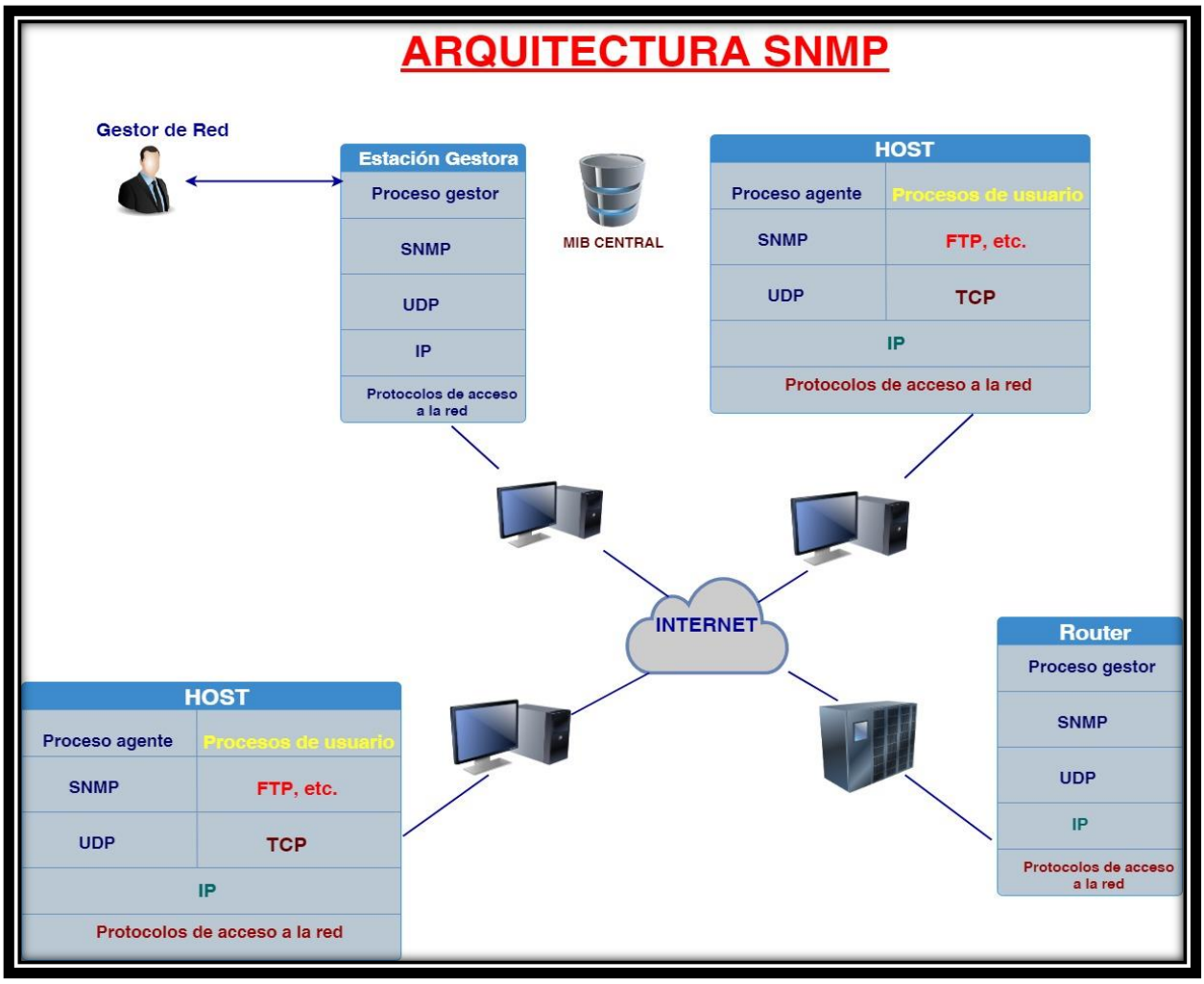


Figura N° 9. Arquitectura SNMP

Fuente: (Ford & Lew, 1998, pág. 560)

2.2.12 RED DE DATOS.

Para (Forouzan, 2002) define lo siguiente:

La palabra red de datos corresponde a una infraestructura cuyo diseño posibilita la transmisión de información a través del intercambio de datos. Cada una de estas redes ha sido diseñada específicamente para satisfacer sus objetivos, con una arquitectura determinada para facilitar el intercambio de los contenidos. (p.45)

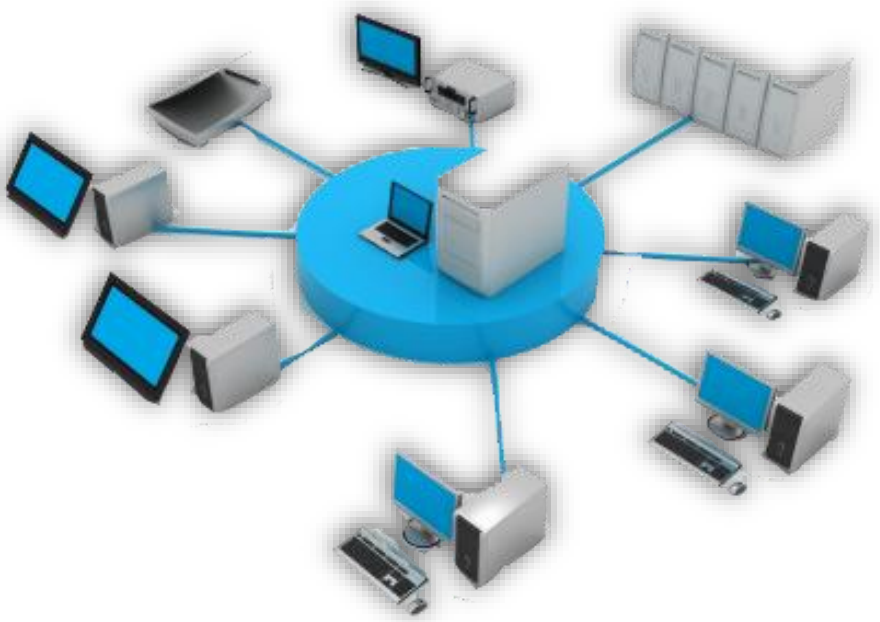


Figura N° 10. Relación Gestor - Agente

Fuente: (Forouzan, 2002, pág. 45)

Además (Forouzan, 2002) también menciona que:

> La red existe para cumplir un determinado objetivo que es la transmisión de datos donde se realiza el intercambio de datos entre dos dispositivos a través de algún medio de transmisión. Esta transmisión se considera local si los dispositivos se encuentran en un área geográfica delimitada y se considera remota si los dispositivos están separados por una distancia considerable. (p.46)

> Este intercambio de datos es la base de muchos servicios, basados en redes de computadoras y se han convertido en una parte indispensable de los negocios, la industria y el entretenimiento. Existen muchos ejemplos donde las redes de datos son usadas por ejemplo en una aplicación de venta donde se capturen los pedidos ya sean por internet o vía telefónica y éstos se conecten a una red de procesamiento de pedidos. Un ejemplo más es la transferencia de dinero sin tener que ir a un banco, un cajero automático es un ejemplo de transferencia electrónica de fondos. La mayoría de los servicios que se ofrecen actualmente están ligados de una u otra forma a una red de datos. (Dordoigne, 2015, pág. 215)

2.2.13 RED DE ÁREA LOCAL (LAN – Local Area Network)

Este tipo de red es utilizada tanto en hogares como en empresas, caracterizándose por ser una red privada con acceso único a sus dispositivos. Está formada por varios dispositivos conectados a un mismo establecimiento, como, por ejemplo: una oficina, edificio, local. Debido a que es una red más grande, permite compartir de esta manera mayor cantidad de información y uso de los recursos. Normalmente para conectarse con la red se utiliza cable, como se muestra en la figura: (Stallings, Comunicaciones y Redes de Computadores, 2004, pág. 17)

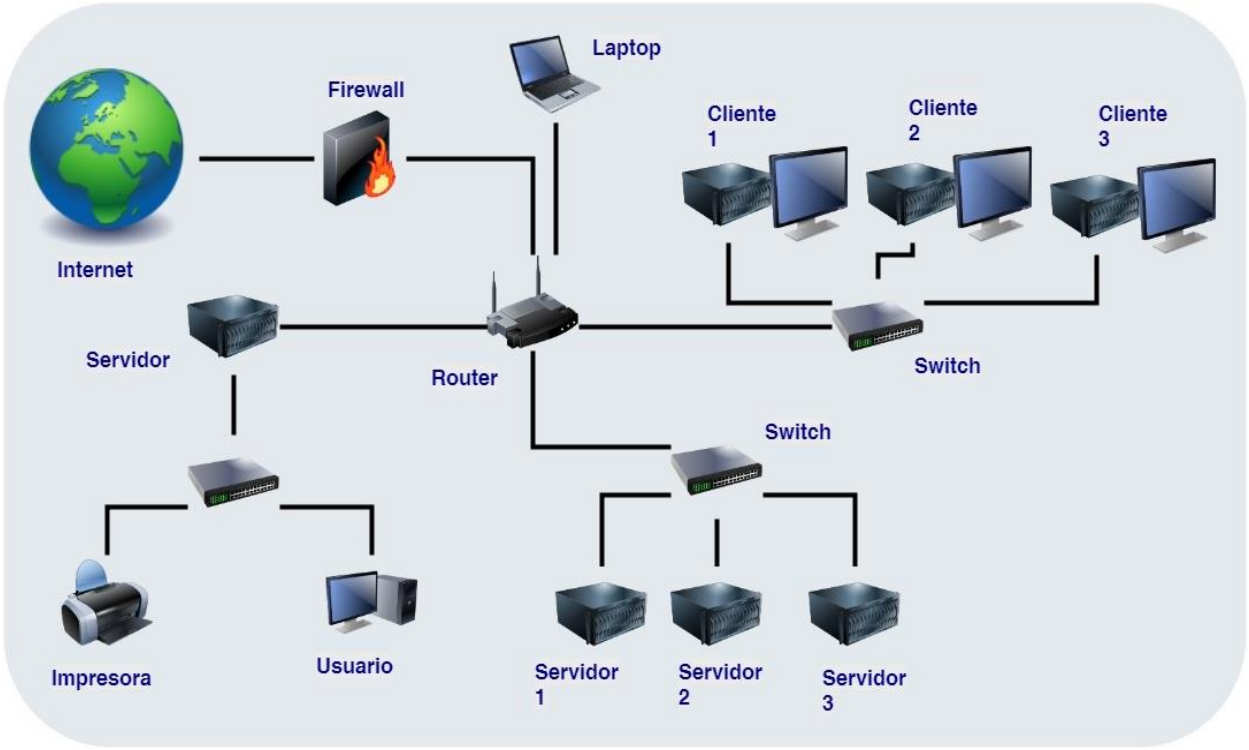


Figura N° 11. Red de Área Local (LAN)

Fuente: (Carrasco, 2014)

2.2.14 RED WLAN (WLAN - Wireless Local Area Network)

Una Red de Área Local Inalámbrica, más conocida como WLAN, es básicamente un sistema de transferencia y comunicaciones de datos el cual no requiere que las computadoras que la componen tengan que estar cableadas entre sí, ya que todo el tráfico de datos entre las mismas se realiza a través de ondas de radio. (Carrasco, 2014)

A pesar de que son menos seguras que su contrapartida cableada, ofrecen una amplia variedad de ventajas, y es por ello que su implementación crece día a día en todos los

ámbitos. Sin embargo, la característica más destacada de las redes inalámbricas es el ahorro en el tendido de los cables para la interconexión de las PC y dispositivos que componen la misma, ya que no requiere de ningún cable para su interconexión. (Carrasco, 2014)

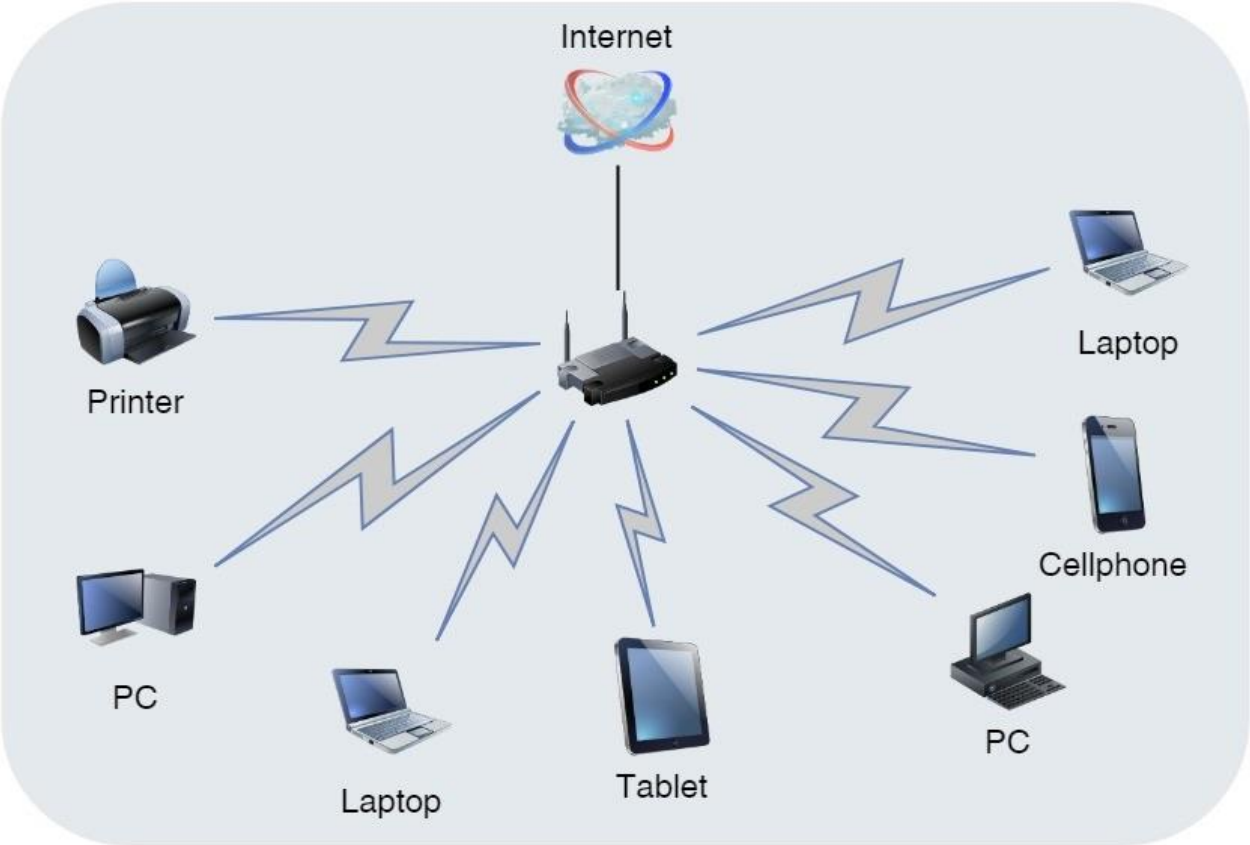


Figura N° 12. Red de Área Local Inalámbrica (WLAN)

Fuente: (Carrasco, 2014)

A. TOPOLOGÍAS DE RED

El término topología se define como la forma en que está diseñada la red ya sea de manera física o lógica. La topología de una red es la representación geométrica de la relación entre todos los enlaces y los dispositivos que los enlazan entre sí. Las topologías básicas se clasifican en malla, estrella, árbol, bus y anillo (Forouzan, 2002, pág. 9)

B. TOPOLOGÍA EN MALLA

Según (Forouzan, 2002) define la topología en malla como:

La configuración que se realiza en cada dispositivo que está conectado a uno o más de los otros dispositivos (también llamados nodos) y así, es posible llevar los datos de un

nodo al otro por diferentes caminos. Una diferencia importante con las otras topologías es que no se requiere tener un concentrador o servidor central. Entre las ventajas que se tienen con esta topología son: el sistema completo no se inhabilita si un enlace falla, la seguridad de saber que cuando un mensaje viaja a través de un enlace, solamente lo ve el receptor adecuado, también es más fácil detectar y aislar fallos. Entre las desventajas, están la cantidad de cable necesario y el número de puertos de entrada/salida. Por estas razones, la topología en malla se utiliza junto con otras topologías para formar una topología híbrida. (p.9)

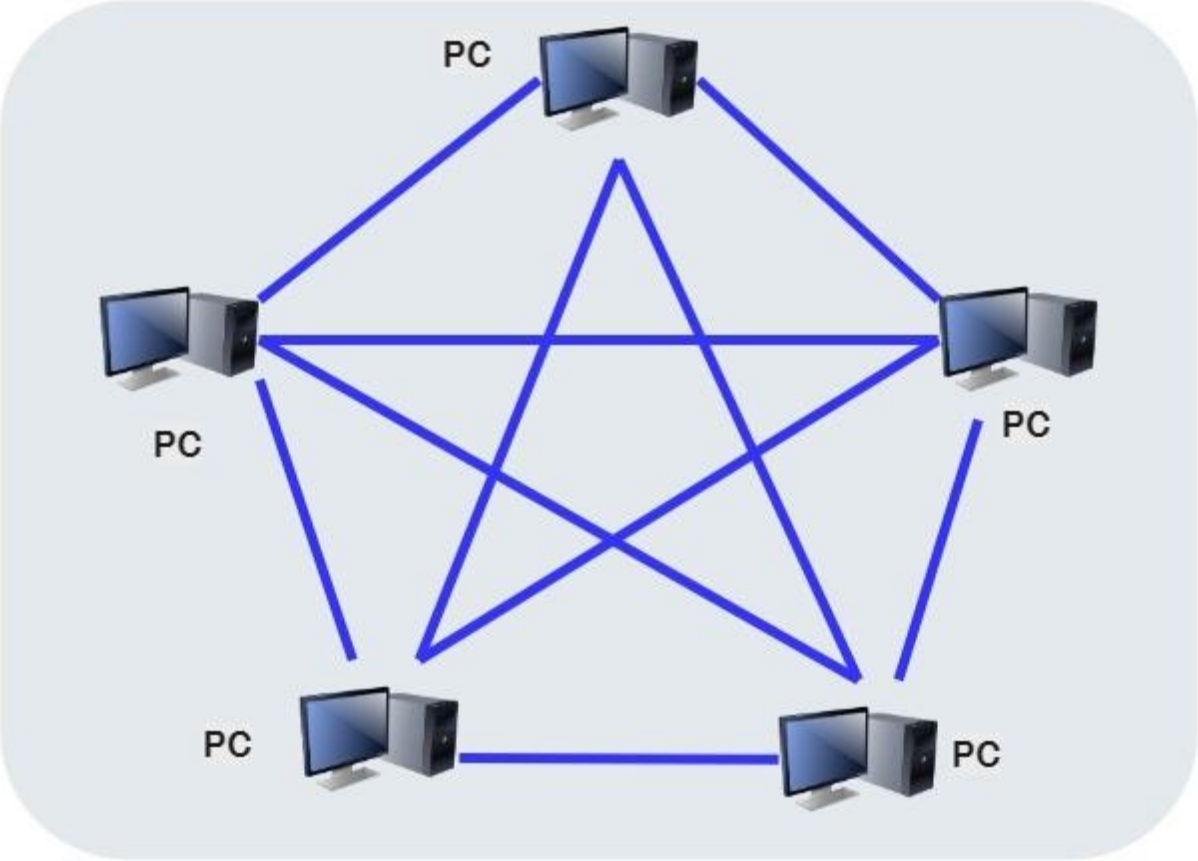


Figura N° 13. Topología en malla

Fuente: (Forouzan, 2002, pág. 10)

C. TOPOLOGÍA EN ESTRELLA

En esta topología cada dispositivo solamente tiene un enlace directo con el concentrador central. Los dispositivos no están directamente enlazados entre sí. La topología en estrella no permite el tráfico directo entre dispositivos. El controlador actúa como un intercambiador, es decir, si un dispositivo quiere enviar un dato a otro, se envían los datos al controlador para que éste retransmita ese dato al dispositivo final. Si falla un

enlace, solamente ese enlace se verá afectado. Todos los demás enlaces permanecerán activos. La desventaja es que cada nodo debe estar enlazado con el nodo central, por ello, en la estrella se requiere más cable que en otras topologías de red, excepto en la de malla. (Forouzan, 2002, p. 10)

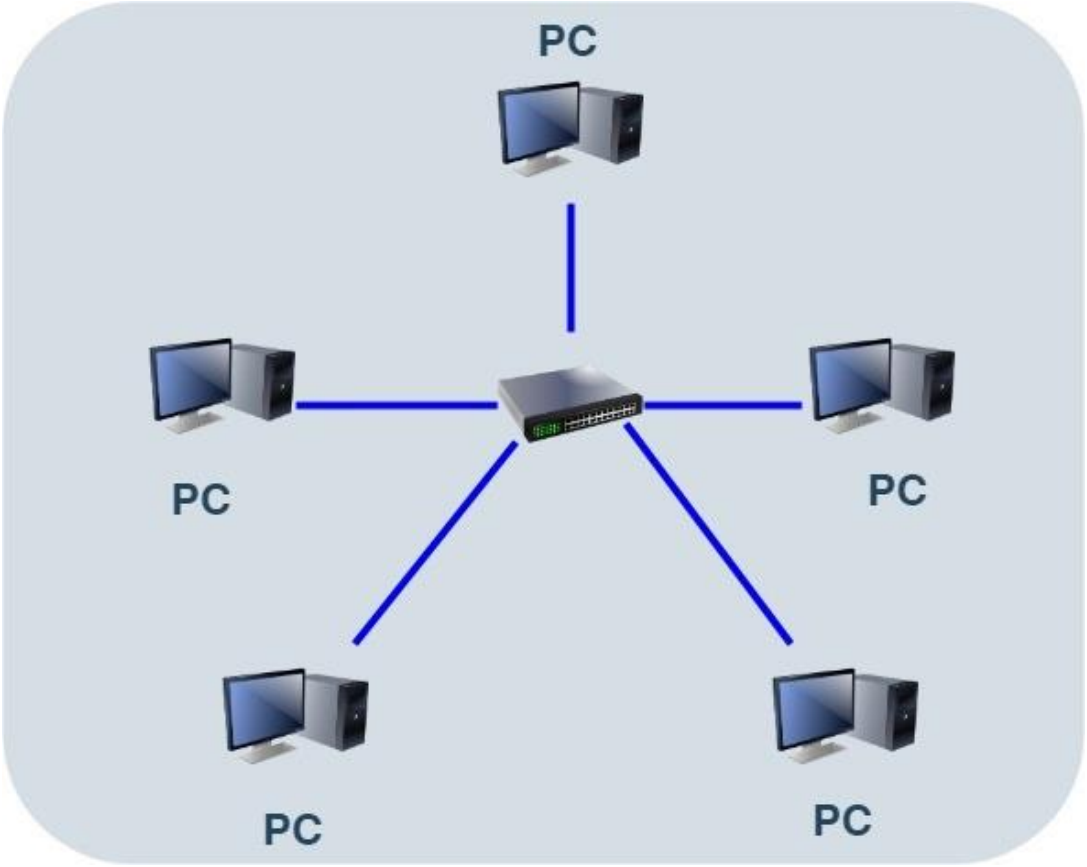


Figura N° 14.Topología en estrella

Fuente: (Forouzan, 2002, pág. 10)

D. TOPOLOGÍA EN ÁRBOL

Por otra parte, (Forouzan, 2002) respecto a la topología de árbol manifiesta:

La topología en árbol es una variante de la de estrella. Los nodos del árbol están conectados a un concentrador central que controla el tráfico de la red. Sin embargo, no todos los dispositivos se conectan directamente al concentrador central. La mayoría de los dispositivos se conectan a un concentrador secundario que, a su vez, se conecta al concentrador central que generalmente es un hub3 o switch. Las ventajas y desventajas son, casi las mismas que las de una estrella. Sin embargo, el incluir concentrador secundario puede incrementar la distancia a la que puede viajar la señal entre dos dispositivos y permite a la red aislar y priorizar las comunicaciones de distintas computadoras. (p.11)

Figura N° 15. Topología en árbol

Fuente: (Forouzan, 2002, pág. 11)

E. TOPOLOGÍA EN BUS

Una topología en bus es multipunto, es decir, un cable largo actúa como una red troncal que conecta a todos los dispositivos de red. Existen muchas limitantes para esta configuración. Cuando las señales viajan a través de la red troncal, parte de la energía se transforma en calor, lo que se traduce en debilitamiento de la señal a medida que viaja por el cable. Por esta razón, hay un límite en el número de conexiones que un bus puede soportar y en la distancia entre estas conexiones. Como ventaja de esta topología está la sencillez de instalación, menor uso de cable que en otras topologías. Entre sus desventajas está la dificultad para agregar nuevos dispositivos y si el cable de bus llega a fallar, interrumpe todas las comunicaciones. (Forouzan, 2002, pág. 11)

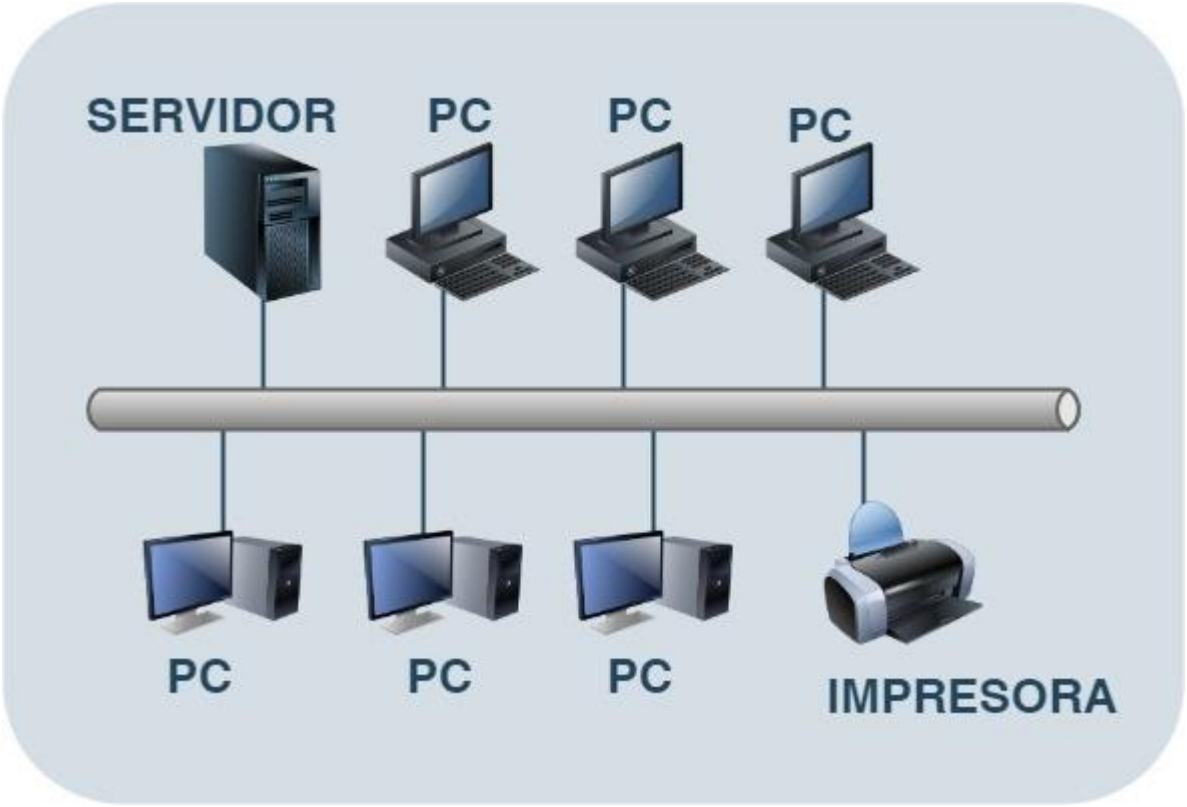


Figura N° 16. Topología en bus

Fuente: (Forouzan, 2002, pág. 12)

F. TOPOLOGÍA EN ANILLO

Cada dispositivo tiene una línea de conexión directa solamente con los dos dispositivos que están a sus lados. La señal pasa a lo largo del anillo en una dirección hasta que alcanza su destino. Un anillo es relativamente fácil de instalar y reconfigurar. Cada dispositivo está enlazado solamente a sus vecinos inmediatos. Las únicas restricciones están relacionadas con aspectos del medio físico y el tráfico. Sin embargo, el tráfico unidireccional puede ser una desventaja, una rotura del anillo puede inhabilitar toda la red. Fuente: (Forouzan, 2002, pág. 12)

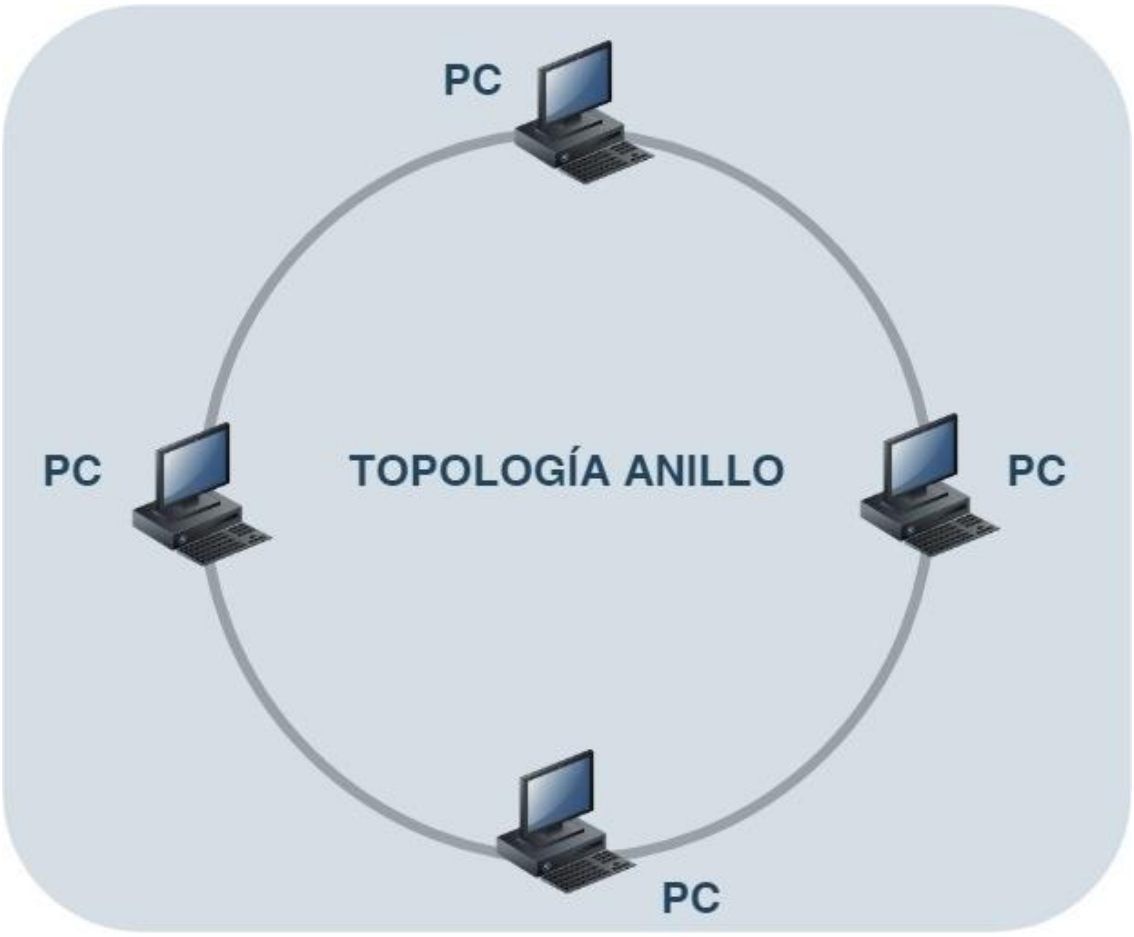


Figura N° 17. Topología en anillo

Fuente: (Forouzan, 2002, pág. 13)

2.2.15 MODELO OSI

Para (Santos, 2014) respecto al Modelo OSI define lo siguiente:

> OSI es un modelo basado en niveles para el diseño de sistemas de red. Este modelo además permite la interconexión de sistemas abiertos, o lo que es lo mismo, permite que dos sistemas diferentes se puedan comunicar independientemente de su arquitectura. Es importante resaltar que OSI es un modelo, no un protocolo. Además, el modelo OSI no especifica los servicios ni los protocolos que forman parte de cada nivel. Los niveles definidos en el modelo OSI son siete: físico, enlace, red, transporte, sesión, presentación, aplicación. El modelo OSI se clasifica en 7 niveles que son: Aplicación, Presentación, Sesión, Transporte, Red, Enlace y Físico (p.22)

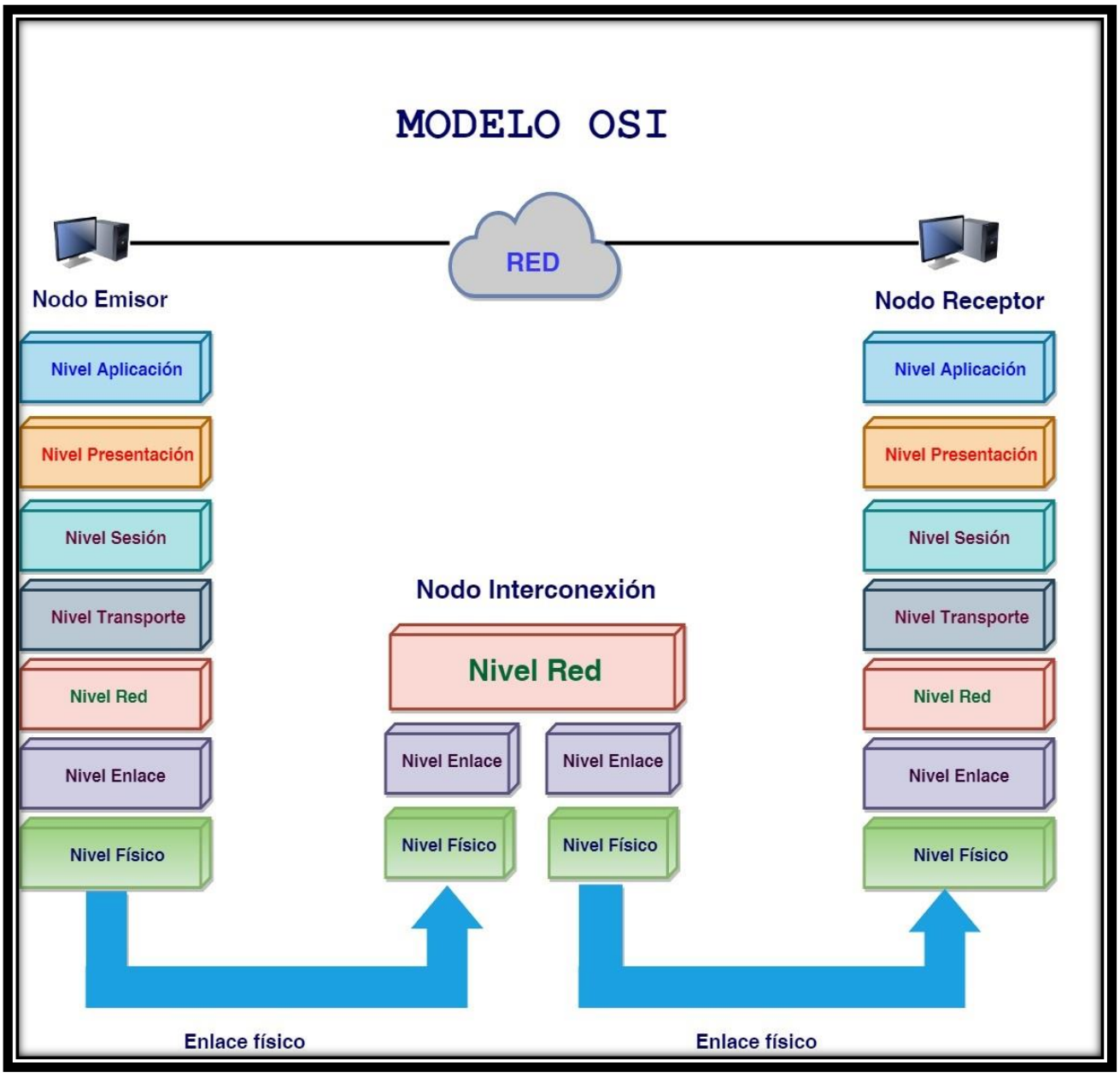


Figura N° 18. Modelo OSI

Fuente: (Santos, 2014, p. 23)

A. Nivel Aplicación

El nivel de aplicación es el nivel de la comunicación en el que un usuario interactúa con la red. Éste es el nivel más alto del modelo y por tanto es el nivel donde se generan los datos que luego viajarán por las redes. En este nivel se define lo que se conoce como servicios de red. (Santos, 2014, pág. 23)

B. Nivel Presentación

El nivel de presentación se encarga básicamente de aislar las capas inferiores del formato de los datos del nivel de aplicación. Este nivel implementa características que tienen que ver con la sintaxis y la semántica de la información que se intercambia entre un emisor y un receptor. (Santos, 2014, pág. 23)

C. Nivel Sesión

El nivel de sesión organiza y sincroniza el intercambio de datos entre procesos de aplicación. El nivel de sesión asume que los dos extremos de la comunicación tienen la misma categoría, algo que no es muy frecuente en los servicios de red, los cuales son en su gran mayoría de tipo cliente-servidor. (Santos, 2014, pág. 23)

D. Nivel de transporte

El nivel de transporte es responsable de la entrega origen a destino de todo el mensaje. En el nivel de red se supervisa la entrega de paquetes individuales sin reconocer ninguna relación entre estos paquetes. El nivel de transporte asegura que todo el mensaje llegue intacto y en orden, supervisando tanto el control de errores como el control de flujo a nivel origen a destino. (Santos, 2014, pág. 24)

E. Nivel de Red

El nivel de red se encarga de todas las funciones necesarias para encaminar la información a través de varias redes. Sus funciones son necesarias cuando el emisor y el receptor están en redes diferentes. Este nivel recibe un paquete de datos del nivel superior y se encarga de que llegue a su destino, siendo necesario llevar a cabo mecanismos de enrutamiento. (Santos, 2014, pág. 25)

F. Nivel de Enlace

La transmisión de los datos se lleva a cabo en el nivel físico, aunque dicho nivel no proporciona ningún mecanismo para asegurar que los datos (bits) que se envían llegarán libres de errores al receptor. El objetivo del nivel físico es llevar a cabo la transmisión de los datos con la mayor fiabilidad posible, pero sin llevar a cabo ningún control de errores, función de la que se encarga el nivel de enlace. La principal función del nivel de enlace es, por tanto, proporcionar fiabilidad a la transmisión entre dos dispositivos unidos mediante un enlace. (Santos, 2014, pág. 26)

G. Nivel de Físico

El nivel físico se encarga de la transmisión de la información a través de un medio físico, es decir, el nivel físico debe ser capaz de enviar datos (bits) a través de un canal de comunicaciones (cable de cobre, fibra óptica, aire) procurando que esos datos no sufran alteraciones y puedan ser correctamente interpretados en el receptor. (Santos, 2014, pág. 27)

2.2.16 MODELO TCP/IP

Para (Tanenbaum & Wetherall, 2012) manifiesta que la familia de protocolos TCP/IP se desarrolló antes que el modelo OSI. Por lo tanto "Los niveles de Protocolo de Control de Transmisión/Protocolo de Red (TCP/IP) no coinciden exactamente con los del modelo OSI. La familia de protocolos TCP/IP. Está compuesta por cuatro niveles: acceso a red, internet, transporte y aplicación" (p.39).

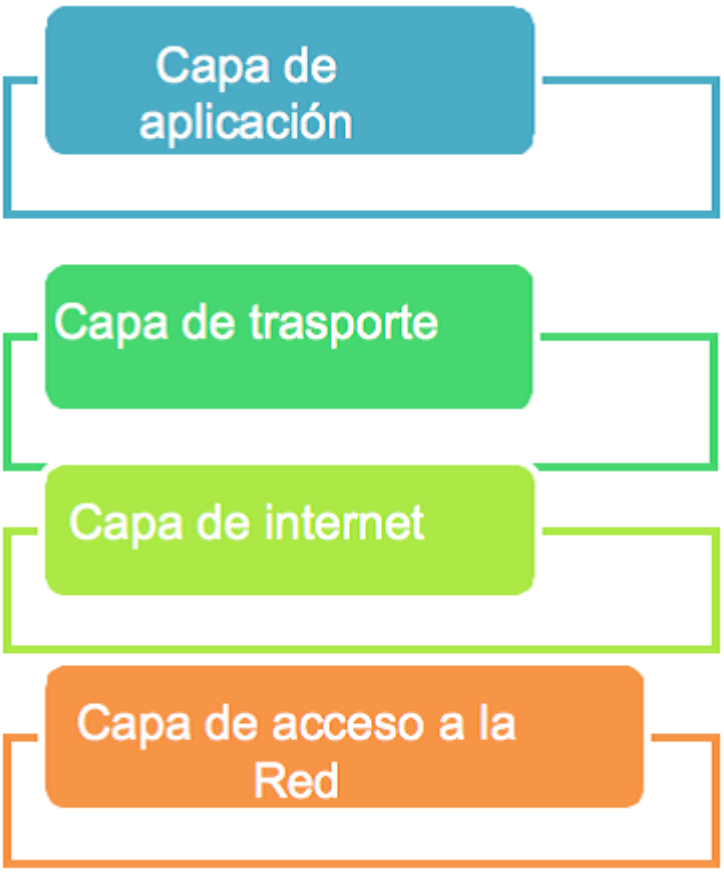


Figura N° 19. Modelo TCP/IP

Fuente: (Tanenbaum & Wetherall, 2012, pág.40)

A. Capa de Enlace

Para Tanenbaum & Wetherall (2012) considera.

La capa más baja en este modelo es la capa de enlace; ésta describe qué enlaces como las líneas seriales y Ethernet clásica se deben llevar a cabo para cumplir con las necesidades de esta capa de internet sin conexión. En realidad, no es una capa en el sentido común del término, sino una interfaz entre los hosts y los enlaces de transmisión. El primer material sobre el modelo TCP/IP tiene poco que decir sobre ello. (p.39)

B. Capa de Internet

Por medio de esta capa se permite que los hosts inyecten paquetes en cualquier red y que viajen de manera independiente hacia el destino. Incluso pueden llegar en un orden totalmente diferente al orden en que se enviaron, en cuyo caso es responsabilidad de las capas más altas volver a ordenarlos, si se desea una entrega en orden. Se tiene que tener en cuenta que se utiliza "interred" en un sentido genérico, aunque esta capa esté presente en la Internet. (Tanenbaum & Wetherall, 2012, p.39)

C. Capa de Transporte

Esta capa está diseñada para permitir que las entidades pares, en los nodos de origen y de destino, lleven a cabo una conversación, al igual que en la capa de transporte de OSI. Aquí se definieron dos protocolos de transporte de extremo a extremo. (Tanenbaum & Wetherall, 2012, p.40)

D. Capa de Aplicación

Las aplicaciones simplemente incluyen cualquier función de sesión y de presentación que requieran. La experiencia con el modelo OSI ha demostrado que esta visión fue correcta: estas capas se utilizan muy poco en la mayoría de las aplicaciones. Encima de la capa de transporte se encuentra la capa de aplicación. Ésta contiene todos los protocolos de alto nivel. (Tanenbaum & Wetherall, 2012, p.41)

2.2.17 PROTOCOLO TCP/IP

El principal protocolo que utiliza la arquitectura TCP/IP en el nivel de red es el protocolo IP. (Santos, 2014) afirma:

IP (Internet Protocol) es un protocolo del nivel de red no orientado a conexión, basado en datagramas y no fiable. IP es un protocolo no orientado a conexión, es decir, no se

establece un camino previamente, con lo cual cada datagrama viaja de forma independiente, pudiendo llegar al destino fuera de secuencia o duplicado. No se crean circuitos virtuales. Y, además, es un protocolo no fiable, es decir, no ofrece comprobaciones ni seguimientos. IP intenta que los datos lleguen a su destino lo mejor que puede, pero sin ofrecer garantías. (p.123)

2.2.18 DATAGRAMA IPV4

La transmisión de los datos en el nivel de red utilizando el protocolo IP se realiza en unidades de información llamadas datagramas.

Esto significa que un datagrama consta de dos partes, una cabecera y los datos. La longitud de un datagrama es variable, pudiendo alcanzar un tamaño máximo de 65.535 bytes. A continuación, se muestra la estructura de un datagrama IP. Los números mostrados en la parte inferior de la figura son los tamaños de los campos de la cabecera expresados en bits. (Santos, 2014, pág. 124)

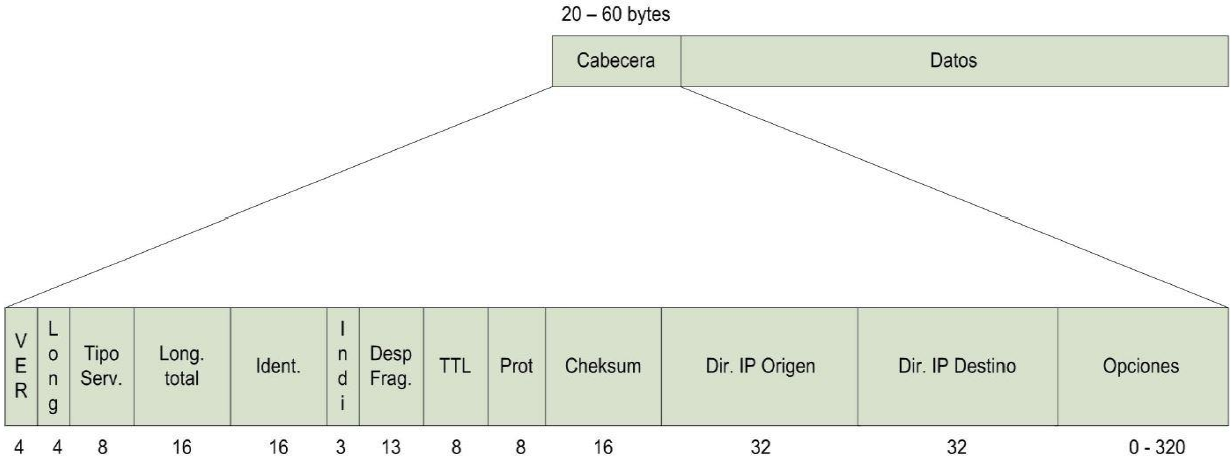


Figura N° 20. Diagrama IPv4

Fuente: (Santos, 2014, pág. 124)

2.2.19 DIRECCIONAMIENTO IPV4

Una de las principales funciones del nivel de red es el llamado direccionamiento lógico. Este direccionamiento lógico se utiliza para definir un identificador para cada dispositivo de la red, pero teniendo en cuenta la jerarquía necesaria en la arquitectura de

las redes. Por tanto, en el protocolo IP, cada dispositivo debe tener asignada una dirección lógica conocida también como dirección de red o dirección IP. (Santos, 2014, pág. 127).

2.2.20 CLASIFICACIÓN DEL PROTOCOLO IP

La clasificación del protocolo IP se definió para optimizar el uso del enrutamiento de los datagramas, ya que no usar clases hubiera supuesto que los routers deberían almacenar una gran cantidad de información en sus tablas de enrutamiento, lo cual hubiera sido negativo para el funcionamiento de las redes. Se establecieron varios tipos de redes, es decir, de clases, para cubrir las necesidades de los diferentes tipos de organizaciones, ya que cada clase permite un máximo de direcciones IP en cada red que pertenezca a dicha clase. Las clases que se definieron en el protocolo IP son Clase A, B, C, D y E. (Santos, 2014, pág. 128)

a) **Clase A.** "En esta clase, el bit más significativo de la dirección IP vale siempre 0. Se utilizan 7 bits para identificar la red y el resto de bits, es decir, 24, se utilizan para identificar un host dentro de la red" (Santos, 2014, p. 128).
b) **Clase B**. "En este caso, el valor de los dos primeros bits de la dirección es siempre 10. Se utilizan 14 bits para identificar la red y 16 bits para identificar un host dentro de la red" (Santos, 2014, p. 128).
c) **Clase C**. "En este caso, el valor que se utiliza en los tres primeros bits para asignar la clase C es el 110. Se utilizan 21 bits para identificar la red y 8 bits para identificar un host dentro de la red" (Santos, 2014, p. 128).
d) **Clase D**. "Esta clase se identifica por contener en los cuatro primeros bits el valor 1110 y se utiliza para establecer direcciones de multienvío" (Santos, 2014, p. 128).
e) **Clase E**. "Identificada por sus primeros 4 bits tiene el valor 1111. Estas direcciones están reservadas inicialmente para usos futuros, aunque en la práctica nunca se ha llegado a definir ningún uso para estas direcciones" (Santos, 2014, p. 128).

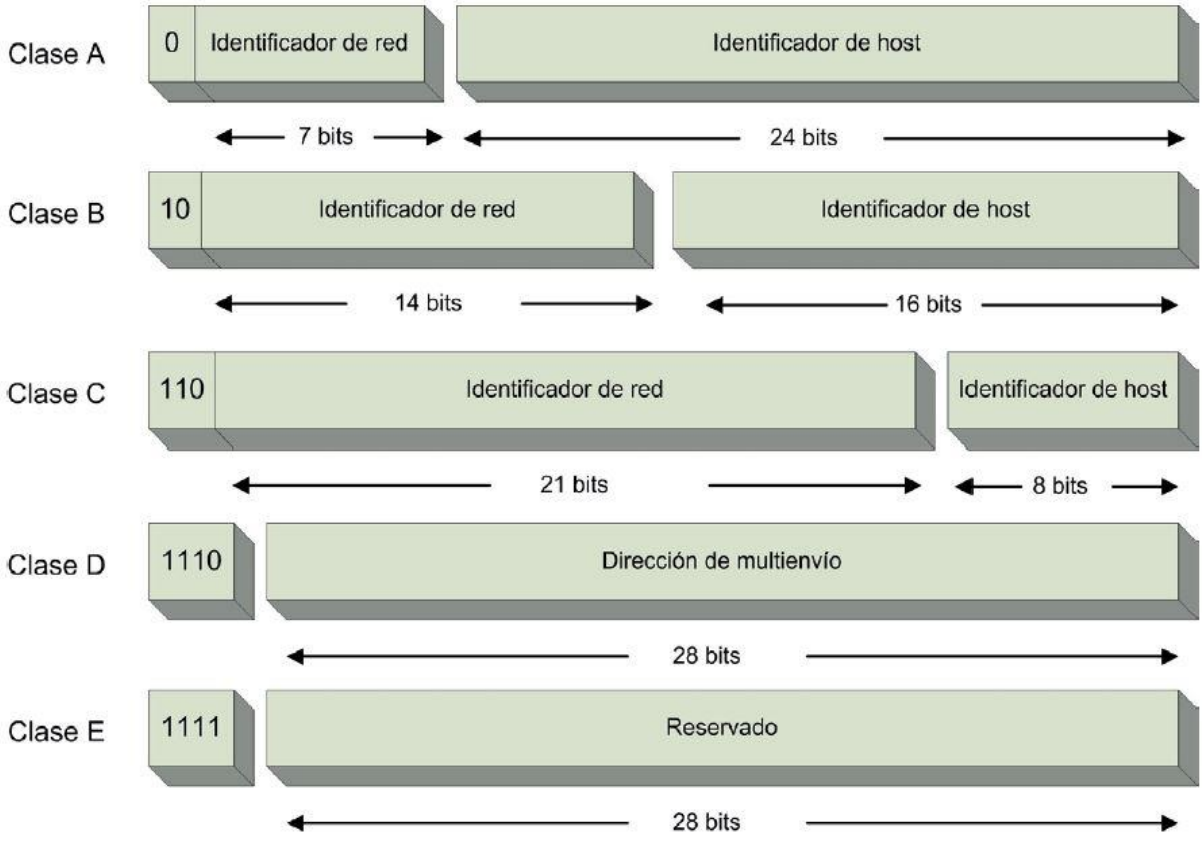


Figura N° 21. Clases del Protocolo IP

Fuente: (Santos, 2014, pág. 128)

2.2.21 SEGURIDAD INFORMÁTICA

La información es un activo que, como otros importantes activos de negocios, tiene valor para una organización y en consecuencia necesita ser debidamente protegido. (Baca, 2016) afirma:

> La seguridad informática protege la información de un amplio rango de amenazas con el objetivo de asegurar la continuidad de negocios, minimizar el daño comercial y maximizar el reembolso de las inversiones y oportunidades comerciales. La información puede existir en muchas formas. Puede ser impresa o escrita en papel, almacenada electrónicamente, trasmitida por correo o usando medios electrónicos, impreso en películas o hablado en conversación. No importa la forma que tome, el medio por el que se comparta o en el que se almacene, siempre debe ser correctamente protegida. (p.19)

2.2.22 PRINCIPIOS DE LA SEGURIDAD INFORMÁTICA

Según (Álvarez & Pérez, 2004) define los principios de la seguridad informática como: "Una referencia que puede ayudar a alcanzar los objetivos de seguridad dentro de una organización, pero nunca debe constituir un fin en sí mismo"(p.95).

A continuación se detalla cada principio según (Álvarez & Pérez, 2004):

A. CONFIDENCIALIDAD: La confidencialidad tiene las siguientes características:

- Propiedad de la información que impide que ésta esté disponible o sea revelada a individuos, entidades o procesos no autorizados. Según esta norma la confidencialidad es un servicio de seguridad.
- Prevención de la revelación no autorizada de información.
- Característica de los datos e informaciones que son revelados sólo a los usuarios, entidades o procesos en el tiempo y forma autorizados.

B. INTEGRIDAD: El objetivo de la integridad es, entonces, prevenir modificaciones no autorizadas de la información.

La integridad hace referencia a:

a. La integridad de los datos (el volumen de la información)
b. La integridad del origen (la fuente de los datos, llamada autenticación)

C. DISPONIBILIDAD: La disponibilidad hace referencia a que la información del sistema debe permanecer accesible a elementos autorizados. El objetivo de la disponibilidad es, entonces, prevenir interrupciones no autorizadas/controladas de los recursos informáticos. En términos de seguridad informática "un sistema está disponible cuando su diseño e implementación permite deliberadamente negar el acceso a datos o servicios determinados.

2.2.23 AUDITORIA DE SISTEMAS

Para (Tamayo, 2003) define a la auditoria de sistemas como:

> La Auditoría de sistemas es parte de la auditoría interna que se encarga de llevar a cabo la evaluación de normas, controles, técnicas y procedimientos que se tienen establecidos en una empresa para lograr confiabilidad, oportunidad, seguridad y confidencialidad de la información que se procesa a través de computadores; es decir, en estas evaluaciones

se está involucrando tanto los elementos técnicos como humanos que intervienen en el proceso de la información. (p.9)

Por otra parte, el concepto de José A. Echenique, que al respecto expone lo siguiente:

> La auditoría de sistemas es la revisión y evaluación de los controles, sistemas, procedimientos de informática; de los equipos de cómputo, su utilización, eficiencia y seguridad, de la organización que participa en el procesamiento de la información, a fin de que por medio del señalamiento de cursos alternativos se logre una utilización más eficiente y segura de la información que servirá para una adecuada toma de decisiones. (Echenique, 2001, pág. 13)

Figura N° 22. Objetivos de la Auditoria de Sistemas

Fuente: (Tamayo, 2003, pág. 11)

2.2.24 ANÁLISIS Y GESTIÓN DE RIESGOS

Según (Gómez, 2014) define lo siguiente: “El análisis y gestión de riesgos busca definir un plan para la implantación de ciertas salvaguardas o contramedidas, que permitan disminuir la probabilidad de que se materialice una amenaza, o bien reducir la vulnerabilidad del sistema o el posible impacto en la organización” (p.59)

Para (Vargas, 2018) considera lo siguiente:

> El análisis y la gestión de riesgos consiste en un proceso sistemático para estimar la probabilidad de ocurrencia y la magnitud del impacto de cada riesgo identificado. Para llevar a cabo este proceso es necesario partir de una lista de riesgos identificados que conviene que estén categorizados de modo que resulte más sencillo su tratamiento.

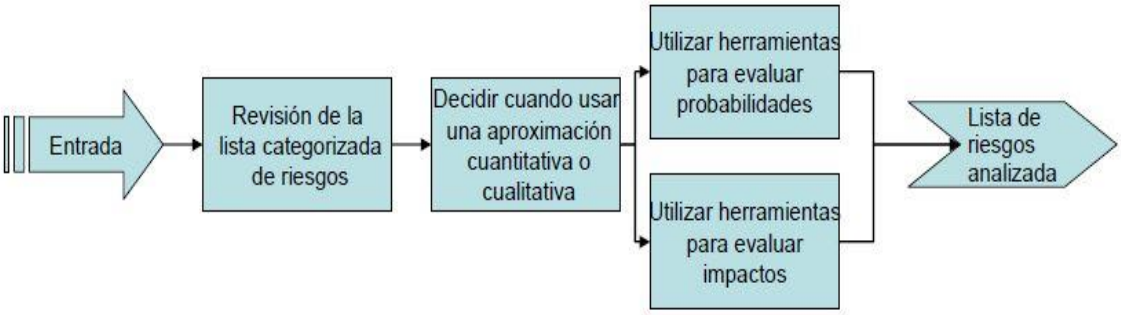


Figura N° 23. Procesos de análisis de riesgos
Fuente: (Vargas, 2018)

2.2.25 RIESGOS

Para (Izquierdo, 2005) considera que: "El riesgo es un incidente o situación, que ocurre en un sitio concreto durante un intervalo de tiempo determinado, con consecuencias positivas o negativas que podrían afectar el cumplimiento de los objetivos" (p.47).

El riesgo es la probabilidad de que una amenaza se materialice sobre una vulnerabilidad del recurso informático (Gómez, 2014) define lo siguiente:

> El nivel de riesgo depende, por lo tanto, del análisis previo de vulnerabilidades del sistema, de las amenazas y del posible impacto que estas puedan tener en el funcionamiento de la organización, causando determinado impacto en la organización. (p.64)

2.2.26 MEDIDAS DE SEGURIDAD

Para (Gómez, 2014) manifiesta que las medidas de seguridad son: "Cualquier medio empleado para eliminar o reducir un riesgo. Su objetivo es reducir las vulnerabilidades de los activos, la probabilidad de ocurrencia de las amenazas y/o el nivel de impacto en la organización y estas se dividen en medidas de seguridad activa y pasiva" (p.65).

A continuación (Gómez, 2014, pág. 71) define las medidas de seguridad activa y pasiva.

A. Medidas de seguridad activa: Es cualquier medida utilizada para anular o reducir el riesgo de una amenaza. Las medidas activas podrían, a su vez, clasificarse en medidas de prevención (de aplicación antes del incidente) y medidas de detección (de aplicación durante el incidente). Se consideran como medidas de detección el Sistema de Detección de Intrusiones

(IDS) o las herramientas y procedimientos para el análisis de los "logs" (registros de actividad de los equipos).

B. Medidas de seguridad pasiva: Es cualquier medida empleada para reducir el impacto cuando se produzca un incidente de seguridad. Por ello, a las medidas pasivas también se las conoce como medidas de corrección (se aplican después del incidente). Por otra parte, se considera como medida correctiva las copias de seguridad, el plan de respuesta a incidentes y de continuidad del negocio.

2.2.27 POLÍTICAS DE SEGURIDAD

"Las políticas de seguridad son una declaración de intenciones de alto nivel que cubre la seguridad de los sistemas informáticos y que proporciona las bases para definir y delimitar responsabilidades para las diversas actuaciones técnicas y organizativas que se requieran." (RFC's 1244 & 2196, 2002, pág. 194)

A. CARÁCTERÍSTICAS DE LAS POLÍTICAS DE SEGURIDAD

Las Políticas de Seguridad de una organización deberían cumplir con las siguientes características y requisitos básicos (Gómez, 2014) considera las siguientes políticas de seguridad:

- Las políticas de seguridad deberían poder ser implementadas a través de determinados procedimientos administrativos y la publicación de unas guías de uso aceptable del sistema por parte del personal, así como mediante la instalación, configuración y mantenimiento de determinados dispositivos y herramientas de hardware que implanten servicios de seguridad.
- Deben definir claramente las responsabilidades exigidas al personal con acceso al sistema: técnicos, analistas y programadores, usuarios finales, directivos, personal externo a la organización.
- Debe cumplir con las exigencias del entorno legal.
- Se tienen que revisar de forma periódica para poder adaptarlas a las nuevas exigencias de la organización y del entorno tecnológico y legal.
- Aplicación del principio de "Defensa en profundidad": definición e implantación de varios niveles o capas de seguridad.

- Asignación de los mínimos privilegios: los servicios, las aplicaciones y usuarios del sistema deberían tener asignados los mínimos privilegios necesarios para que puedan realizar sus tareas. La política por defecto debe ser aquella en la que todo lo que no se encuentre expresamente permitido en el sistema estará prohibido. Las aplicaciones y servicios que no sean estrictamente necesarios deberían ser eliminados de los sistemas informáticos.
- Configuración robusta ante fallos: los sistemas deberían ser diseñados e implementados para que, en caso de fallo, se situaran en un estado seguro y cerrado, en lugar de en uno abierto y expuesto a accesos no autorizados.
- Las Políticas de Seguridad no deben limitarse a cumplir con los requisitos impuestos por el entorno legal o las exigencias de terceros, sino que deberían estar adaptadas a las necesidades reales de cada organización. (p.73-74)

2.2.28 INFRAESTRUCTURA DE TI

A. DEFINICIÓN DE LA ESTRUCTURA DE TI

Kenneth & Jane (2012) definen lo siguiente: "La infraestructura de TI consiste en un conjunto de dispositivos físicos y aplicaciones de software requeridas para operar toda la empresa. Sin embargo, esta infraestructura también es un conjunto de servicios a nivel empresarial presupuestado por la gerencia, que abarca las capacidades tanto humanas como técnicas" (p.165).

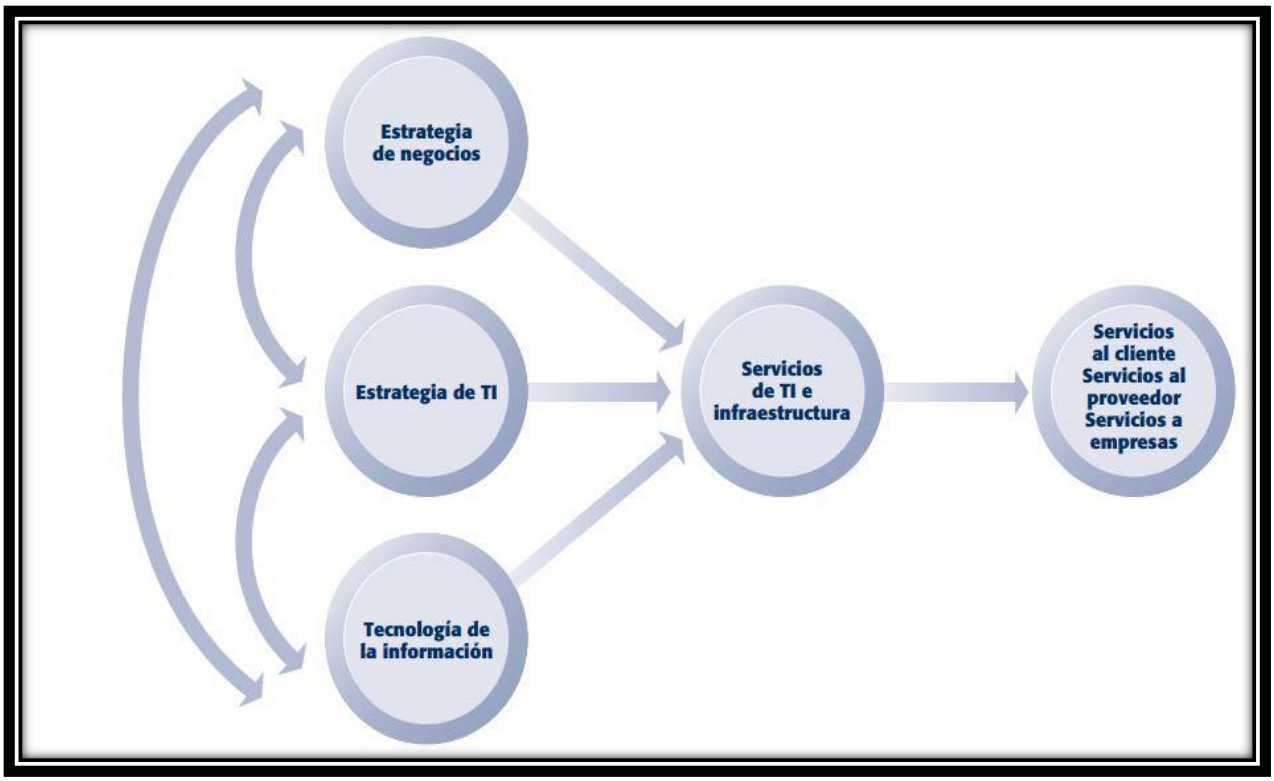


Figura N° 24. Conexión entre la empresa, la infraestructura de TI y las capacidades de negocios

Fuente: (Kenneth & Jane, 2012)

B. COMPONENTES DE LA INFRAESTRUCTURA

Según (Kenneth & Jane, 2012) concluyen que: "En la actualidad, la infraestructura de TI está compuesta de siete componentes principales. Estos componentes constituyen inversiones que se deben coordinar entre sí para proveer a la empresa una infraestructura coherente" (p.175).

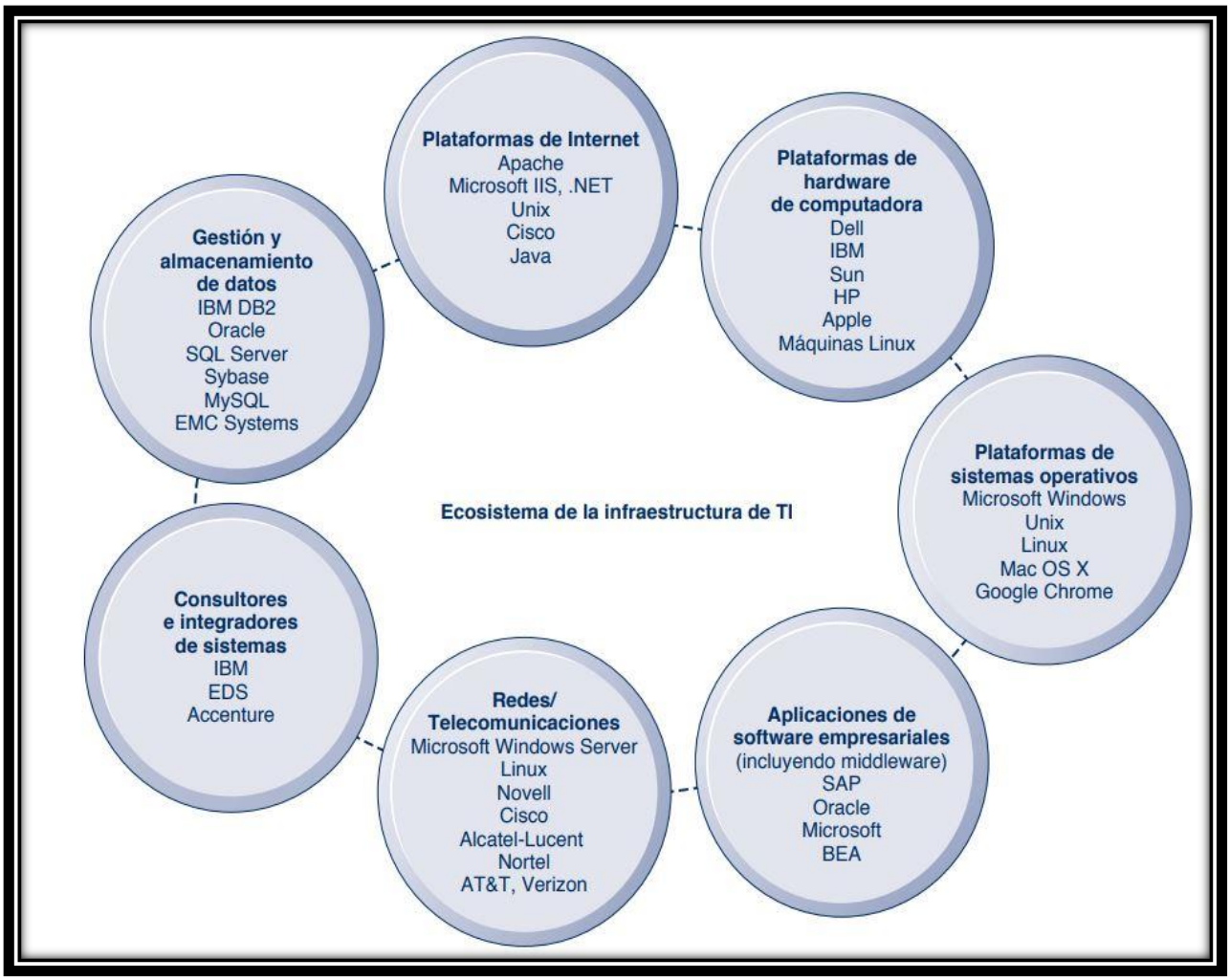


Figura N° 25. Ecosistema de la Infraestructura de TI

Fuente: (Kenneth & Jane, 2012, p. 176)

Para (Kenneth & Jane, 2012) considera lo siguiente: "Se tiene siete componentes principales que se deben coordinar para proveer a la empresa una infraestructura de TI efectiva. Aquí se muestra una lista de las principales y de los proveedores para cada componente" (p.175).

C. PLATAFORMAS DE HARDWARE DE COMPUTADORA

Hoy en día las máquinas cliente usan microprocesadores Intel o AMD. El mercado de los servidores utiliza en su mayoría procesadores Intel o AMD en forma de servidores blade en estantes, pero también incluye microprocesadores Sun SPARC y chips IBM POWER diseñados de manera especial para uso en servidores. El mercado para el hardware de computadora se enfoca cada vez más en las principales empresas como IBM, HP, Dell y Sun Microsystems (adquirida por Oracle), y en tres productores de chips: Intel, AMD e IBM. La industria se decidió en forma colectiva por Intel como el

procesador estándar, aunque hay importantes excepciones en el mercado de servidores para las máquinas Unix y Linux, que podrían usar procesadores Sun o IBM Unix (Kenneth & Jane, 2012, pág. 176).

D. PLATAFORMAS DE SISTEMAS OPERATIVOS

Los Sistemas Operativos de Microsoft Windows Server son capaces de proveer un sistema operativo y servicios de red a nivel empresarial, y llama la atención de las organizaciones que buscan infraestructuras de TI basadas en Windows.

Unix y Linux son escalables, confiables y mucho menos costosos que los sistemas operativos de mainframe. El sistema Chrome OS de Google provee un sistema operativo ligero para la computación en la nube mediante el uso de netbooks. Los programas no se almacenan en la PC del usuario, sino que se utilizan a través de Internet y se accede a éstos por medio del navegador Web Chrome. (Kenneth & Jane, 2012, pág. 176)

E. APLICACIONES DE SOFTWARE EMPRESARIALES

En la actualidad los proveedores más importantes de software de aplicaciones empresariales son SAP y Oracle. En esta categoría también se incluye el software middleware que proveen los distribuidores tales como BEA, para obtener una integración a nivel empresarial mediante la vinculación de los sistemas de aplicaciones existentes de la empresa. Por otra parte, Microsoft intenta entrar a los extremos inferiores de este mercado al enfocarse en las empresas pequeñas y de tamaño mediano que aún no han implementado aplicaciones empresariales. (Kenneth & Jane, 2012, pág. 177)

F. APLICACIONES DE SOFTWARE EMPRESARIALES

El software de gestión de bases de datos empresariales es responsable de organizar y administrar la información de la empresa, de modo que sea posible acceder a ella y utilizarla en forma eficiente. Los principales proveedores de software de bases de datos son IBM (DB2), Oracle, Microsoft (SQL Server) y Sybase (Adaptive Server Enterprise), quienes proveen más del 90 por ciento del mercado de software de bases de datos en Estados Unidos. MySQL es un producto de bases de datos relacionales de código fuente abierto de Linux, que ahora pertenece a Oracle Corporation. (Kenneth & Jane, 2012, pág. 177)

G. PLATAFORMAS DE REDES/TELECOMUNICACIONES

Respecto a Microsoft, Windows Server se utiliza de manera predominante como sistema operativo de red de área local, seguido de Linux y Unix. La mayor parte de las redes de área amplia empresariales extensas utilizan alguna variante de Unix. La mayoría de las redes de área local, así como las redes empresariales de área amplia, utilizan la suite de protocolos TCP/IP como estándar. Por lo general, las compañías de servicios de telecomunicaciones/telefónicos que ofrecen conectividad de voz y datos, redes de área amplia, servicios inalámbricos y acceso a Internet son las que proveen las plataformas de telecomunicaciones. (Kenneth & Jane, 2012, pág. 180)

H. PLATAFORMAS DE INTERNET

Las plataformas de Internet se traslapan y deben estar relacionadas con la infraestructura de redes general de la empresa, además de sus plataformas de hardware y software. Un servicio de hospedaje Web mantiene un servidor Web grande o una serie de servidores, además de proporcionar espacio a los suscriptores que pagan una cuota por mantener sus sitios Web. Las principales herramientas y suites de desarrollo de aplicaciones de software Web las proveen Microsoft (Microsoft Expression Web, SharePoint Designer y la familia Microsoft .NET de herramientas de desarrollo); Oracle-Sun (Java de Sun es la herramienta más utilizada para desarrollar aplicaciones Web interactivas, tanto del lado servidor como del lado cliente), y una variedad de desarrolladores de software independientes, como Adobe (Flash y herramientas de texto como Acrobat) y Real Media (software de medios). (Kenneth & Jane, 2012, pág. 180)

I. SERVICIOS DE CONSULTORÍA E INTEGRACIÓN DE SISTEMAS

Para (Kenneth & Jane, 2012) menciona que para implementar una nueva infraestructura se requieren cambios considerables en los procesos y procedimientos de negocios, capacitación y educación, e integración de software.

Integración de software significa asegurar que la nueva infraestructura funcione con los sistemas anteriores de la empresa, conocidos como sistemas heredados, y también significa asegurar que los nuevos elementos de la infraestructura puedan trabajar en conjunto. Por lo general los sistemas heredados son sistemas de procesamiento de transacciones antiguos, creados para computadoras mainframe que se siguen utilizando para evitar el alto costo de reemplazarlos o rediseñarlos. (p. 181)

2.2.29 CORTAFUEGOS (FIREWALLS)

"Los cortafuegos pueden ser un medio eficaz de protección de un sistema o red local frente a las amenazas de seguridad provenientes de la red, mientras que al mismo tiempo proporcionan acceso al exterior mediante redes de área ancha e Internet" (Stallings, 2004, p.376).

A. CARACTERÍSTICAS DE LOS CORTAFUEGOS

Para (Stallings, 2004) considera 3 tipos de características de cortafuegos:

a) Todo el tráfico desde el interior hacía el exterior, y viceversa, debe pasar a través del cortafuego. Esto se consigue bloqueando físicamente todos los accesos a la red local excepto a través del cortafuego. Hay diferentes configuraciones, como se explicará más tarde en esta sección.
b) Se permitirá pasar solamente el tráfico autorizado, definido por la política de seguridad local. Se utilizan diferentes tipos de cortafuegos que implementan diferentes tipos de políticas de seguridad, como se explicará más tarde en esta sección.
c) El propio cortafuegos es inmune a la penetración. Esto implica que utiliza un sistema a de confianza con un sistema operativo seguro. (p.363)

B. TIPOS DE CORTAFUEGOS

Según (Stallings, 2004) existe tres tipos de cortafuegos más comunes: filtradores de paquetes, pasarelas del nivel de aplicación y pasarelas del nivel de circuito.(p.365)

a) Router de Filtrado de Paquetes
b) Pasarela del Nivel de Aplicación
c) Pasarela del Nivel de Circuito

a) Router de Filtrado de Paquetes: Un router de filtrado de paquetes aplica un conjunto de reglas a cada paquete IP y entonces retransmite o descarta dicho paquete. El router, normalmente, se configura para filtrar paquetes que van en ambas direcciones (desde y hacia la red interna). Las reglas de filtrado se basan en la información contenida en un paquete de red. (Stallings, 2004, pág. 366)

- **Dirección IP de Origen:** Se conoce como la dirección IP del sistema que originó el paquete IP.

- **Dirección IP de Destino:** Se conoce como la dirección IP del sistema al que se intenta llegar el paquete IP.
- **Direcciones de nivel de transporte de origen y destino:** el número de puerto del nivel de transporte (por ejemplo, TCP o UDP), que define aplicaciones como SNMP o TELNET.
- **Campo de protocolo IP:** Se encarga de definir el protocolo de transporte.
- **Interfaz:** La interfaz se realiza para un router con tres o más interfaces, indica desde qué interfaz viene el paquete o hacia cuál va destinado.

b) Pasarela del Nivel de Aplicación: Una pasarela del nivel de aplicación, también llamada servidor *proxy*; actúa como un repetidor del tráfico del nivel de aplicación El usuario contacta con la pasarela utilizando una aplicación TCP/IP como, por ejemplo, Telnet o FTP, y la pasarela solicita al usuario el nombre del computador remoto al que desea acceder. Cuando el usuario responde y proporciona un identificador de usuario e información de autentificación válidos, la pasarela contacta con la aplicación en el computador remoto y retransmite los segmentos TCP que contienen los datos de aplicación entre los dos puntos finales. Si la pasarela no implementa el código *proxy* de una aplicación específica, entonces el servicio no está permitido y no puede atravesar el cortafuegos. Además, la pasarela puede configurarse para permitir solamente algunas características específicas de una aplicación que el administrador de red considere aceptables mientras que deniega las otras características. (Stallings, 2004, pág. 370)

c) **Pasarela del Nivel de Circuito:** Una pasarela del nivel de circuito no permite una conexión TCP extremo a extremo; en vez de eso, la pasarela establece dos conexiones TCP, una entre ella y un usuario TCP en un computador interno, y otra entre ella y un usuario TCP en un computador externo. Una vez se han establecido las dos conexiones, la pasarela normalmente retransmite segmentos TCP desde una conexión hacia la otra sin examinar los contenidos. La función de seguridad consiste en determinar qué conexiones serán permitidas. (Stallings, 2004, pág. 370)

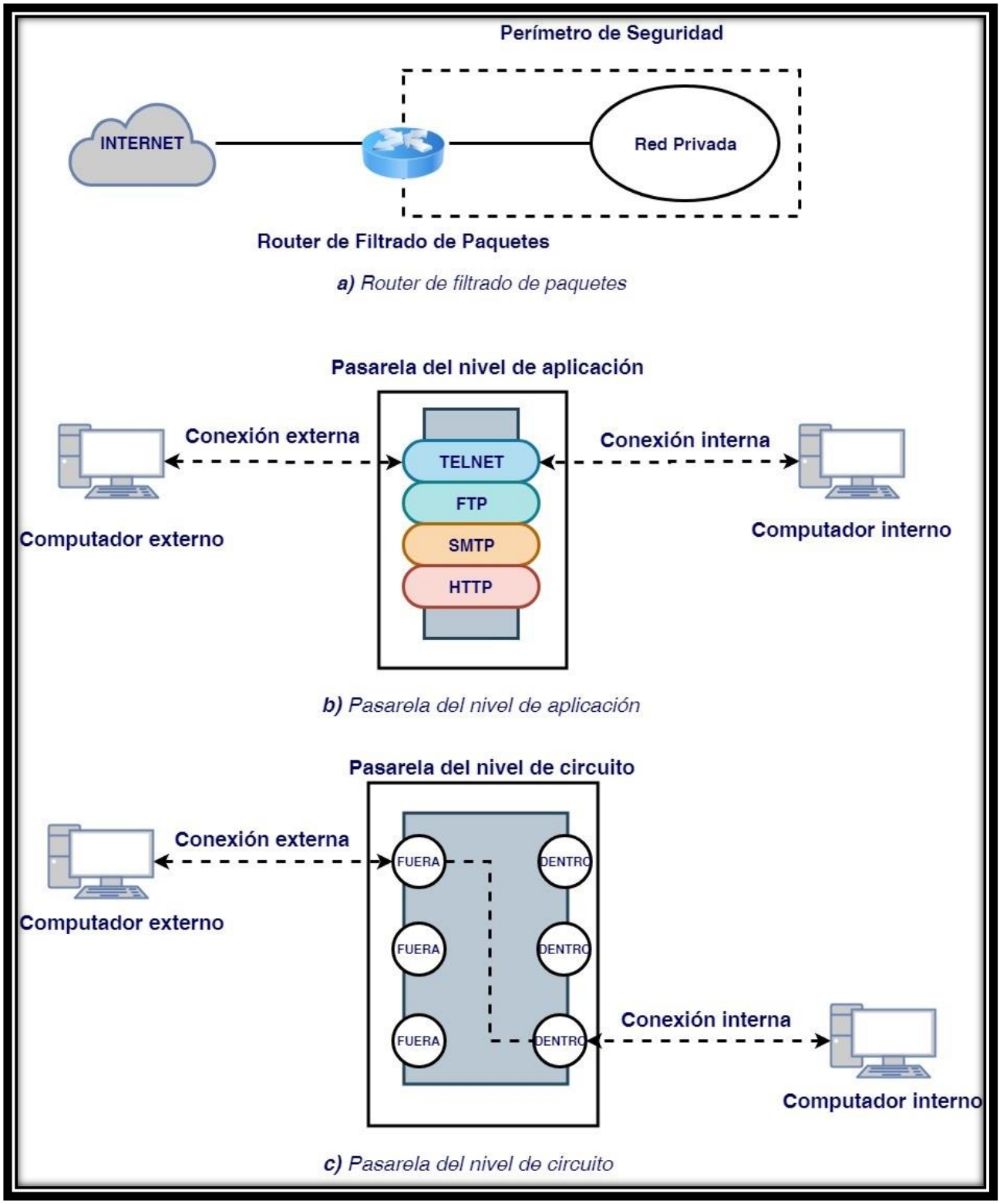


Figura N° 26. Tipos de Cortafuegos

Fuente: (Stallings, 2004, p.365).

2.2.30 GUÍA DE FUNDAMENTOS PARA LA DIRECCIÓN DE PROYECTOS

A. ¿QUÉ ES UN PROYECTO?

Un proyecto es un esfuerzo temporal que se lleva a cabo para crear un producto, servicio o resultado único. (Project Managament Institute, 2013) considera que: "Al mencionar "temporal", lo que se quiere dejar claro es que tiene una fecha de inicio definida y una fecha de término establecida, es decir, se limita a un lapso de tiempo en el que se tiene que llevar cabo" (p.3).

> Un proyecto es cuando se busca desarrollar un objetivo y se desea conocer cuál puede ser el resultado final de materializar por ejemplo una idea. En concreto se desea dar respuesta a un problema planteado, buscar posibles soluciones a un escenario desconocido, es buscar como de forma organizada se puede llegar a un resultado que se dio en primera instancia por una incógnita, una necesidad inicial, cuando se conoce el resultado se da fin a ese proyecto, y tal vez, se puede empezar otro. (Estrada, 2015, pág. 13)

B. ¿QUÉ ES LA DIRECCIÓN DE PROYECTOS?

La dirección de proyectos es la aplicación de conocimientos, habilidades, herramientas y técnicas a las actividades del proyecto para cumplir con los requisitos del mismo. Se logra mediante la aplicación e integración adecuadas de los 47 procesos de la dirección de proyectos, agrupados de manera lógica, categorizados en cinco Grupos de Procesos. (Project Managament Institute, 2013, pág. 32)

- Inicio
- Organización y Preparación
- Ejecución del Trabajo.
- Cierre.

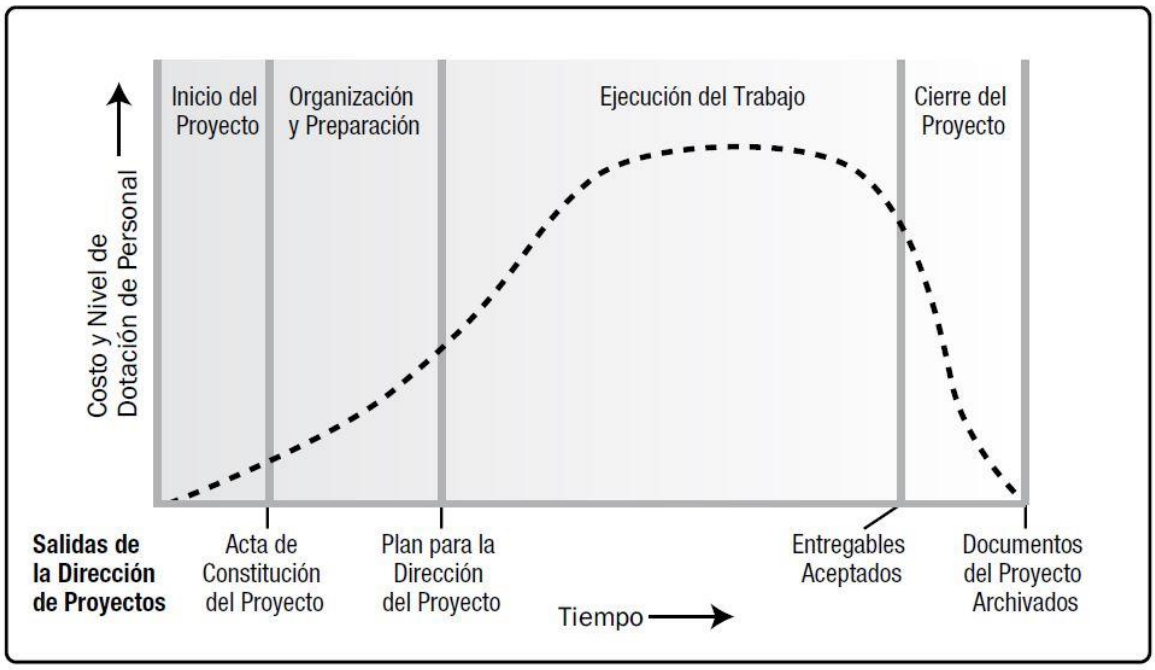


Figura N° 27. Niveles Típicos de Costo y Dotación de Personal en una Estructura Genérica del Ciclo de Vida del Proyecto

Fuente: (Project Managament Institute, 2013, pág. 38)

C. FASES DEL PROYECTO

Es un conjunto de actividades, que marcan un inicio y un final de una etapa dentro del proyecto con la realización de uno o varios entregables. El (Project Managament Institute, 2013) manifiesta que:

> Las diferentes fases que se presentan son de forma secuencial, en ciertas situaciones suelen superponerse, por lo que representan un esfuerzo y una duración diferente. Al estructurar las fases del proyecto nos permite dividirlo en pequeñas partes lógicas, para su dirección planificación y control. Esta división o el número de fases depende únicamente del tamaño del proyecto, su complejidad o el impacto del proyecto. (p.40)

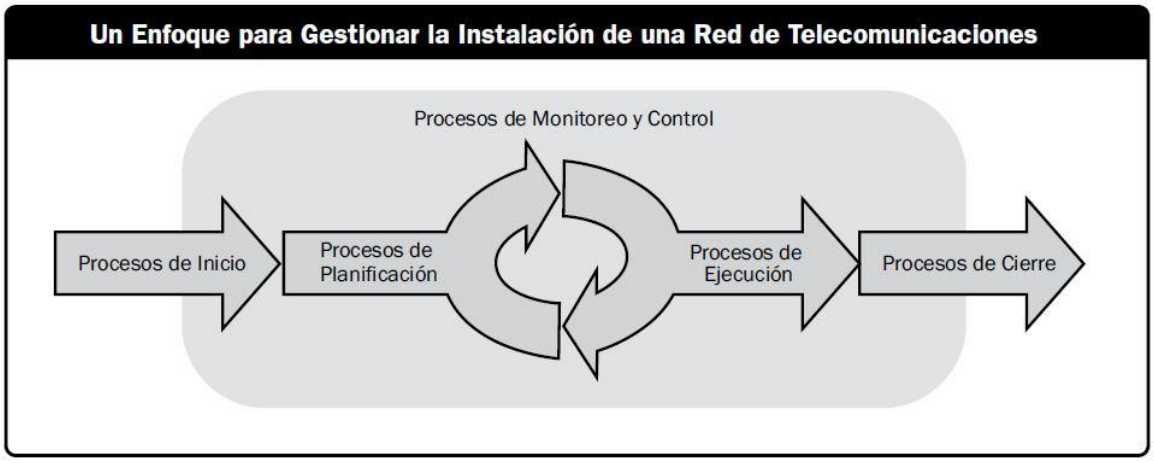


Figura N° 28. Niveles Típicos de Costo y Dotación de Personal en una Estructura Genérica del Ciclo de Vida del Proyecto

Fuente: (Project Managament Institute, 2013, pág. 41)

D. ÁREAS DE CONOCIMIENTO DE LA DIRECCIÓN DE PROYECTOS

"En las áreas de conocimiento de la dirección de proyectos se ha considerado conveniente dividirlos en diez áreas de conocimiento" (Project Managament Institute, 2013, pág. 62).

1. Gestión de la Integración
2. Gestión del Alcance
3. Gestión del Tiempo
4. Gestión de Costos
5. Gestión de Calidad
6. Gestión de Recursos Humanos
7. Gestión de Comunicaciones
8. Gestión de Riesgos
9. Gestión de Adquisiciones
10. Gestión de los Interesados

1. GESTIÓN DE LA INTEGRACIÓN

La gestión de la integración radica en tomar decisiones sobre donde concentrar recursos y esfuerzos requeridos para asegurar una adecuada iniciación del proyecto y de sus fases, así como en la búsqueda de la unificación, consolidación, articulación y

acciones de integración que son cruciales para concluir el proyecto. (Project Managament Institute, 2013, pág. 63).

- Documentación de los criterios específicos de los requisitos del producto.
- Análisis del alcance. Lo cual incluye los requisitos del proyecto, los criterios, las asunciones, las restricciones, etc.
- Preparación del EDT.
- Identificación de las acciones necesarias para que se realice el proyecto de acuerdo a lo planificado.
- Establecer métricas para los procesos y productos del proyecto.
- Análisis de los riesgos del proyecto.

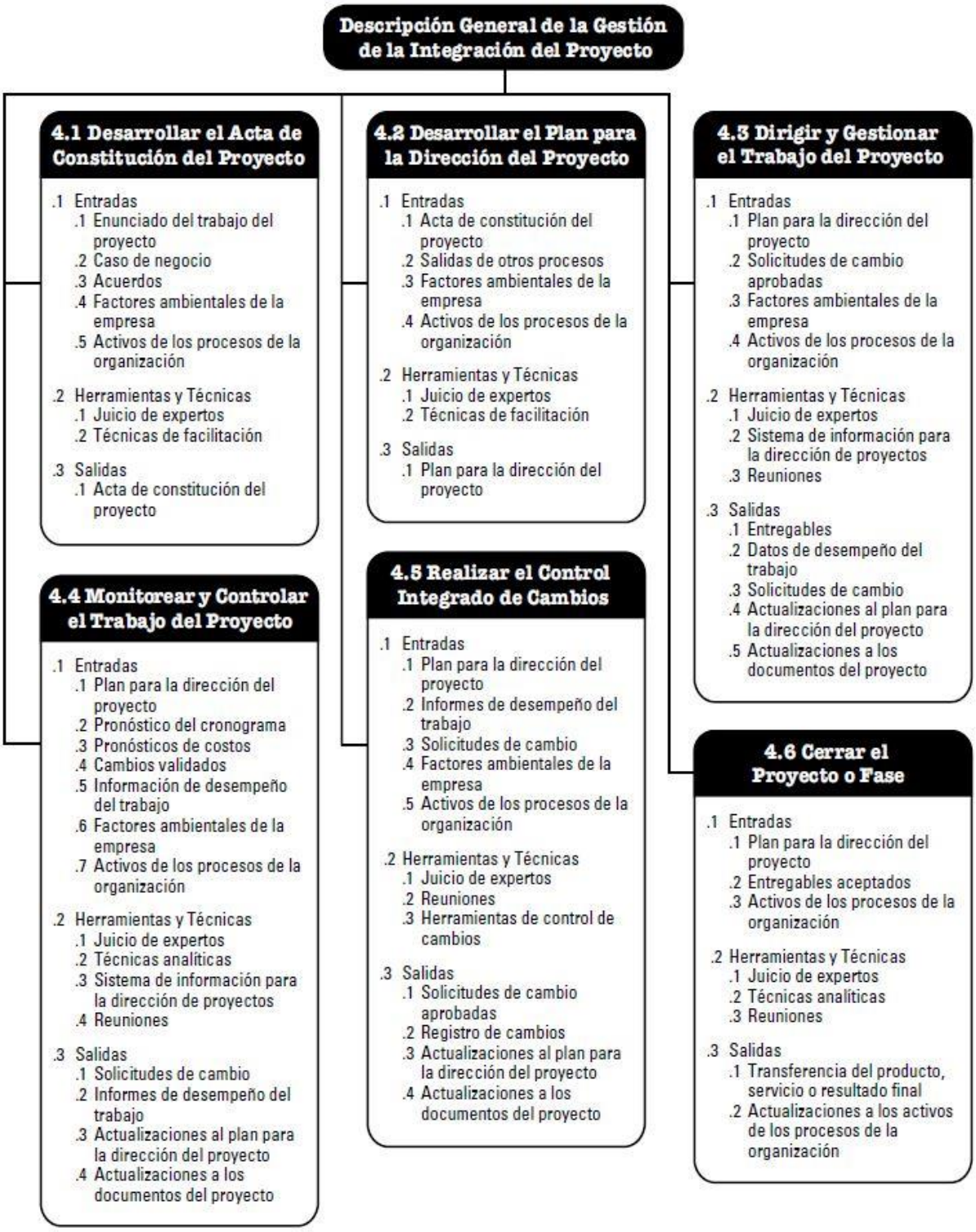


Figura N° 29. Descripción General de la Gestión de la Integración del Proyecto

Fuente: (Project Managament Institute, 2013, pág. 64)

2. GESTIÓN DEL ALCANCE

La Gestión del Alcance es la suma de procesos identificados para asegurar que el proyecto incluya todo el trabajo requerido, y sólo el trabajo requerido, para completar el

proyecto con éxito. Como medio de registro en la entrada se utiliza el Acta de Constitución del Proyecto y el Registro de Interesados del Proyecto, como técnica para la creación de la EDT (herramienta), se utilizará la técnica de descomposición a nivel de paquetes de trabajo, desarrollando el Plan de Gestión del Alcance con sus componentes. (Project Managament Institute, 2013, pág. 104)

- Definir la Estructura de desglose del trabajo (EDT)
- Definir por tanto los Entregables del proyecto.
- Verificar que el EDT presentado por terceros gestionados (Proyectos, proveedores, etc.), incluyan todo el trabajo requerido, para alcanzar los objetivos del Proyecto y cumplan con los requerimientos del Cliente.
- Plantear trabajos adicionales, que deben de incluirse en el EDT de los Terceros (Proyectos, proveedores, etc.,) para asegurar alcanzar los objetivos del proyecto.
- Realizar el "Control de Cambios", que permitan registrar y controlar los cambios en el alcance del proyecto. Toda variación debe ejecutarse, previo sustento aprobado por el Consultor y aprobado por el Cliente.

3. GESTIÓN DEL TIEMPO

La gestión del tiempo incluye los procesos necesarios, para lograr la conclusión del proyecto a tiempo, dentro del plazo contractual previsto. Para la Gestión del Tiempo, se desarrollará el plan de Gestión del Cronograma, teniendo como entrada la información generada en la línea base del alcance, como técnica de definición de las actividades se utilizará la técnica de descomposición y el "juicio experto", dichas actividades serán creadas sobre la base de la EDT, donde cada paquete de trabajo podrá descomponerse hasta un máximo de 10 actividades. (Project Managament Institute, 2013, pág. 143)

- Definir las Actividades, de sus fases de Obras, suministro u otras actividades
- Definir la estimación de la duración de dichas Actividades
- Definir la estrategia y/o plan para implementar sus fases y el Proyecto completo,
- mediante un Cronograma y/o Diagrama Gantt y un Diagrama de Red (Ruta Crítica) del Proyecto, utilizando algún software de Gestión de Proyectos: Ms Project, primavera, etc.

- Actualizar periódicamente el Cronograma del Proyecto, e implementar "Curvas S de avance" programado vs real, para controlar el avance del mismo, implementando las reprogramaciones que sean necesarias en caso de variaciones adicionales.
- Implementar Reportes de avance, de notificación de problemas y de planteamiento de soluciones a los mismos.
- Implementar la Técnica del Valor Ganado.

4. GESTIÓN DE COSTOS

El Plan de Gestión del Costo incluye los procesos necesarios, para controlar el presupuesto del proyecto, de manera que el mismo pueda completarse dentro del presupuesto aprobado, cuyo principal objetivo es el de describir cómo será gestionado la culminaron del proyecto en el Presupuesto. Para esto, se incluye los procesos requeridos, desde la estimación de los costos de cada actividad, determinación de la Línea base del costo y la Necesidad de financiamiento. Finalmente se incluye un proceso de control del costo del proyecto. (Project Managament Institute, 2013, pág. 194)

- Ajustarse al presupuesto aprobado y formalizado, mediante los diversos contratos que el Cliente suscriba con sus diversos proyectos y/o proveedores.
- Implementar la Técnica del Valor Ganado, para verificar sobrecostos y proyecciones
- Verificar la procedencia de los Presupuestos, presentados por los Proyectos y/o Proveedores.
- Controlar los Costos del proyecto, la procedencia de los pagos por cada concepto, pagos puntuales o por hitos (para el caso de las adquisiciones) y pago por valorizaciones (para el caso de las Obras)
- Aprobar los trabajos adicionales, requeridos para alcanzar los objetivos del Proyecto.
- Efectuar proyecciones, sobre los costos finales del proyecto.

5. GESTIÓN DE CALIDAD

La Gestión de Calidad va a tener su base en la Política de Calidad del Proyecto, la cual cumplirá con los requisitos de calidad desde el punto de vista del cliente, es decir culminar el Proyecto en el tiempo y presupuesto planificado, cumpliendo con las normas aplicables y utilizando la tecnología adecuada con el fin de brindar la satisfacción a los requerimientos del cliente. Incluye los procesos necesarios, para determinar políticas,

parámetros y responsabilidades necesarias para ejecutar el proyecto, satisfaciendo los requerimientos y necesidades del Cliente, para lo cual utilizaremos los conceptos y plantillas para los procesos de ejecución, seguimiento y control de la calidad. (Project Managament Institute, 2013, pág. 228)

- Presentar el Plan de Calidad y sus respectivos sus parámetros.
- Presentar Normas y Especificaciones para sus entregables.
- Presentar procedimientos de Aseguramiento de Calidad de tal forma que los productos satisfagan los objetivos del Proyecto.
- Aprobar Plan de Calidad, presentado por los Proyectos y Proveedores.
- Verificar que los Suministros y Obras, se ejecuten cumpliendo con las Normas,
- Especificaciones y buenas prácticas de la Ingeniería.
- Establecer Acciones Preventivas y/o Correctivas, ante la detección de desviaciones.

6. GESTIÓN DE RECURSOS HUMANOS

La gestión de recursos humanos se realizará con el fin de determinar los roles del proyecto, las responsabilidades y las relaciones de informe en el proyecto. Para realizar la planificación se tomarán en cuenta la estructura de la organización, asimismo se definirán los requisitos de recursos de las actividades a través de plantillas y listas de control. Incluye los procesos necesarios, para organizar, dirigir y controlar el uso de los recursos humanos planteados, de manera que sean los suficientes y capaces para lograr los objetivos del proyecto, verificando que se asignen eficientemente roles y responsabilidades, en cada una de sus fases. (Project Managament Institute, 2013, pág. 256)

- Establecer procesos de desarrollo y capacitación del personal del proyecto, a fin de contar con personal capacitado en la ejecución de sus tareas.
- Cumplir con las “Normas de Seguridad y Salud Ocupacional” para los trabajadores del Proyecto.
- Crear un Organigrama del personal, así como una matriz de responsabilidad y funciones.
- El Reclutamiento y Selección del personal y equipo de proyecto

- Controlar el cronograma de uso de recursos humanos del proyecto, verificando que la asignación real de recursos humanos sea igual o mayor a la programada.
- Implementar procesos de Desarrollo y capacitación de su personal asignado al Proyecto.
- Verificar que se asignen los recursos ofrecidos en conformidad a su matriz de responsabilidad y función.

7. GESTIÓN DE COMUNICACIONES

La gestión de comunicaciones incluye los procesos necesarios, para asegurar la generación, recolección, distribución, almacenamiento, recuperación y disposición oportuna y apropiada de la información del Proyecto. Para la planificación de las comunicaciones se utilizará el registro de los interesados en la medida que impacten en el desarrollo del proyecto con el fin de determinar las necesidades de información y como serán abordadas por los interesados del proyecto. Como herramienta se utilizará el análisis de los requisitos de las comunicaciones, este análisis da como resultado la suma de las necesidades de información de los interesados en el Proyecto. (Project Managament Institute, 2013, pág. 288)

- Definir sus requerimientos y tecnología, para implementar una buena comunicación dentro del proyecto.
- Registrar las Lecciones Aprendidas, éxitos y fracasos en la ejecución de sus tareas, para que sirva para fases posteriores o para futuros proyectos.
- Establecer informes de rendimiento para presentar Informes Mensuales Ejecutivos que muestren el estado situacional, técnico –económico y contractual, de las diversas fases del proyecto.
- Establecer una adecuada y oportuna distribución de la Información: técnica, comercial, contractual, legal, etc.
- Implementar un sistema adecuado de generación, recolección y difusión de las comunicaciones, a las personas que lo requieran, para que todo los involucrados, conozcan la información que deben conocer, para facilitar el logro de los objetivos del Proyecto.

8. GESTIÓN DE LOS RIESGOS

El Objetivo del Plan de Gestión de Riesgos, está definido por identificar los riesgos que tienen probabilidad de impactar positiva o negativamente en el proyecto, así como planificar las respuestas a los riesgos identificados con mayor probabilidad de ocurrencia, durante el ciclo de vida del Proyecto. Incluyendo los procesos relacionados con la planificación de los riesgos, su identificación y análisis, el planteamiento de respuestas a dichos riesgos y el seguimiento y control de la gestión de los riesgos del proyecto en la búsqueda de incrementar la probabilidad de ocurrencia de aquellos positivos y disminuir o eliminar la ocurrencia de aquellos negativos. (Project Managament Institute, 2013, pág. 310)

- Desarrollar la "Planificación de la Gestión de Riesgos".
- Identificar los posibles riesgos para las diferentes fases del Proyecto.
- Definir la probabilidad e Impacto de dichos riesgos.
- Generación de plan de contingencias ante los riesgos, con el fin de mitigarlos, evitarlos y/o afrontarlos.
- Análisis Cualitativo de los riesgos identificados, para desarrollar respuestas efectivas a los riesgos. El Análisis Cuantitativo de los riesgos, tiene más valor en proyectos complejos y de alta inversión (megaproyectos).
- Priorización de riesgos identificados para el proyecto.
- Seguimiento y control permanente de dichos riesgos.

9. GESTIÓN DE ADQUISICIONES

El propósito de la gestión de adquisiciones es documentar y describir como serán gestionados los procesos de adquisiciones para el proyecto, desde la identificación y el desarrollo de la documentación para las adquisiciones hasta el cierre del contrato, incluyendo los procesos necesarios para comprar o adquirir los bienes y servicios, necesarios para ejecutar el proyecto. También incluye los procesos de gestión que son necesarios para administrar, implementar cambios contractuales y cerrar los contratos con los potenciales proveedores. (Project Managament Institute, 2013, pág. 356)

- Suscribir oportunamente los contratos con los proveedores de manera que se cumpla con el cronograma del Proyecto, dentro de los plazos contractuales.
- Los clientes y proveedores deben cumplir con sus obligaciones contractuales, de manera que no afecte al desarrollo de sus obligaciones.
- Preparar la liquidación de sus contratos.
- Revisión y aprobación de las liquidaciones de los diversos contratos de proveedores.
- Verificar que proveedores cumplan con sus obligaciones contractuales.
- Revisión de los Expedientes Técnicos, documentos y procesos de adquisición, concurso o licitación de suministros y obras.
- Verificar los criterios de evaluación utilizados para los proveedores.

10. GESTIÓN DE INTERESADOS

El propósito de la gestión de los interesados es identificar a las personas, grupos u organizaciones que pueden afectar o ser afectados por el proyecto, para analizar las expectativas de los interesados y su impacto en el proyecto, y para desarrollar estrategias de gestión adecuadas a fin de lograr la participación eficaz de los interesados en las decisiones y en la ejecución del proyecto. La gestión de los interesados también se centra en la comunicación continua con los interesados para comprender sus necesidades y expectativas, abordando los incidentes en el momento en que ocurren, gestionando conflictos de intereses y fomentando una adecuada participación de los interesados en las decisiones y actividades del proyecto. La satisfacción de los interesados debe gestionarse como uno de los objetivos clave del proyecto. (Project Managament Institute, 2013, pág. 392)

- Identificar las personas, grupos u organizaciones que podrían afectar o ser afectados por una decisión, actividad o resultado del proyecto
- Analizar y documentar información relevante relativa a los intereses, participación, interdependencias, influencia y posible impacto en el éxito del proyecto de los interesados.
- Desarrollar estrategias de gestión adecuadas para lograr la participación eficaz de los interesados a lo largo del ciclo de vida del proyecto.
- Comunicar y trabajar con los interesados para satisfacer sus necesidades/expectativas, abordar los incidentes en el momento en que ocurren y fomentar la participación

adecuada de los interesados en las actividades del proyecto a lo largo del ciclo de vida del mismo.

- Monitorear globalmente las relaciones de los interesados del proyecto y ajustar las estrategias y los planes para involucrar a los interesados.

2.2.31 SOFTWARE

La IEEE (2011) considera que: "El software es el conjunto de los programas de cómputo, procedimientos, reglas, documentación y datos asociados que forman parte de las operaciones de un sistema de computación" (p.69).

Para (Ibañez & García, 2009) considera lo siguiente:

> El software es el conjunto de programas, documentos, procedimientos y rutinas asociados con la operación de una computadora; tiene las funciones de administrar los recursos o medios de la computadora, proporcionar herramientas para usar eficientemente estos recursos, actuar como enlace entre el usuario y la computadora. Se clasifican en software del sistema, software de aplicación, software de usuario final. (pág. 178)

> El software es un conjunto de programas que gestionan y controlan el hardware. Se encuentran almacenados en dispositivos de almacenamiento como, por ejemplo, discos duros. Uno de estos principales programas es el sistema operativo. MS-DOS, Windows o Linux son ejemplos de SO. Existen otras aplicaciones o utilidades que permiten trabajar con el ordenador, como son, el word, excel, etc. (López, 2004, pág. 210)

2.2.32 HARDWARE

Según (Ibañez & García, 2009) respecto al hardware definen:

> El hardware es la parte materia, o que puedes tocar, de la computadora: dispositivos de entrada, de salida, CPU, etc.; se clasifican en básico y complementario, el básico es todo dispositivo o aparato necesario para iniciar el funcionamiento de la computadora y el complementario realiza funciones específicas o más allá de las básicas. (p. 169)

Por otra parte (López, 2004) considera que: “El hardware es la parte que estudia los componentes físicos del equipo, es decir, el material tangible que compone el ordenador” (p.67).

“El Hardware corresponde a todas las partes tangibles de un sistema informático; sus componentes son: eléctricos, electrónicos, electromecánicos y mecánicos. Son cables, gabinetes o cajas, periféricos de todo tipo y cualquier otro elemento físico involucrado”. (Ibañez & García, 2009, pág. 170)

CAPÍTULO III
METODOLOGÍA DE LA INVESTIGACIÓN

3.1 TIPO Y NIVEL DE INVESTIGACIÓN

3.1.1 TIPO DE INVESTIGACIÓN

Según (Hernández, Fernández, & Baptista, 1991), concluyen lo siguiente respecto a la investigación de tipo observacional.

> Es aquella que se basa en la observación de los fenómenos, características, situaciones, variaciones, etc. del asunto que se quiere investigar. Solo se observa, sin manipular, cambiar o variar nada. Luego, las observaciones hechas se pueden registrar para posterior análisis. (p.57)

Por lo tanto, el estudio es de tipo observacional, porque no se interviene en el manejo de la información, solo se limita a observar la información que existe de los recursos proporcionados en la red de datos de la UGEL Huamanga.

> Según (Supo, 2015), manifiesta que los estudios retrospectivos son estudios que utilizan datos de registros que existen, datos que provienen de mediciones donde el investigador no tuvo participación, denominada datos secundarios. Es decir, son mediciones que no fueron realizadas por el investigador, donde se desconoce si las mediciones fueron controladas. (p.63)

La investigación también es considerada de tipo retrospectivo porque utilizamos los recursos existentes en la red de datos de la UGEL Huamanga, que son el tráfico de red, servicios, consumo de ancho de banda, equipos TIC.

El tipo de estudio es longitudinal porque levantamos datos de forma repetitiva para las variables de estudio y así realizar las pruebas en el periodo 2018.

3.1.2 NIVEL DE INVESTIGACIÓN

Para (Murillo, 2015) la investigación aplicada recibe el nombre de "investigación practica o empírica", que se caracteriza porque busca la aplicación o utilización de los

conocimientos adquiridos, a la vez que se adquieren otros, después de implementar y sistematizar la practica basada en investigación. El uso del conocimiento y los resultados de investigación que da como resultado una forma rigurosa, organizada y sistemática de conocer la realidad.

El nivel de investigación es aplicada debido a que a partir de la información generada se buscará la aplicación de ello y dar solución al problema respecto a los recursos, servicios y equipos con los que se cuenta en la red de datos de la UGEL Huamanga.

3.2 DISEÑO DE LA INVESTIGACIÓN

La información que se necesita para el estudio se ha recolectado de todos los recursos, servicios y equipos que se maneja en la red de datos de la UGEL Huamanga 2018, es decir se describe las características a detalle como son el tráfico de red, consumo de ancho de banda, inactividad de servicios y así emplear la Gestión y Monitoreo.

3.3 MÉTODO

En la presente investigación se utilizaron los siguientes métodos:

A. MÉTODO INDUCTIVO: Proceso de conocimiento que se inicia por la observación de fenómenos particulares con el propósito de llegar a conclusión y premisas generales que pueden ser aplicadas a situaciones similares a la observación.

B. MÉTODO DE ANÁLISIS: Proceso de conocimiento que se inicia por la identificación de cada una de las partes que caracterizan una realidad. De esa manera se establece la relación causa-efecto entre los elementos que compone el objeto de investigación.

3.4 POBLACIÓN Y MUESTRA

3.4.1 POBLACIÓN

La población está compuesta por todos los recursos de la red que vienen a ser los dispositivos, servicios de la red de datos en la UGEL Huamanga, 2018.

3.4.2 MUESTRA

La muestra aleatoria se calculará con un 95% de confianza y un 5% de error, de todos los recursos de la red de datos de la UGEL Huamanga, 2018.

3.5 VARIABLES E INDICADORES

VARIABLE INDEPENDIENTE

Gestión y Monitoreo. – La gestión define el control de los recursos en una red con el fin de evitar que esta llegue a funcionar incorrectamente degradando sus prestaciones, mientras que el monitoreo define un proceso continuo de recolección y análisis de datos con el fin de anticipar problemas en la red.

INDICADORES DE LA VARIABLE INDEPENDIENTE

Base de Información (MIB). –Es un tipo de base de datos que contiene información jerárquica, estructurada en forma de árbol, de todos los parámetros gestionables en cada dispositivo gestionado de una red de comunicaciones. Es parte de la gestión de red definida en el modelo OSI. Define las variables usadas por el protocolo SNMP para supervisar y controlar los componentes de una red. Está compuesta por una serie de objetos que representan los dispositivos (como enrutadores y conmutadores) en la red. Cada objeto manejado en un MIB tiene un identificador de objeto único e incluye el tipo de objeto (tal como contador, secuencia o gauge), el nivel de acceso (tal como lectura y escritura), restricciones de tamaño, y la información del rango del objeto.

Protocolo SNMP (Simple Network Management Protocol). - El protocolo de estándar de la capa de aplicación para manejar y monitorear dispositivos y servicios de redes, se basa en paquetes UDP, protocolo de la capa de transporte, basado en IP como se puede ver en la figura 2.1, compatible con SMNP. UDP es un protocolo sin conexión que no garantiza la entrega del paquete, por lo tanto, SMNP es un protocolo no orientado a la conexión y utiliza los puertos 161 y 162.

Estación de Gestión (NMS). - También conocido como sistema de gestión de red o NMS (Network Management System), es una aplicación o conjunto de aplicaciones que permite a los administradores de red administrar los componentes independientes de una red dentro de un marco de administración de red más grande. Un NMS se puede usar para monitorizar componentes de software y hardware en una red. Por lo general, registra los datos de los puntos remotos de una red para llevar a cabo informes centrales a un administrador del sistema.

VARIABLE DEPENDIENTE

Red de Datos. – La red de datos a aquellas infraestructuras o redes de comunicación que se ha diseñado específicamente a la transmisión de información mediante el intercambio de datos. Las redes de datos se diseñan y construyen en Arquitecturas que pretenden servir a sus objetivos de uso. Las redes de datos, generalmente, están basadas en la Comunicación de paquetes y se clasifican de acuerdo a su tamaño, la distancia que cubre y su arquitectura física

INDICADORES DE LA VARIABLE DEPENDIENTE

Red LAN. - Una red de área local, red local o LAN (del inglés local area network) es la interconexión de varias Computadoras y Periféricos. Su extensión está limitada físicamente a un edificio o a un entorno de 200 metros, o con Repetidores podría llegar a la distancia de un campo de 1 kilómetro. Su aplicación más extendida es la interconexión de computadoras personales y estaciones de trabajo en oficinas, fábricas, etc., para compartir recursos e intercambiar Datos y Aplicaciones. En definitiva, permite una conexión entre dos o más equipos. El término red local incluye tanto el Hardware como el Software necesario para la interconexión de los distintos dispositivos y el tratamiento de la información.

Red WLAN. - La WLAN es un tipo específico de LAN: una red informática formada por unidades ubicadas en un espacio geográfico de dimensiones reducidas. Mientras que las computadoras (ordenadores) que forman parte de una LAN se conectan entre sí o a un router con cables, en una WLAN la conexión se realiza utilizando ondas de radiofrecuencia. Las WLAN suelen posibilitar que los usuarios tengan una amplia movilidad, ya que no dependen de cables o elementos físicos para permanecer en la red. La ausencia de cables también contribuye a mantener un orden o una organización en la oficina o el ambiente en cuestión.

3.6 DEFINICIÓN OPERACIONAL DE LAS VARIABLES

VARIABLE INDEPENDIENTE

X: Gestión y Monitoreo

INDICADORES DE LA VARIABLE INDEPENDIENTE

X1: Base de Información (MIB)

X2: Protocolo SNMP

X3: Estación de Gestión (NMS)

VARIABLE DEPENDIENTE

Y: Red de Datos

INDICADORES DE LA VARIABLE DEPENDIENTE

Y1: Red LAN

Y2: Red WLAN

3.7 TÉCNICAS E INSTRUMENTOS PARA EL TRATAMIENTO DE DATOS E INFORMACIÓN

3.7.1 TÉCNICAS PARA RECOLECTAR INFORMACIÓN

Se utilizó las técnicas de análisis documental y entrevista al responsable de la Oficina de Informática de la UGEL Huamanga, para recolectar información detallada en relación a la infraestructura, los recursos que existen en la red de datos como son los hosts, servicios, dispositivos y el tráfico de red en horas pico.

3.7.2 INSTRUMENTOS PARA RECOLECTAR INFORMACIÓN

Se utilizó el instrumento guía de entrevista al responsable de la Oficina de Informática de la UGEL Huamanga para obtener información acerca de la infraestructura, los recursos que maneja la red de datos, instrumento que se muestra en el anexo B, por otra parte, también se utilizó el instrumento de observación documental que consta del análisis profundo de las fuentes documentales, es decir, se toma la información y se registra para su posterior análisis. La observación es un elemento fundamental de todo proceso investigativo; en ella se apoya la investigación para obtener el mayor número de datos.

3.8 HERRAMIENTAS PARA EL TRATAMIENTO DE LA INFORMACIÓN

Las herramientas tecnológicas que utilizamos en el tratamiento de datos, serán considerando de acuerdo a las limitaciones de la situación actual como son; los recursos humanos, infraestructura y financiamiento para la implementación del servidor de gestión y monitoreo es necesario prepararlo con un software mínimo requerido.

NOMBRE	FABRICANTE	SERVICIO
Windows 7, 8, 10	**Microsoft Corporation**	Sistema Operativo de Microsoft, línea de sistemas operativos con licencia producida por Microsoft Corporación.
CENTOS 7	**Linux**	Es una distribución de Linux como Sistema Operativo, que proporciona una plataforma

		informática gratuita, de clase empresarial y compatible con la comunidad.
Nethserver	**Linux**	NethServer es una distribución basada en Linux que está orientada específicamente a actuar como servidor en pequeñas y medianas oficinas. Esta distribución está basada en las populares distribuciones CentOS y Red Hat Enterprise Linux, por lo que la estabilidad y el soporte con actualizaciones está garantizado.
Ntopng	**Linux**	Es una poderosa herramienta que permite analizar en tiempo real el tráfico de red. Esto te permite evaluar el ancho de banda utilizado por IPS o hosts individuales, por puertos, e identificar los protocolos de red más utilizados.
Suricata-Nethserver	**Linux**	Es un sistema para el análisis de intrusiones en la red. El software analiza todo el tráfico en el firewall en busca de ataques conocidos y anomalías. Cuando se detecta un ataque o anomalía, el sistema puede decidir si bloquear el tráfico o simplemente guardar el evento en un registro.
Zabbix	**Linux**	Zabbix es un Sistema de Monitorización de Redes. Está diseñado para monitorizar y registrar el estado de varios servicios de red, Servidores, y hardware de red. Usa MySQL, PostgreSQL, SQLite, Oracle o IBM DB2 como base de datos. Su backend está escrito en C y el frontend web está escrito en PHP. Zabbix ofrece varias opciones de monitorización

VMware Workstation Player	**EMC Corporation**	Es un software de virtualización disponible para ordenadores compatibles X86. Entre este software se incluyen VMware Workstation, y los gratuitos VMware Server y VMware Player. El software de VMware puede funcionar en Windows, Linux, y en la plataforma macOS que corre en procesadores Intel.

Tabla1. Herramientas tecnológicas para el tratamiento de datos

3.9 TÉCNICAS PARA APLICAR LA METODOLOGÍA

Observando la revisión literaria desarrollada en el capítulo II, sección 2.2.30, formulamos el proceso seleccionado, que considera áreas de conocimiento que aplica la Guía de los fundamentos para la dirección de proyectos (Guía del PMBOK), como se muestra en la siguiente tabla:

ÁREAS DE CONOCIMIENTO	GRUPOS DE PROCESOS DE LA DIRECCIÓN DE PROYECTOS				
	Grupo de Procesos de Inicio	**Grupo de Procesos de Planificación**	**Grupo de Procesos de Ejecución**	**Grupo de Procesos de Monitoreo y Control**	**Grupo de Procesos de Cierre**
1. Gestión de la Integración	• Desarrollar el Acta de Constitución del Proyecto	• Objetivos del Proyecto	• Descripción del Producto del Proyecto	• Factores Críticos del éxito del Proyecto	• Identificación de Interesados
2. Gestión de Alcance	• Definir el Alcance		• Crear la WBS/EDT		

3. Gestión de Tiempo	• Desarrollar el cronograma		• Cronograma de Actividades	• Controlar el cronograma	

4. Gestión de la Calidad	Planificar la gestión de la calidad	• Política de Calidad del Proyecto	• Realizar el Aseguramiento de Calidad	• Controlar la calidad	• Pruebas Unitarias • Pruebas de Integración • Pruebas de Comunicación • Pruebas de Aceptación • Pruebas Funcionales
5. Gestión de los Riesgos	• Planificar la gestión de los riesgos	• Identificar los riesgos	• Realizar el análisis Cualitativo de riesgos • Realizar el análisis Cualitativo de riesgos	• Planificar la respuesta a los riesgos	• Controlar los riesgos
6. Gestión de los Interesados	• Identificar a los interesados		• Gestionar la participación de los interesados	• Controlar la participación de los interesados	

Tabla 2. Grupos de Procesos de la Dirección de Proyectos

CAPÍTULO IV
ANÁLISIS Y RESULTADOS DE LA INVESTIGACIÓN

4.1 RESULTADOS DE LA INVESTIGACIÓN

El siguiente capítulo contiene el desarrollo de la investigación mediante la guía PMBOK, la información técnica de la evaluación y diseño, que servirán para la implementación del servidor de Gestión y Monitoreo de servicios para la red de datos en la sede principal de la UGEL Huamanga.

4.1.1 DESCRIPCIÓN DEL PROYECTO

El proyecto denominado “Implementación de un servidor como gestión y monitoreo de servicios para la red de datos en la UGEL Huamanga” con el objetivo de monitorear el consumo de ancho de banda, análisis de todo el tráfico en el firewall en busca de ataques y anomalías conocidos, los servicios que más usan el CPU, monitorización de los recursos de un host (carga del procesador, uso de los discos, logs del sistema) en varios sistemas operativos como son los que utilizan los servidores, controlar el consumo del ancho de banda, Chequeo de servicios paralizados. reportes y estadísticas del estado cronológico de disponibilidad de servicios y hosts. De tal manera que se logre el correcto funcionamiento de elementos de hardware y software para la red de datos.

4.1.2 UBICACIÓN DEL PROYECTO

A. UGEL Huamanga Sede Principal

La UGEL Huamanga Sede Principal se encuentra ubicada en el Jirón San Martín N° 771, la función principal es la de garantizar el servicio educativo de calidad en todos los niveles y modalidades del sistema educativo, se encarga de coordinar labores y funciones con las entidades educativas asignadas en el departamento de Ayacucho**.**

Figura N° 30. UGEL Huamanga Sede Principal

Fuente: UGEL Huamanga

B. UGEL Huamanga Sede – Área de Gestión Pedagógica

Es el Órgano de línea de la UGEL Huamanga se encuentra ubicada en el Jirón Mario Ramos N° 125, es el encargado de asesorar, orientar, investigar, capacitar, experimentar, supervisar y evaluar las acciones educativas de las Instituciones Educativas, Públicas y Privadas, del ámbito de su competencia, así como las acciones culturales, deportivas y recreacionales**.**

Figura N° 31. UGEL Huamanga Sede Área de Gestión Pedagógica

Fuente: UGEL Huamanga

C. ORGANIGRAMA DE LA UGEL HUAMANGA

El organigrama de la Institución se muestra en el ANEXO A.

4.1.3 GRUPO DE PROCESOS DE INICIO

En este grupo la UGEL Huamanga definirá la existencia del proyecto "Implementación de un servidor como gestión y monitoreo de servicios para la red de datos" mediante los procesos generados según la Guía de Fundamentos para la Dirección de Proyectos (PMBOK)

4.1.4 GESTIÓN DE LA INTEGRACIÓN

A. DESARROLLAR EL ACTA DE CONSTITUCIÓN DEL PROYECTO

Con el Acta de Constitución del Proyecto se autorizará formalmente el Proyecto, se documentará los requisitos iniciales que satisfacen las necesidades y expectativas de los Interesados del Proyecto y se establecerá una relación de cooperación entre la Organización Ejecutante y el Cliente.

NOMBRE DEL PROYECTO	
"IMPLEMENTACIÓN DE UN SERVIDOR COMO GESTIÓN Y MONITOREO DE SERVICIOS PARA LA RED DE DATOS EN LA UGEL HUAMANGA"	
DESIGNACIÓN DEL RESPONSABLE DEL PROYECTO	
Entidad Ejecutora	SOFTTECH S.A.
Cliente:	UGEL HUAMANGA
Elaborado por:	Omar Fernández- Responsable del Proyecto
Revisado por:	Wilfredo Valdivia – Responsable Oficina de Informática
Aprobado por:	Wilfredo Valdivia – Responsable Oficina de Informática

NIVELES DE AUTORIDAD

1. Responsable máximo por realizar todo el trabajo necesario para lograr los objetivos de proyecto.
2. Para la gestión del proyecto sus pares son el personal que labora como soporte en la oficina de informática y sistemas.

1. OBJETIVOS DEL PROYECTO:

a. Implementar un servidor como gestión y monitoreo de dispositivos y servicios, mediante el protocolo SNMP, tecnologías de virtualización, Sistema Operativo CENTOS 7, Nethserver 7, herramientas Open Source como Ntop, Suricata y Zabbix con la finalidad de monitorear el consumo de ancho de banda, análisis de todo el tráfico en el firewall en busca de ataques y anomalías conocidos y verificar el correcto funcionamiento de elementos de hardware y software para la red de datos.

b. El plazo de ejecución del proyecto son de 3 meses calendarios.

c. Cumplir con los requisitos exigidos por el cliente para lograr su satisfacción.

2. FACTORES CRÍTICOS DE ÉXITO DEL PROYECTO:

- Término del análisis de las condiciones físicas 19/11/18

y topológicas de la red de datos.

- Término de definir los dispositivos y servicios de red 03/12/18
- Término de determinar los requerimientos 13/12/18
  y principales problemas de monitoreo de la red existente.
- Término de seleccionar y describir las herramientas. 17/12/18
- Término del diseño e implementación del servidor
  para el control de dispositivos y servicios de la red de datos. 29/01/19
- Término de la evaluación y pruebas ante posibles fallas 13/02/19
  que tenga el servidor y comprobación de su correcto funcionamiento.
- Término del proyecto 13/02/19

3. DESCRIPCIÓN DEL PRODUCTO DEL PROYECTO:

El proyecto de diseño e implementación de un servidor contempla el objetivo de monitorear el consumo de ancho de banda, análisis de todo el tráfico en el firewall en busca de ataques y anomalías conocidos con el uso de herramientas Open Source como son Ntop, Suricata, además los servicios que más usa el CPU, monitorización de los recursos de un host (carga del procesador, uso de los discos, logs del sistema) en varios sistemas operativos como son los que utilizan los servidores, Chequeo de servicios paralizados. reportes y estadísticas del estado cronológico de disponibilidad de servicios y hosts con la herramienta Zabbix.

Como alcance de la ejecución del proyecto se hará el monitoreo de los siguientes equipos:

N°	DISPOSITIVOS Y SERVICIOS	CANTIDAD
1	PCs	115
2	IMPRESORAS	27
3	SERVIDOR SIGA	1
4	SERVIDOR SIAF	1
5	SERVIDOR PLANILLAS	1
6	SERVIDOR CHAT	1
7	SERVIDOR LEGIX	1
8	WEB INSTITUCIONAL	1
	TOTAL:	147

4. UBICACIÓN DEL PROYECTO:

La UGEL Huamanga está organizada en 2 ambientes ubicados en diferentes espacios. La Sede Principal se encuentra ubicada en el Jirón San Martín N° 771, mientras que el Área de

Gestión Pedagógica se encuentra ubicada en el Jirón Mario Ramos N° 125, provincia y departamento de Ayacucho.

5. DE LA PROPUESTA:		
PLAZO DE EJECUCIÓN DEL PROYECTO	**FECHA DE INICIO**	**FECHA DE TÉRMINO**
66 días calendario	12/11/18	13/02/19
MONTO DE LA PROPUESTA	**MODALIDAD DEL CONTRATO**	
S/. 4,000 (Cuatro mil /100 Nuevos Soles)	SUMA ALZADA	

6. RIESGOS DEL PROYECTO:
PRINCIPALES AMENAZAS DEL PROYECTO (Riesgos Negativos)
a. Presentación de documentos a cada jefe de línea para la respectiva autorización de acceso a la información y recursos de la UGEL Huamanga. b. Demora en la respuesta de autorización por cada jefe de línea para el acceso a la información y recursos de la UGEL Huamanga. c. Falta de coordinación e interés por parte del Responsable de la Oficina de Informática y Sistemas. d. No cuenta con un mapa de cableado de red estructurado en la UGEL Huamanga. e. Reporte desactualizado referente al inventariado de dispositivos como Switch, Router, Access Point, etc.
PRINCIPALES OPORTUNIDADES DEL PROYECTO (Riesgos Positivos)
a. Implementar tecnología de calidad con herramientas de software libre. b. Menor grado de riesgo ante vulnerabilidades, plataforma de monitorización del consumo de ancho de banda, análisis de todo el tráfico en el firewall, monitorización de los recursos de un host (carga del procesador, uso de los discos, logs del sistema) dentro de los servidores en la red de datos. c. Obtener experiencia en este tipo de proyectos.

Tabla 3. Acta de Constitución del Proyecto

4.1.5 GESTIÓN DE ALCANCE

Con la Gestión del Alcance se garantiza que el proyecto incluya solamente el trabajo necesario para culminarlo con éxito, es decir define y controla qué se incluye y que no se incluye en el proyecto. En la gestión del alcance se utilizaron tres procesos los cuales son los siguientes:

- Definir el Alcance
- Crear la EDT
- Controlar el Alcance

A. Definir el Alcance

Se detalla el enunciado del alcance del proyecto y del producto, los cuales fueron obtenidos utilizando las técnicas de Entrevista y Análisis de Requerimientos; ambas técnicas fueron trabajadas en la oficina de informática y sistemas y son detallas en el siguiente cuadro.

NOMBRE DEL PROYECTO
"IMPLEMENTACIÓN DE UN SERVIDOR COMO GESTIÓN Y MONITOREO DE SERVICIOS PARA LA RED DE DATOS EN LA UGEL HUAMANGA"
PLAN DE GESTIÓN DEL ALCANCE
PROCESO DE RECOPILACIÓN DE REQUISITOS
Entradas: • Acta de Constitución del proyecto • Registro de interesados **Herramientas y técnicas:** • Entrevista al responsable de la oficina de Informática y Sistemas, los puntos consultados fueron enfocados en los siguientes temas: a. Referente a los servicios y/o funciones que brinda la Oficina de Informática. b. Si existe alguna herramienta de monitoreo que utilicen en la red de datos. c. Los problemas existentes al monitorear la red de datos d. Recursos que van a tener que ser monitoreados e. Ataques o anomalías que pusieron en riesgo la información • Análisis de Requerimientos: Permitió conocer a fondo los detalles de los requerimientos necesarios para el monitoreo y control de dispositivos y servicios de la red de datos **Salidas:** • Realidad actual referente a los problemas que se presenta en la red de datos. • Requerimientos específicos de que dispositivos y servicios se necesitan monitorear.

Tabla 4. Plan de Gestión de Alcance

B. Crear el EDT

En el proceso de creación de la EDT, se va a desarrollar un esquema basado en 7 etapas del proyecto, las cuales detallaremos a continuación:

1.1 Análisis de las condiciones físicas y topológicas de la red de datos

1.2 Definición de los dispositivos y servicios de red

1.3 Determinación de los requerimientos y principales problemas de monitoreo de la red existente

1.4 Selección y descripción de las herramientas

1.5 Diseño del servidor

1.6 Implementación del servidor para el control de dispositivos y servicios de la red de datos

1.7 Pruebas y funcionamiento

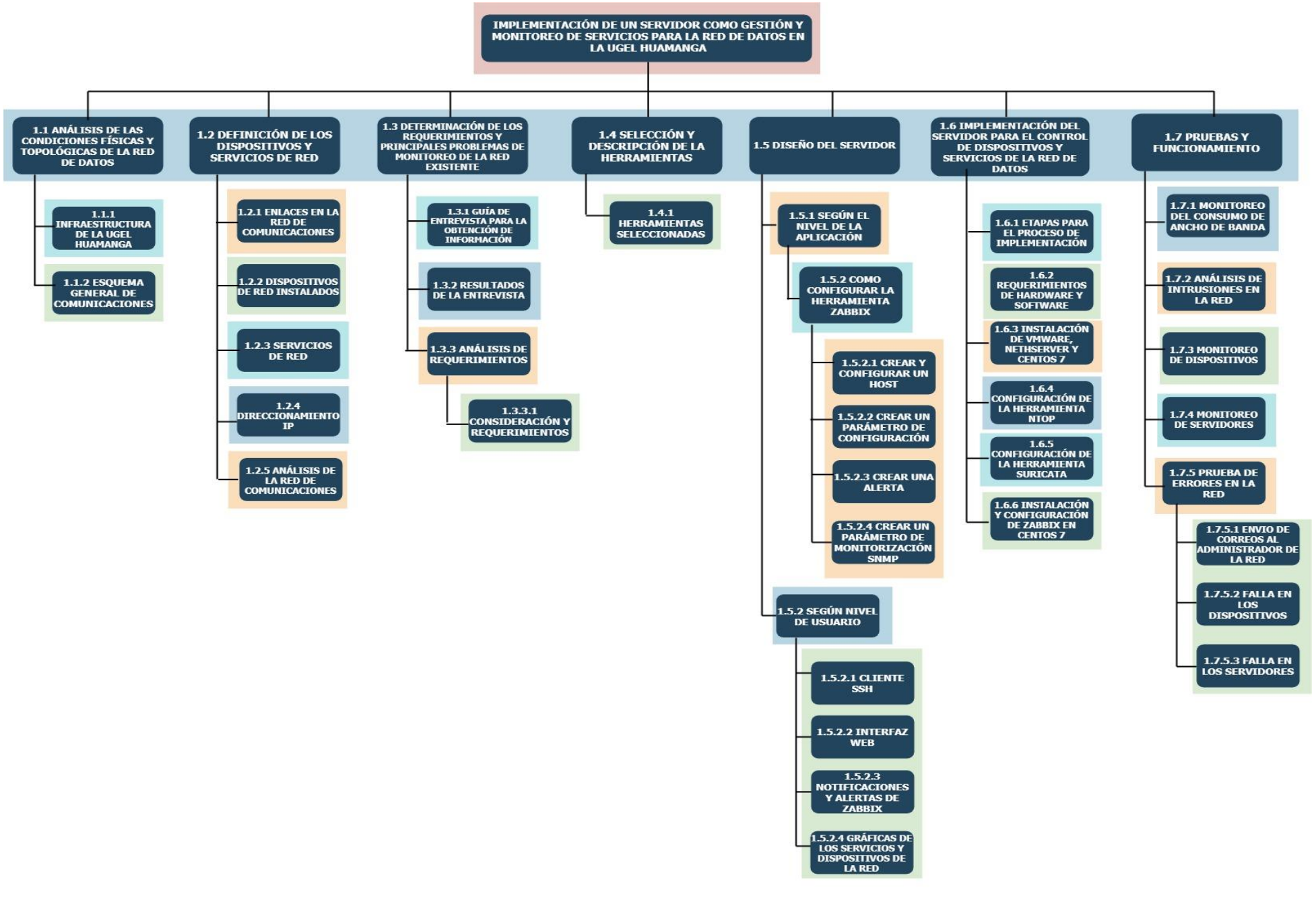

IMPLEMENTACIÓN DE UN SERVIDOR COMO GESTIÓN Y MONITOREO DE SERVICIOS PARA LA RED DE DATOS EN LA UGEL HUAMANGA
1.1 ANÁLISIS DE LAS CONDICIONES FÍSICAS Y TOPOLÓGICAS DE LA RED DE DATOS
1.1.1 INFRAESTRUCTURA DE LA UGEL HUAMANGA
1.1.2 ESQUEMA GENERAL DE COMUNICACIONES
1.2 DEFINICIÓN DE LOS DISPOSITIVOS Y SERVICIOS DE RED
1.2.1 ENLACES EN LA RED DE COMUNICACIONES
1.2.2 DISPOSITIVOS DE RED INSTALADOS
1.2.3 SERVICIOS DE RED
1.2.4 DIRECCIONAMIENTO IP
1.2.5 ANÁLISIS DE LA RED DE COMUNICACIONES
1.3 DETERMINACIÓN DE LOS REQUERIMIENTOS Y PRINCIPALES PROBLEMAS DE MONITOREO DE LA RED EXISTENTE
1.3.1 GUÍA DE ENTREVISTA PARA LA OBTENCIÓN DE INFORMACIÓN
1.3.2 RESULTADOS DE LA ENTREVISTA
1.3.3 ANÁLISIS DE REQUERIMIENTOS
1.3.3.1 CONSIDERACIÓN Y REQUERIMIENTOS
1.4 SELECCIÓN Y DESCRIPCIÓN DE LA HERRAMIENTAS
1.4.1 HERRAMIENTAS SELECCIONADAS
1.5 DISEÑO DEL SERVIDOR
1.5.1 SEGÚN EL NIVEL DE LA APLICACIÓN
1.5.2 COMO CONFIGURAR LA HERRAMIENTA ZABBIX
1.5.2.1 CREAR Y CONFIGURAR UN HOST
1.5.2.2 CREAR UN PARÁMETRO DE CONFIGURACIÓN
1.5.2.3 CREAR UNA ALERTA
1.5.2.4 CREAR UN PARÁMETRO DE MONITORIZACIÓN SNMP
1.5.2 SEGÚN NIVEL DE USUARIO
1.5.2.1 CLIENTE SSH
1.5.2.2 INTERFAZ WEB
1.5.2.3 NOTIFICACIONES Y ALERTAS DE ZABBIX
1.5.2.4 GRÁFICAS DE LOS SERVICIOS Y DISPOSITIVOS DE LA RED
1.6 IMPLEMENTACIÓN DEL SERVIDOR PARA EL CONTROL DE DISPOSITIVOS Y SERVICIOS DE LA RED DE DATOS
1.6.1 ETAPAS PARA EL PROCESO DE IMPLEMENTACIÓN
1.6.2 REQUERIMIENTOS DE HARDWARE Y SOFTWARE
1.6.3 INSTALACIÓN DE VMWARE, NETHSERVER Y CENTOS 7
1.6.4 CONFIGURACIÓN DE LA HERRAMIENTA NTOP
1.6.5 CONFIGURACIÓN DE LA HERRAMIENTA SURICATA
1.6.6 INSTALACIÓN Y CONFIGURACIÓN DE ZABBIX EN CENTOS 7
1.7 PRUEBAS Y FUNCIONAMIENTO
1.7.1 MONITOREO DEL CONSUMO DE ANCHO DE BANDA
1.7.2 ANÁLISIS DE INTRUSIONES EN LA RED
1.7.3 MONITOREO DE DISPOSITIVOS
1.7.4 MONITOREO DE SERVIDORES
1.7.5 PRUEBA DE ERRORES EN LA RED
1.7.5.1 ENVIO DE CORREOS AL ADMINISTRADOR DE LA RED
1.7.5.2 FALLA EN LOS DISPOSITIVOS
1.7.5.3 FALLA EN LOS SERVIDORES

Figura N° 32. Creación del EDT

4.1.6 GESTIÓN DEL TIEMPO

Para la gestión de tiempo, el proyecto está sujeto al cronograma de trabajo. Con el objetivo de cumplirlo de acuerdo a lo planificado y se deben ordenar las actividades y designar los recursos de una manera adecuada.

A. Desarrollar el Cronograma

Es el proceso de análisis de secuencias de actividades, duraciones, las necesidades de recursos y las limitaciones de programación para crear el modelo de cronograma del proyecto. Este cronograma incluye por lo menos, una fecha de inicio planificada y una fecha de finalización para cada actividad del cronograma. La creación del cronograma se realizó usando el software Ms Project, este utiliza el Método de la ruta crítica, calculando las fechas teóricas de inicio y finalización tempranas y tardías, para todas las actividades, sin considerar limitaciones de recursos.

El cronograma de actividades se muestra en el **Anexo D.**

4.1.7 GESTIÓN DE LA CALIDAD

En la gestión de la calidad se elabora el plan de calidad donde se identifica los requisitos y/o estándares para el proyecto y sus entregables, así como documentar cómo el proyecto demuestra el cumplimiento con los requisitos de calidad.

A. Plan de Gestión de la Calidad

El objetivo del plan de gestión de la calidad es describir la metodología general que se establece para realizar correctamente el aseguramiento y el control de la calidad, así como la mejora continua en los procesos del proyecto a desarrollarse para el cliente obteniendo como resultado el cumplimiento de los requerimientos del cliente.

A continuación, se describe las partes que maneja el Plan de Gestión de la Calidad

a) Política de Calidad del Proyecto:

La Política de Calidad del Proyecto cumplirá con los requisitos de calidad desde el punto de vista con que la UGEL Huamanga establezca, es decir culminar el proyecto en el

tiempo y presupuesto planificado, cumpliendo con las normas aplicables y utilizando la tecnología adecuada con el fin de brindar la satisfacción a los requerimientos del cliente.

El Sistema de gestión de la calidad certificado de los estándares ISO 9001 – 2000, está basado en buscar la satisfacción del cliente, el mejoramiento continuo y el registro detallado de los procesos de trabajo.

b) Realizar el Aseguramiento de Calidad:

Para dar la garantía de calidad de resultado se realizarán las pruebas, siendo la primera a cargo del encargado de la Implementación de un servidor como gestión y monitoreo de servicios para la red de datos y posteriormente la segunda revisión a cargo del Administrador de la red en la UGEL Huamanga.

Se describe aquí el plan de pruebas confeccionado con objeto de verificar que el resultado final obtenido al crear el servidor como gestión y monitoreo se adecúa a las necesidades iniciales descritas en la fase de requerimientos.

Según Métrica v3 define una serie de pruebas a desarrollar a distintos niveles:

1. Pruebas unitarias.
2. Pruebas de integración.
3. Pruebas de sistema.
4. Pruebas de implementación.
5. Pruebas de aceptación (usabilidad).

1. Pruebas Unitarias: En las pruebas Unitarias se realizará la verificación de cada componente en la plataforma, es decir que se verificará la funcionalidad y estructura de cada componente individualmente.

IDENTIFICADOR: UGELHGA-MON-PU-001	
Propósitos	Comprobación de la herramienta NTOPNG
Pasos a Ejecutar	Dentro del Sistema Operativo de Nethserver, se comprobará que existe la opción "Uso del ancho de banda", herramienta ntopng que será habilitada y que a su vez se activará las interfaces de red que serán monitoreadas. Así mismo se hará la prueba si la herramienta está activa ingresando al puerto 3000, de esta manera se ejecutará localmente un telnet a dicho puerto.
Salida o estado esperado	Ingresando a la URL http://172.31.200.117:3000 para la red que se maneja mediante un proxy y http://192.168.1.41:3000 en la segunda red libre sin proxy, se muestra la interfaz web, otro medio de ingreso a la URL es seleccionando la opción aplicaciones e ingresando a la herramienta NTOPNG respecto al monitoreo del tráfico de red en tiempo real con sus respectivas gráficas y análisis estadísticos. En caso contrario se muestra un mensaje de error de conexión o que la herramienta no está habilitada.

Tabla 5. Comprobación de la herramienta NTOPNG

IDENTIFICADOR: UGELHGA-MON-PU-001	
Propósitos	Comprobación de la herramienta SURICATA
Pasos a Ejecutar	Dentro del Sistema Operativo de Nethserver, se comprobará que existe la opción "Sistema de prevención de intrusos", herramienta SURICATA que será habilitada y que a su vez se seleccionará las categorías de reglas para el análisis de intrusiones y el tráfico que se genera en la red. Así mismo se hará la prueba si la herramienta está activa ingresando al puerto 980 y seguidamente a la aplicación EVEBOX herramienta de alerta y gestión de eventos generados por Suricata.
Salida o estado esperado	Ingresando a la aplicación EVEBOX se muestra la interfaz web con las alertas y anomalías que la herramienta va identificando e indicando la fecha, el usuario, el tipo de categoría, la dirección

	IP y la descripción de la categoría. Si existen problemas de conexión la plataforma mostrará un mensaje de que el servicio está inhabilitado

Tabla 6. Comprobación de la herramienta Suricata

IDENTIFICADOR: UGELHGA-MON-PU-001	
Propósitos	Comprobación de los agentes Zabbix
Pasos a Ejecutar	Dentro del Sistema Operativo de Windows, se comprobará que existe un servicio para el agente Zabbix y que el servicio este ejecutándose. Así mismo se ingresará la dirección IP del servidor de Zabbix http://172.31.200.64/zabbix para la red que se maneja mediante un proxy y http://192.168.1.67/zabbix en la segunda red libre sin proxy, el cuál hará la prueba si los agentes aceptan conexiones en el puerto 10050, se ejecutará localmente un telnet a dicho puerto.
Salida o estado esperado	En la lista de servicios del Sistema Operativo de Windows aparecerá un servicio por nombre “Zabbix Agent” y con estado “En ejecución”. La ejecución del telnet no mostrará ningún mensaje de error.

Tabla 7. Comprobación de los agentes Zabbix

IDENTIFICADOR: UGELHGA-MON-PU-002	
Propósitos	Comprobación de los agentes SNMP
Pasos a Ejecutar	Para realizar la comprobación de funcionamiento de los agentes SNMP en los dispositivos, se realizará la configuración del protocolo en las versiones SNMPv1 y SNMPv2, de esta manera en la plataforma web se ejecutará un telnet al puerto 161 para cada uno de los dispositivos habilitados.
Salida o estado esperado	En la relación de los Host en la plataforma web de Zabbix se observa si está activo el protocolo SNMP en el puerto 161. La ejecución del telnet no mostrará ningún mensaje de error.

Tabla 8. Comprobación de los agentes SNMP

IDENTIFICADOR: UGELHGA-MON-PU-003	
Propósitos	Comprobación de la plataforma web de Zabbix
Pasos a Ejecutar	El servidor de Zabbix tiene las conexiones con el puerto 10050 y en el puerto 10051. Se ejecutará un telnet a ambos puertos.
Salida o estado esperado	La ejecución del telnet no mostrará ningún mensaje de error.

Tabla 9. Comprobación del servidor Zabbix

IDENTIFICADOR: UGELHGA-MON-PU-004	
Propósitos	Comprobación del servidor Apache
Pasos a Ejecutar	El administrador de la red abrirá un navegador web y en la barra de direcciones se digitará la dirección IP con el cuál está registrado el servidor Zabbix es decir http://172.31.200.64/ para la red que se maneja mediante un proxy y http://192.168.1.67 en la segunda red libre sin proxy.
Salida o estado esperado	Se mostrará en el navegador un mensaje indicando que el servidor Apache está activo y funcionando correctamente.

Tabla 10. Comprobación del servidor Apache

IDENTIFICADOR: UGELHGA-MON-PU-005	
Propósitos	Comprobación del funcionamiento de MariaDB
Pasos a Ejecutar	Después de verificar que el servidor Apache está funcionando correctamente, se tendrá el acceso a la interfaz web de Zabbix en la plataforma web.
Salida o estado esperado	Si se presenta un fallo se mostrará los errores de conexión a la base de datos MariaDB. Por otra parte la interfaz web no mostrará ningún problema.

Tabla 11. Comprobación del funcionamiento de MariaDB

2. Pruebas de Integración: Para las pruebas de integración se realiza las verificaciones que están asociadas a grupos de componente. Es decir que el objetivo de las pruebas de integración es el de verificar el correcto ensamblaje entre los distintos componentes.

Las pruebas de integración se clasifican como pruebas de comunicación entre los distintos componentes de la plataforma web.

3. Pruebas de Comunicación: Se realizará las pruebas de comunicación que existe entre el servidor central de Zabbix y los demás componentes de la plataforma: monitorización de los dispositivos, de los servidores y servicios.

IDENTIFICADOR: UGELHGA-MON-PC-001	
Propósitos	Comunicación entre la herramienta NTOPNG y los Hosts
Pasos a Ejecutar	La comunicación que se realiza entre la herramienta NTOPNG y los hosts conectados a la red de la UGEL Huamanga es a través de las interfaces de red. Es decir si la red local está habilitada en la red "ens33" dicha herramienta se encarga analizar e identificar los protocolos más utilizados, el tráfico que existe en la red, además evalúa el ancho de banda utilizado por los hosts utilizando gráficas y estadísticas.
Salida o estado esperado	De no existir ningún problema, se observa el resultado en la URL http://172.31.200.117 para la red que se maneja mediante un proxy y http://192.168.1.41 en la segunda red libre sin proxy, el análisis de los hosts en la red con la herramienta NTOPNG

Tabla 12. Comunicación entre la herramienta NTOPNG y los hosts

IDENTIFICADOR: UGELHGA-MON-PC-002	
Propósitos	Comunicación entre la herramienta SURICATA y los Hosts
Pasos a Ejecutar	La comunicación que se realiza entre la herramienta Suricata y los Hosts conectados a la red de la UGEL Huamanga es a través de que categorías de reglas el administrador de la red habilita para el análisis de intrusiones. Por ejemplo, se tiene las opciones de habilitar, alertar, bloquear la categoría TOR que son normas basadas en IP para la identificación del tráfico hacia y desde los nodos de salida. De esta manera se comprobará que la

	herramienta Suricata muestra todo el análisis e identifica las anomalías y sucesos en la red.
Salida o estado esperado	De no existir ningún problema, se observa en la aplicación EVEBOX el registro de todas las incidencias y anomalías que ocurren en la red.

Tabla 13. Comunicación entre la herramienta SURICATA y los hosts

IDENTIFICADOR: UGELHGA-MON-PC-003	
Propósitos	Comunicación entre el servidor Zabbix con los dispositivos y servicios
Pasos a Ejecutar	La comunicación que se realiza entre el servidor Zabbix con los dispositivos y servicios conectados a la red de la UGEL Huamanga es a través del agente Zabbix instalado. De esta manera se comprobará que los agentes aceptan peticiones del servidor central en el puerto 10050, tal como se define en los ficheros de configuración.
Salida o estado esperado	De no existir ningún problema, se observa en la plataforma web de Zabbix el registro y la monitorización de los dispositivos y servicios conectados a la red

Tabla 14. Comunicación entre el servidor Zabbix con los dispositivos y servicios

IDENTIFICADOR: UGELHGA-MON-PC-004	
Propósitos	Comunicación entre la plataforma Zabbix y los equipos conectados vía SNMP
Pasos a Ejecutar	Para realizar la comunicación utilizando el protocolo en las versiones SNMPv1 y SNMPv2 en los dispositivos, el puerto utilizado por defecto para que ese agente SNMP escuche peticiones del servidor Zabbix es el 161. Se realizará la verificación comprobando que dicho puerto esté habilitado.
Salida o estado esperado	Al realizarse la comunicación utilizando el protocolo en las versiones SNMPv1 y SNMPv2 se observa en la plataforma Zabbix estos equipos están marcados como “Enabled” con un icono indicativo de color verde correspondiente a SNMP.

Tabla 15. Comunicación entre la plataforma Zabbix y los equipos conectados vía SNMP

4. **Pruebas de Aceptación:** Las pruebas de aceptación están dirigidas a validar que la plataforma web cumpla con los requisitos de funcionamiento esperado, de tal manera que se pueda conseguir la aceptación final por parte del usuario.

5. **Pruebas Funcionales:** Las pruebas funcionales se realiza para probar que la plataforma cumpla con las funcionalidades específicas en los requisitos.

Es decir, se ejecutan las pruebas para comprobar si la plataforma cubre los requisitos especificados en la fase de requerimientos. Aquí se detallará las pruebas definidas para comprobar si se satisfacen los requisitos de funcionamientos más importantes.

IDENTIFICADOR: UGELHGA-MON-PF-001	
Propósitos	Comprobación de la monitorización de las interfaces de red con NTOPNG
Pasos a Ejecutar	Se habilitará las interfaces de red para que la herramienta realice la monitorización. Luego en Sistema Operativo de Nethserver se ingresará en la opción de aplicaciones a la herramienta NTOPNG.
Salida o estado esperado	En la plataforma web se visualizará el tráfico que realiza en cada Host, así como las estadísticas respecto al rendimiento y consumo de ancho de banda.

Tabla 16. Comprobación de la monitorización de las interfaces de red con NTOPNG

IDENTIFICADOR: UGELHGA-MON-PF-002	
Propósitos	Comprobación del análisis de la red con el Sistema de Prevención de Intrusos (IPS) Suricata
Pasos a Ejecutar	Se habilitará en la opción Sistema de Prevención de Intrusos las categorías de reglas en el Sistema Operativo de Nethserver, inmediatamente se ingresará a la Aplicación EVEBOX que es la herramienta de gestión de eventos y alertas para eventos

	generados por el motor de detección de amenazas de la red Suricata.
Salida o estado esperado	En la plataforma web de la aplicación se visualizará la fecha y la hora, la fuente y el destino donde se generó, la descripción de las categorías de reglas que han sido habilitadas, bloqueadas o simplemente archivadas.

Tabla 17. Comprobación del análisis de la red con el Sistema de Prevención de Intrusos (IPS) Suricata

IDENTIFICADOR: UGELHGA-MON-PF-003	
Propósitos	Comprobación de la inserción de parámetros de monitorización
Pasos a Ejecutar	Se creará un ítem en Zabbix dentro de una plantilla y se vinculará con un equipo ya ingresado en la plataforma.
Salida o estado esperado	El parámetro o ítem que ha sido creado tomará valores para el equipo al cual se ha asignado.

Tabla 18. Comprobación de la inserción de parámetros de monitorización

IDENTIFICADOR: UGELHGA-MON-PF-004	
Propósitos	Comprobación de la inserción de dispositivos y servicios
Pasos a Ejecutar	Se insertará un dispositivo en la plataforma a través del frontend de Zabbix.
Salida o estado esperado	Dentro del frontend se mostrará el dispositivo y servicios que van a ser monitoreados y se conectarán a la base de datos MySQL para que se ejecute la consulta con la que se compruebe que el dispositivo ha sido correctamente creado e insertado.

Tabla 19. Comprobación de la inserción de dispositivos y servicios

IDENTIFICADOR: UGELHGA-MON-PF-005	
Propósitos	Comprobación de alertas de notificación al correo electrónico
Pasos a Ejecutar	Para realizar la comprobación de alertas se utilizarán los triggers que se hayan creado, como ejemplo problemas de conexión en los dispositivos y servicios. Este Trigger tiene asociada la acción

	de envió a un correo electrónico para notificar al administrador de la red de la UGEL Huamanga. De esta manera se ampliará el trigger a un valor superior al porcentaje de espacio libre en el disco en el momento actual para así inducir a su activación y a la ejecución de la acción que envía el correo electrónico.
Salida o estado esperado	El administrador de la plataforma web recibirá un mensaje en su bandeja de correo electrónico informando de lo ocurrido.

Tabla 20. Comprobación de alertas de notificación al correo electrónico

IDENTIFICADOR: UGELHGA-MON-PF-006	
Propósitos	Comprobación de la interacción de la plataforma web con el usuario
Pasos a Ejecutar	Se mostrará las operaciones a través de la interfaz web que el usuario podrá observar las interrupciones que se presentan en la red de datos.
Salida o estado esperado	La interfaz tiene una presentación “amigable” desde el punto de vista de usabilidad sin plantear dificultades de navegación.

Tabla 22. Comprobación de la interacción de la plataforma web con el usuario

4.1.8 GESTIÓN DE LOS RIESGOS

La Gestión de Riesgos, se realiza al definir e identificar los riesgos que tienen probabilidad de impactar positiva o negativamente en el proyecto, así como planificar las respuestas a los riesgos identificados con mayor probabilidad de ocurrencia, durante el ciclo de vida del proyecto. Se utilizaron los siguientes procesos para definir e identificar los riesgos:

- Identificación de los Riesgos
- Realizar el análisis cualitativo y cuantitativo de riesgos
- Planificar la respuesta a los riesgos

A. Identificar los Riesgos

Se utilizaron las siguientes herramientas que a su vez son las entradas para identificar los riesgos:

Banco de preguntas para realizar la entrevista y solicitud para la disposición de uso de equipos y dispositivos al encargado de la oficina de informática y sistemas de la UGEL Huamanga.

Revisiones a la documentación, se realizó una revisión estructurada de la documentación del proyecto, incluyendo el organigrama de la UGEL Huamanga para observar la estructura que lo conforma, políticas de seguridad, Sistema de Control Interno, etc.

Se muestra las salidas de este para identificar los riesgos, en el siguiente cuadro.

N°	Identificación de los Riesgos
R1	La oficina de Informática y Sistemas no mantiene el orden y la distribución de los Host según el organigrama que se maneja.
R2	La UGEL Huamanga según las políticas de seguridad no cuenta con un diagrama de red referente a la estructura de red.
R3	Incomodidad por parte de los usuarios al momento de ingresar a sus equipos para la instalación y configuración del agente Zabbix.
R4	Demora en la habilitación de permisos y puertos al Protocolo de Internet versión 4 (IPv4) que den acceso a internet y a sitios web bloqueados por el proxy.

Tabla 32. Identificación de los Riesgos

B. Realizar el análisis cualitativo y cuantitativo de riesgos

Como principales entradas de este proceso fueron las siguientes:

- Registro de Riesgo
- Enunciado del alcance del proyecto
- Plan de Gestión de Riesgos, Cronograma

Se muestra las salidas de este proceso, en el siguiente cuadro:

N°	RIESGOS	Categoría de Riesgo	Probabilidad	Plazo	Impacto de Plazo	Alcance de Gestión	Impacto en Alcance de Gestión	Calidad	Impacto en Calidad	Importancia
R1	La oficina de Informática y Sistemas no mantiene el orden y la distribución de los Host según el organigrama que se maneja.	**Interno**	**0.4**	**4**	**0.60**	**8**	**0.10**	**58%**	**0.50**	**0.95**
R2	La UGEL Huamanga según las políticas de seguridad no cuenta con un diagrama de red referente a la estructura de red.	**Técnico**	**0.3**	**3**	**0.40**	**4**	**0.10**	**70%**	**0.70**	**1.20**
R3	Incomodidad por parte de los usuarios al momento de ingresar a sus equipos para la instalación y configuración del agente Zabbix.	**Externo**	**0.2**	**3**	**0.50**	**10**	**0.10**	**45%**	**0.50**	**0.90**
R4	Demora en la habilitación de permisos y puertos al Protocolo de Internet versión 4 (IPv4) que den acceso a internet y a sitios web bloqueados por el proxy.	**Interno**	**0.5**	**7**	**0.80**	**6**	**0.10**	**80%**	**0.80**	**1.50**

Tabla 234. Cuadro de Riesgos

C. Planificar la respuesta a los riesgos

Riesgo R2:	La UGEL Huamanga según las políticas de seguridad no cuenta con un diagrama de red referente a la estructura de red.					
N°	**Estrategia**	**Causa**	**Responsable**	**Fecha de Implementación**	**Periodo**	**Descripción**
01	Mitigar	La no continuidad del personal encargado de la oficina de informática y sistemas hasta la fecha no han cumplido con la elaboración de un diagrama de red que muestre como está elaborado la estructura y distribución según áreas y oficinas.	Responsable de la Oficina de Informática y Sistemas	A inicios de la primera fase de Análisis de las condiciones físicas y topológicas de la red de datos.	Una sola vez	Como primer compromiso y encargado es organizar y estructurar la red mediante un mapa o diagrama en un software respectivo.

Tabla 24. Planificar la respuesta a los riesgos (Riesgo R2)

Riesgo R4:	Demora en la habilitación de permisos y puertos al Protocolo de Internet versión 4 (IPv4) que den acceso a internet y a sitios web bloqueados por el proxy.					
N°	**Estrategia**	**Causa**	**Responsable**	**Fecha de Implementación**	**Periodo**	**Descripción**
01	Mitigar	Con una previa solicitud para la habilitación de puertos y acceso se tuvo una demora en la respuesta de parte del responsable de la oficina de informática y sistemas	Responsable de la Oficina de Informática y Sistemas	A inicios de la primera fase de Análisis de las condiciones físicas y topológicas de la red de datos.	Una sola vez	El encargado debe de tener conocimiento de la importancia que tiene la implementación de un servidor de monitorización y de los beneficios que traerá para la red de datos en la UGEL Huamanga.

Tabla 25. Planificar la respuesta a los riesgos (Riesgo R4)

4.1.9 GESTIÓN DE LOS INTERESADOS

Los interesados en el proyecto serán las personas que contribuyeron en el proyecto. Los interesados ocupan cargos en diferentes niveles dentro de la organización y poseen diferentes cargos dentro de la Institución, para el proyecto solo se presentó a una persona involucrada externamente a la organización.

Nombres y Apellidos	Organización	Cargo	Información de Contacto	Requisitos /Expectativas	Influencia sobre
WILFREDO VALDIVIA SÁNCHEZ	UGEL HUAMANGA	JEFE DE LA OFICINA DE INFORMÁTICA Y SISTEMAS	wilvalsito @gmail.com	Permisos de acceso a los servidores y encargado de realizar las pruebas de aceptación	Sistemas y Base de Datos
RAÚL MENDOZA TORRES	SOFTECH	DESARROLLADOR DE LA EMPRESA	raulinmichi@gmail.com	Adquisición del Sistema Operativo CentOS 7 en formato ISO	Programación y Desarrollo Web
ERNESTO MARTINEZ MEDINA	UGEL HUAMANGA	PRÁCTICANTE EN LA OFICINA DE INFORMÁTICA	warmachine_54@hotmail.com	Apoyo en el registro de dispositivos y estructurado de la red	Redes y Computadoras

Tabla 26. Cuadro de Distribución de Interesados

CAPÍTULO V
CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

a) Se realizó la implementación de un servidor como gestión y monitoreo de dispositivos y servicios, aplicando la Guía de Fundamentos para la Dirección de Proyectos (PMBOK) se logró como uno de los resultados el análisis del consumo de ancho de banda utilizado por IPS o hosts individuales, por puertos y a su vez se identificó los protocolos de red más utilizados en tiempo real respecto al tráfico de la red.

b) Como otro resultado se logró la detección y bloqueo de anomalías, infiltrados en la red; el sistema realizó la tarea de bloquear, alertar y guardar los eventos en un registro detallado referente al Host o emisor, protocolo, fecha y la descripción de las categorías uniformes; así mismo se registró el estado actual como son la capacidad, el rendimiento y la disponibilidad de los servicios, Servidores, y hardware, de los cuales al presentarse problemas de conectividad la plataforma realizó notificaciones mediante el envío de alertas vía e-mail (correo electrónico).

c) Se logró la implementación de una estación de gestión gráfica (NMS) vía web, el cual permitió mejorar el concepto del uso de las herramientas OpenSource proporcionando varias opciones para visualizar los datos recogidos, desde listas de problemas y gráficos simples hasta mapas de red, de esta manera toda la configuración es transparente y de fácil manejo para el usuario.

d) Se logró establecer la configuración de los dispositivos con el protocolo SNMP en las versiones V1 y V2 permitiendo que las herramientas OpenSource puedan llevar a cabo una mejor gestión de monitoreo hacia esos dispositivos en la red.

e) Trabajar con Zabbix como herramienta de software libre permitió cubrir las necesidades y requerimientos de red, así también otras herramientas complementarias como son Ntopng y Suricata permitieron abaratar costos de implementación del servidor como gestión y monitoreo de dispositivos y servicios.

5.2 RECOMENDACIONES

a) Para realizar la implementación del servidor en futuras organizaciones que cuenten con un centro de datos y utilicen un proxy y firewall es necesario habilitar las Direcciones IPs y los puertos que maneja cada herramienta de monitorización, para así tener acceso a todos los recursos que maneja la red.

b) La implementación del servidor y uso de las herramientas serán útiles en cualquier organización que cuente con una red de datos, ya sea con una pequeña o grande Infraestructura de TI y a su vez es importante estar siempre con las actualizaciones suficientes y necesarias para atender requerimientos internos y externos,

c) Para una futura mejora respecto al envió de notificaciones se debería de realizar la configuración respectiva para enviar dichas notificaciones a través de mensajes cortos SMS mediante el operador de telefonía móvil que se maneje, aprovechando el soporte que Zabbix ofrece a este mecanismo de alertas.

REFERENCIAS BIBLIOGRÁFICAS

Abricot. (26 de Abril de 2017). *Abricot Innovando Ideas Tecnológicas*. Obtenido de http://www.abricot.com.mx/docsES/gestion-de-fallas.html

Álvarez, G., & Pérez, P. (2004). *Seguridad Informática para empresas y Particulares.* Madrid: McGraw-Hill.

Arias Figueroa, D. (1999). *Herramientas de Gestión basada en Web.* Universidad Nacional de la Plata, La Plata.

Arias Figueroa, D. (1999). *Herramientas de Gestión basada en Web.* Universidad Nacional de la Plata, La Plata.

Baca, G. (2016). *Introducción a la Seguridad Informática.* México D.F: Grupo Editorial Patria.

Becerra Orrala, E. (2016). *Implementación de monitoreo de red utilizando los Protocolos ICMP y SNMP.* Universidad Estatal Peninsula de Santa Elena, La Libertad.

Bonilla, F., Iván, J., & Lozada, M. A. (2013). *Herramienta Opensource De Administración Y Monitoreo Basado En Snmp Para El Mejoramiento Del Funcionamiento De La Red En Speedy.com Cia Ltda.* Universidad Técnica de Ambato, Ambato.

Botero Arana, N. (2005). *Modelo de gestión de seguridad con soporte a SNMP.* Pontificia Universidad Javeriana, Bogotá.

Carrasco, M. (12 de Octubre de 2014). *Tecnología & Informática*. Obtenido de https://tecnologia-informatica.com/tipos-de-redes-informaticas-lan-wan-man-wlan-wman-wwman-san-pan/

Dordoigne, J. (2015). *Redes Informáticas, Nociones Fundamentales.* Montevideo: Eni Ediciones.

Echenique, J. (2001). *Auditoria en Informática.* México: McGraw-Hill.

Estrada, J. (2015). *Análisis de los estándares internacionales más utilizados en la gestión de proyectos.* Buenos Aires: UP.

Ford, M., & Lew, K. (1998). *Tecnologías de Interconectividad de Redes.* España: Paperback.

Forouzan, B. (2002). *Transmisión de Datos y redes de Comunicaciones.* Madrid: McGraw-Hill.

Gómez, Á. (2014). *Enciclopedia de la Seguridad Informática.* México D.F: ALFAOMEGA.

Grupo del Banco Mundial. (2015). Productividad a través de la tecnología en Infraestructura de redes. pág. 15.

Hernández, R., Fernández, C., & Baptista. (1991). *Metodología de la Investigación.* México: McGraw-Hill Interamericana de México.

Hucaby, D. (2002). *Cisco Field Manual:Catalyst Switch Configuration.* New York: Cisco Press.

Ibañez, P., & García, G. (2009). *Informatica I.* Mexido D.F.: Cengagen Learning Editores.

Izquierdo, F. (2005). *dministración de riesgos de tecnología de información de una empresa del sector informático.* Guayaquil: Escuela Superior politécnica del Litoral.

Jardinez, R. T., & Ruiz, D. S. (2012). *Propuesta de un Sistema de Monitoreo para la Red de ESIME ZACATENCO utilizando el Protocolo SNMP y Software Libre.* Insituto Politécnico Nacional, México D.F.

Kenneth, L., & Jane, L. (2012). *Sistemas de Información Gerencial.* México: Pearson Educación.

Laporta, J. (2006). *Monitoreo de Red, Fundamentos de Telemática.* España: España U.P.V.

López, A. (2004). *Tecnologías de la Información Conceptos Básicos.* Barcelona: NerBiblo S.L.

Lopez, R. (13 de Julio de 2017). *CIC Consulting Informático*. Obtenido de https://www.cic.es/que-es-un-nms-network-management-system/

Magnini, B., & Cavaglia, G. (2000). *Integrating subjects field codes into Wordnet.* Trento: Pant´e di Povo.

Mauro, D. (09 de Febrero de 2008). *Essential SNMP*. Obtenido de http://www.intranetwerx.com/bookshelf2/networking_2ndEd/snmp/ch02_06.htm

Morris, S. (2003). *Network Management, MIBs and MPLS: Principles, Desing and Implementation.* New Jersey: Pearson Education.

Murillo, W. (29 de Noviembre de 2015). *La Investigación Científica*. Obtenido de La Investigación Científica: http://www.monografias.com/trabajosl5/investcientifica/

Project Managament Institute. (2013). *Guía de Fundamentos para la Dirección de Proyectos (PMBOK).* Pensilvania: National Information Standards Organization.

RFC's 1244, s., & 2196, R. (2002). *Políticas de Seguridad.* New York.

Rose, M., & McCloghrie, K. (1991). *Concise MIB Definitions.* New Jersey: RFC 1212.

Saldarriaga, G. G., & Huila, J. C. (2015). *Implementación de un Sistema de Gestión y Administración de Redes Basados en el Protocolo Simple de Monitoreo de Redes SNMP en la Red ESPOL-FIEC.* Escuela Superior Politecnica del Litoral, Guayaquil.

Sanchez, J. (2015). *Arquitecturas de Gestión de Red.* Madrid: McGraw-Hill.

Santos, M. (2014). *Diseño de Redes Telemáticas.* Madrid: RA-MA, S.A.

Sanz, E. (2006). Monitorización y Gestión de Dispositivos. *tecnimap sevilla*, 7.

Saydam, T., & Magedanz, T. (1996). *Redes, Gestión de Redes y Servicio de Administración, entorno de redes y gestión de sistemas.* New York: Guest Editorial.

Stallings, W. (2004). *Comunicaciones y Redes de Computadores.* Madrid: PEARSON EDUCACIÓN S.A.

Stallings, W. (2004). *Fundamentos de Seguridad en Redes Aplicaciones y Estándares.* Madrid: PEARSON EDUCACIÓN S.A.

Supo, J. (2015). *Las Variables Analísticas.* Lima: McGraw-Hill.

Tamayo, A. (2003). *Auditoria de Sistemas una visión práctica.* Bogotá: Universidad de Colombia.

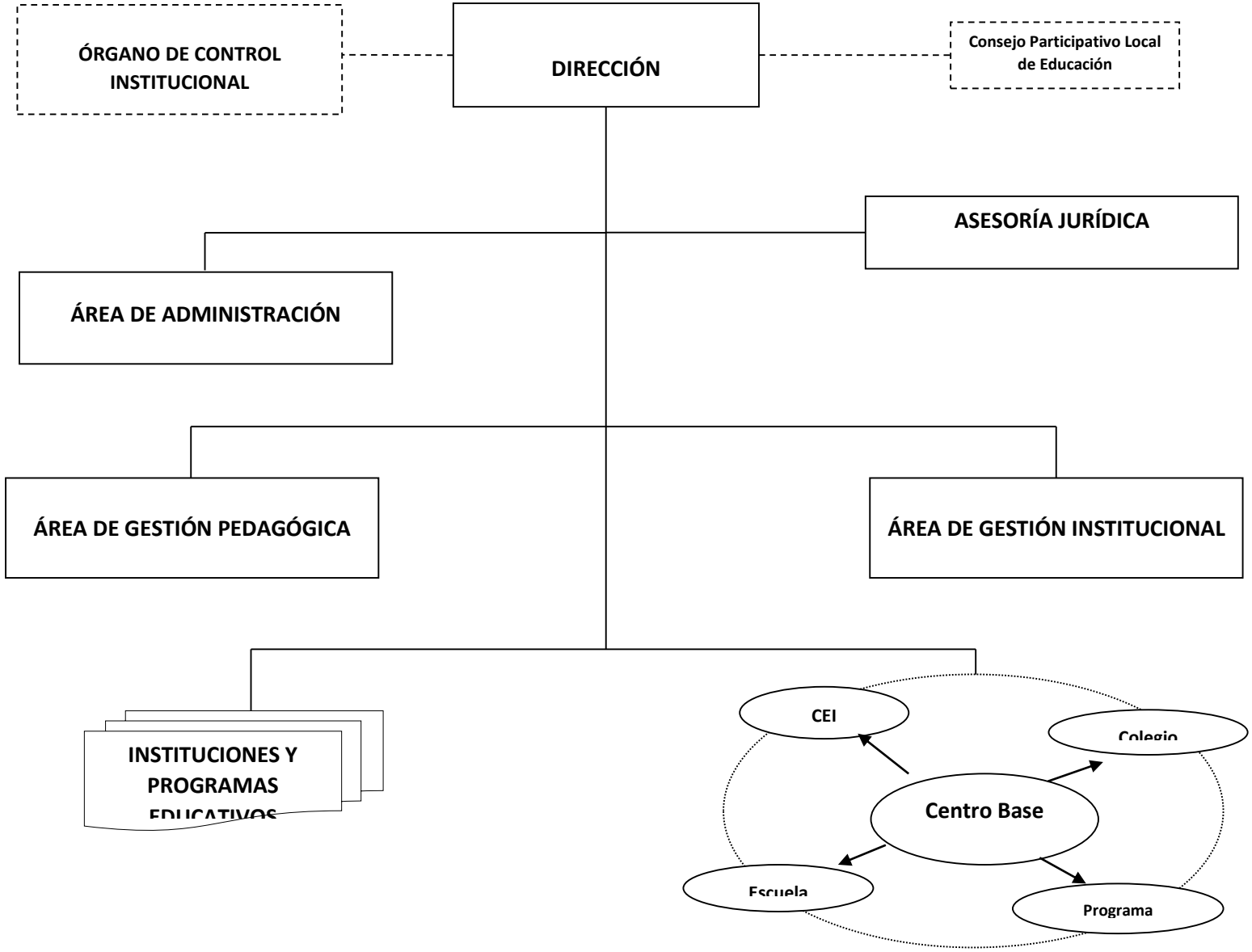
Tanenbaum, A., & Wetherall, D. (2012). *Redes de Computadoras.* México D.F.: Pearson Educación.

Vargas, E. (15 de Noviembre de 2018). *Risk It*. Obtenido de http://cuevabardalesriskti.weebly.com/gestioacuten.html

Verón, R. (2010). *Prácticas de Redes.* Sao Paulo: Ed. Brazil D.R.

ANEXO A

ORGANIGRAMA DE LA UGEL HUAMANGA



ANEXO B
GUIA DE ENTREVISTA

ENTREVISTA REALIZADA AL RESPONSABLE DE LA OFICINA DE INFORMATICA Y SISTEMAS DE LA UNIDAD DE GESTIÓN EDUCATIVA LOCAL HUAMANGA 2018

Nombre del Entrevistado:

Cargo:

1. ¿Cuáles son los principales servicios que la Oficina de Informática de la UGEL Huamanga brinda?

……
……
……

2. ¿Existe algún Software o una de base de datos que contenga información jerárquica de monitoreo de los dispositivos y servicios en la red de datos de la UGEL Huamanga?

……
……
……

3. ¿Cómo administrador de la red, cree usted que para el monitoreo, que una aplicación pueda administrar los componentes independientes de software y hardware que se tiene en la red de datos de la UGEL Huamanga?

……
……
…….

4. ¿Cuáles son las tareas que realiza para determinar el buen funcionamiento de la red de comunicación de datos?

……
……
……

5. ¿Alguna vez usted ha instalado y configurado alguna distribución o herramientas del

sistema Operativo GNU/Linux?

……
……
……

6. ¿Cómo administrador de la red, la estructura diseñada cumple con la definición de las topologías de red?

……
……
……

7. ¿Cuáles son los dispositivos o hosts que facilitan el intercambio de información de administración en la red de datos de la UGEL Huamanga?

……
……
……

8. ¿Qué tipo de problemas se presentan al monitorear los dispositivos que utilizan la capa de aplicación del protocolo SNMP en routers, switches de la red de datos?

……
……
……

9. ¿Qué recursos (hosts) requieren ser monitorizados en la UGEL Huamanga?

……
……
……

10. ¿Cuáles son las características de hardware que se deben monitorizar para un óptimo funcionamiento?

……
……
……

11. ¿De los servidores, que se tiene, que servicios se requieren monitorizar, de los cuales se tienen mayor prioridad?

……
……
……

12. ¿En alguna situación la red de datos de la UGEL de Huamanga ha sufrido de ataques o anomalías que pusieron en riesgo la información en la red WLAN?

……
……
……

13. ¿Qué características debería contar el Servidor de Gestión y Monitoreo utilizando software libre en la red de datos de la UGEL Huamanga? (Escoja las que usted crea necesarias).

- ☐ De fácil manejo.
- ☐ Alerta de falla de red.
- ☐ Datos en tiempo real.
- ☐ Conexión remota.
- ☐ Información de equipos.
- ☐ Detección de Intrusos
- ☐ Análisis de tráfico de Red
- ☐ Consumo de ancho de banda
- ☐ Requisitos mínimos.

14. ¿Cree usted que el Servidor de Gestión y Monitoreo debería utilizar aplicaciones de software libre y una base de datos distribuida que registra información en cada uno de los nodos administrados en la red con datos de todos los objetos?

……
……
……

15. ¿Después de esta entrevista, le interesaría tener implementado un servidor con software libre para la gestión y monitoreo?

……

ANEXO C

MATRIZ DE OPERACIONALIZACIÓN DE VARIABLES

VARIABLES	INDICADORES	DIMENSIONES	ITEMS	INSTRUMENTO
GESTIÓN Y MONITOREO	Base de información	Base de Datos	¿Existe algún Software o una de base de datos que contenga información jerárquica de monitoreo de los dispositivos y servicios en la red de datos de la UGEL Huamanga?	Guía de entrevista
		Registro de Información	¿Cree usted que el Servidor de Gestión y Monitoreo debería utilizar aplicaciones de software libre y una base de datos distribuida donde podrá registrar información en cada uno de los nodos administrados en la red con datos de todos los objetos?	Guía de entrevista
	Protocolo SNMP	Intercambio de Información	¿Cuáles son los dispositivos o hosts que facilitan el intercambio de información de administración en la red de datos de la UGEL Huamanga?	Guía de entrevista

RED DE DATOS		**Capa de Aplicación**	**¿Qué tipo de problemas se presentan al monitorear los dispositivos que utilizan la capa de aplicación del protocolo SNMP en routers, switches de la red de datos?**	**Guía de entrevista**
	Estación de Gestión(NMS)	**Aplicación**	**¿Cómo administrador de la red, cree usted que para el monitoreo, que una aplicación pueda administrar los componentes independientes de software y hardware que se tiene en la red de datos de la UGEL Huamanga?**	**Guía de entrevista**
		Interfaz Web	**¿Cree usted que tendrá más seguridad realizar la monitorización de la red en una interfaz web?**	**Guía de entrevista**
	Red LAN	**Topologías de Red**	**¿Cómo administrador de la red, la estructura diseñada cumple con la definición de las topologías de red?**	**Guía de entrevista**
		Comunicación de datos	**¿Cuáles son las tareas que realiza para determinar el buen funcionamiento de la red de comunicación de datos?**	**Guía de entrevista**
	Red WLAN	**Riesgo de la Información**	**¿Alguna vez la red de datos de la UGEL de Huamanga ha sufrido de ataques o anomalías que pusieron en riesgo la información en la red WLAN?**	**Guía de entrevista**

Tabla 27. Matriz de Operacionalización de variables

ANEXO E

RESULTADOS DE LA IMPLEMENTACIÓN DE UN SERVIDOR COMO GESTIÓN Y MONITOREO DE SERVICIOS PARA LA RED DE DATOS EN LA UGEL HUAMANGA

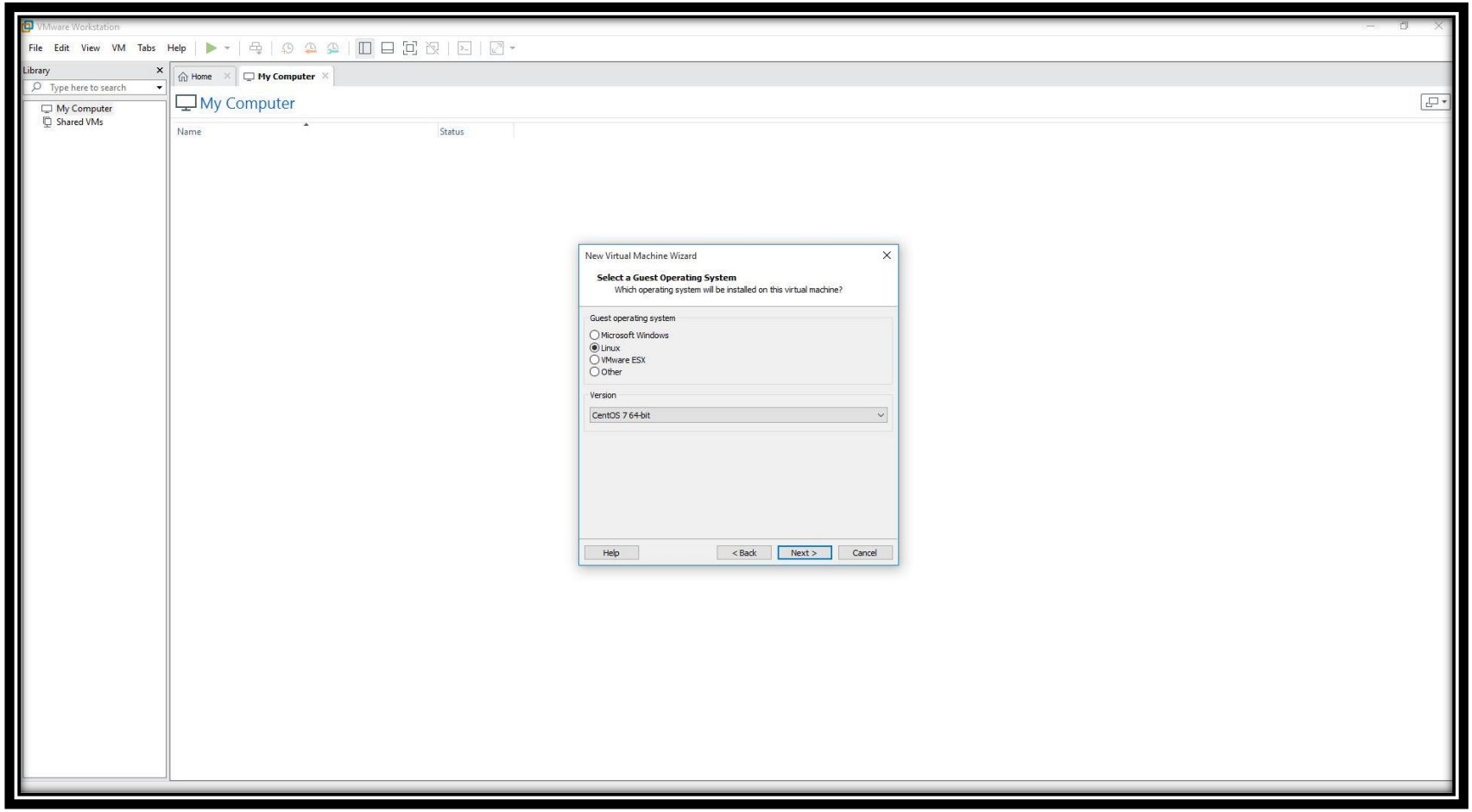


Figura N° 34. Creación de una Máquina Virtual Sistema Operativo NETHSERVER

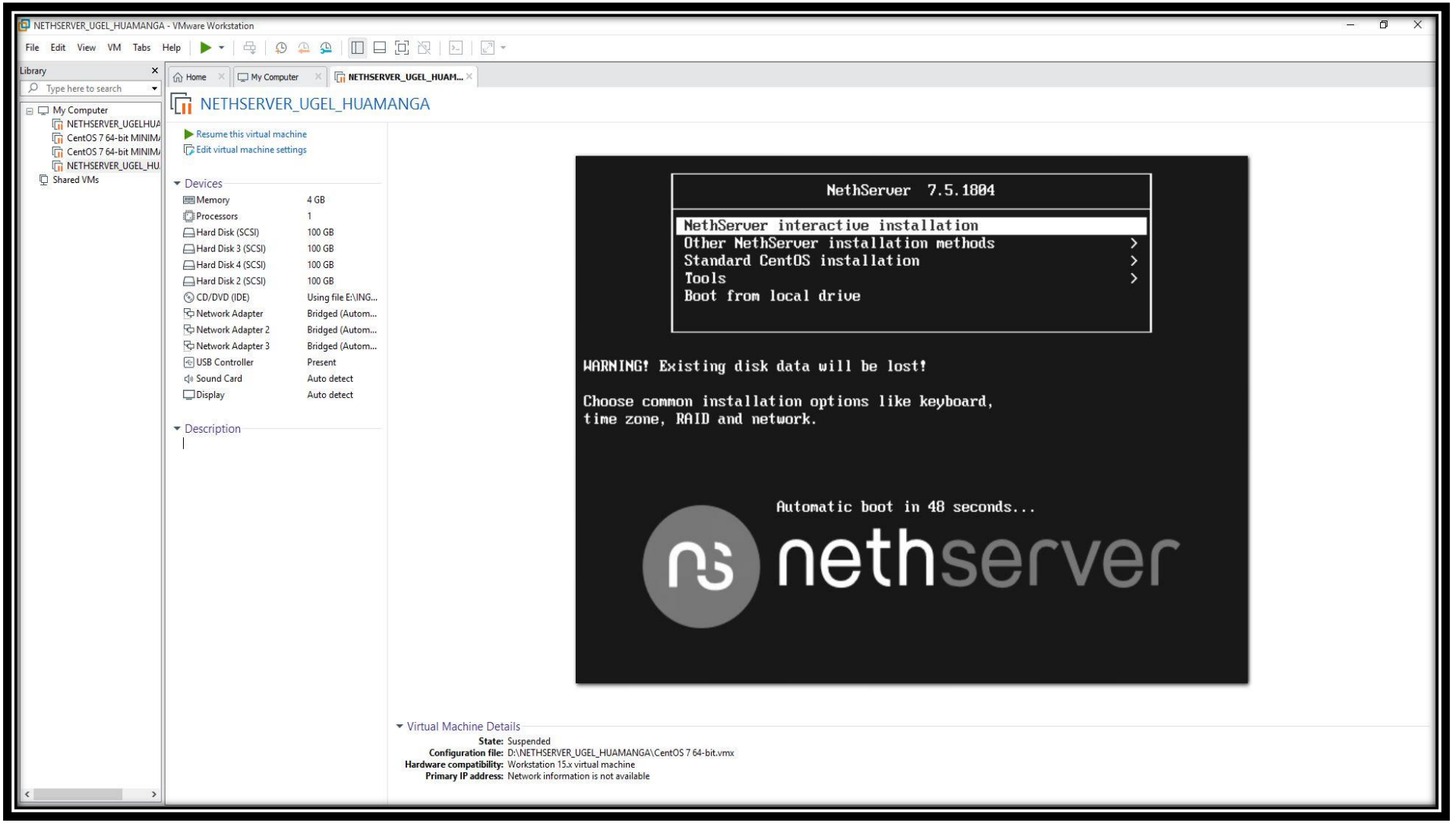


Figura N° 35. Iniciando Máquina Virtual Sistema Operativo NETHSERVER

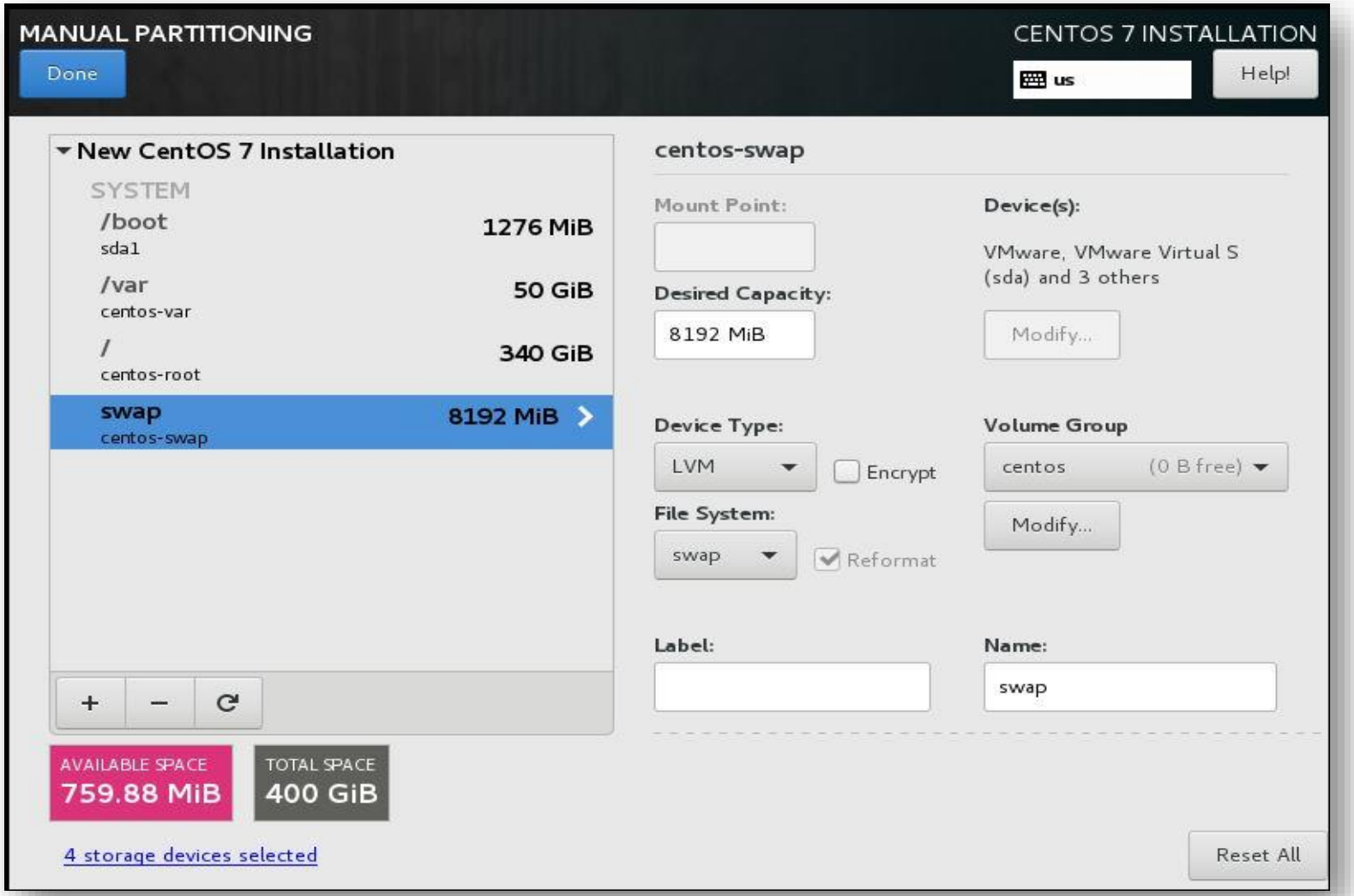


Figura N° 36. Partición de las unidades de disco en NETHSERVER

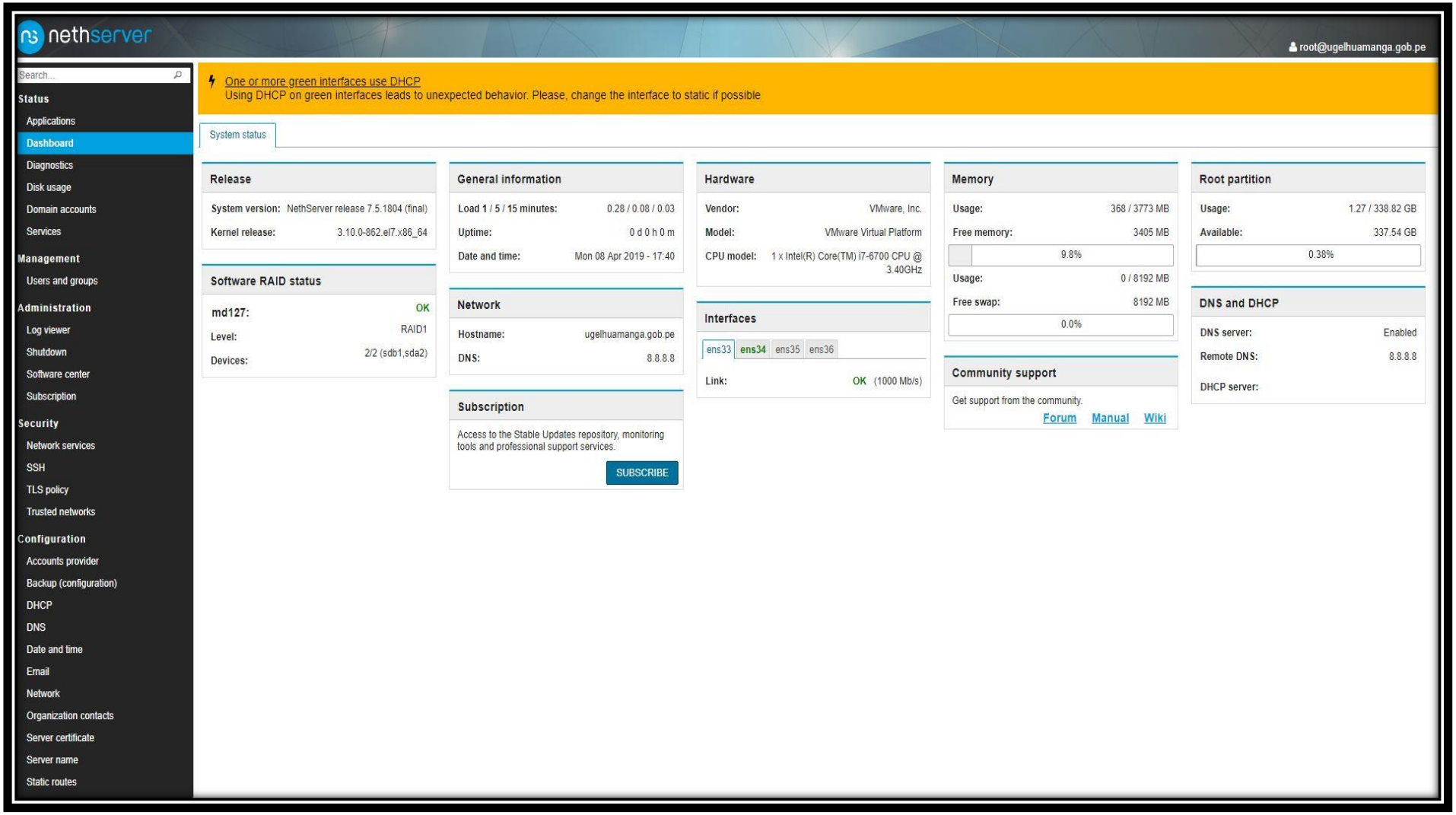


Figura N° 37. Dashboard (Panel de Control) del Sistema Operativo NETHSERVER

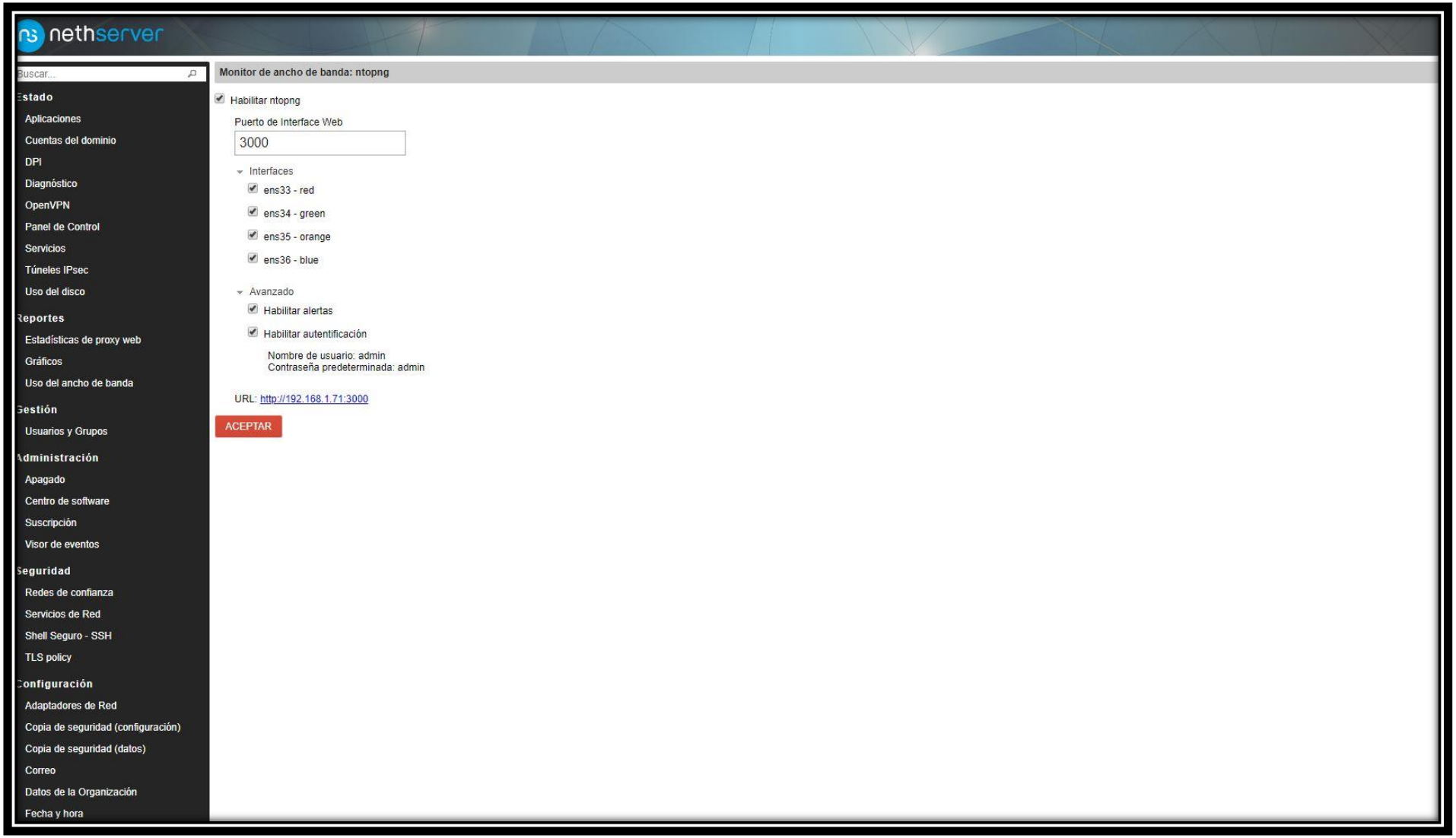


Figura N° 38. Habilitando NTOPNG (Monitor de Ancho de Banda) en el Sistema Operativo NETHSERVER

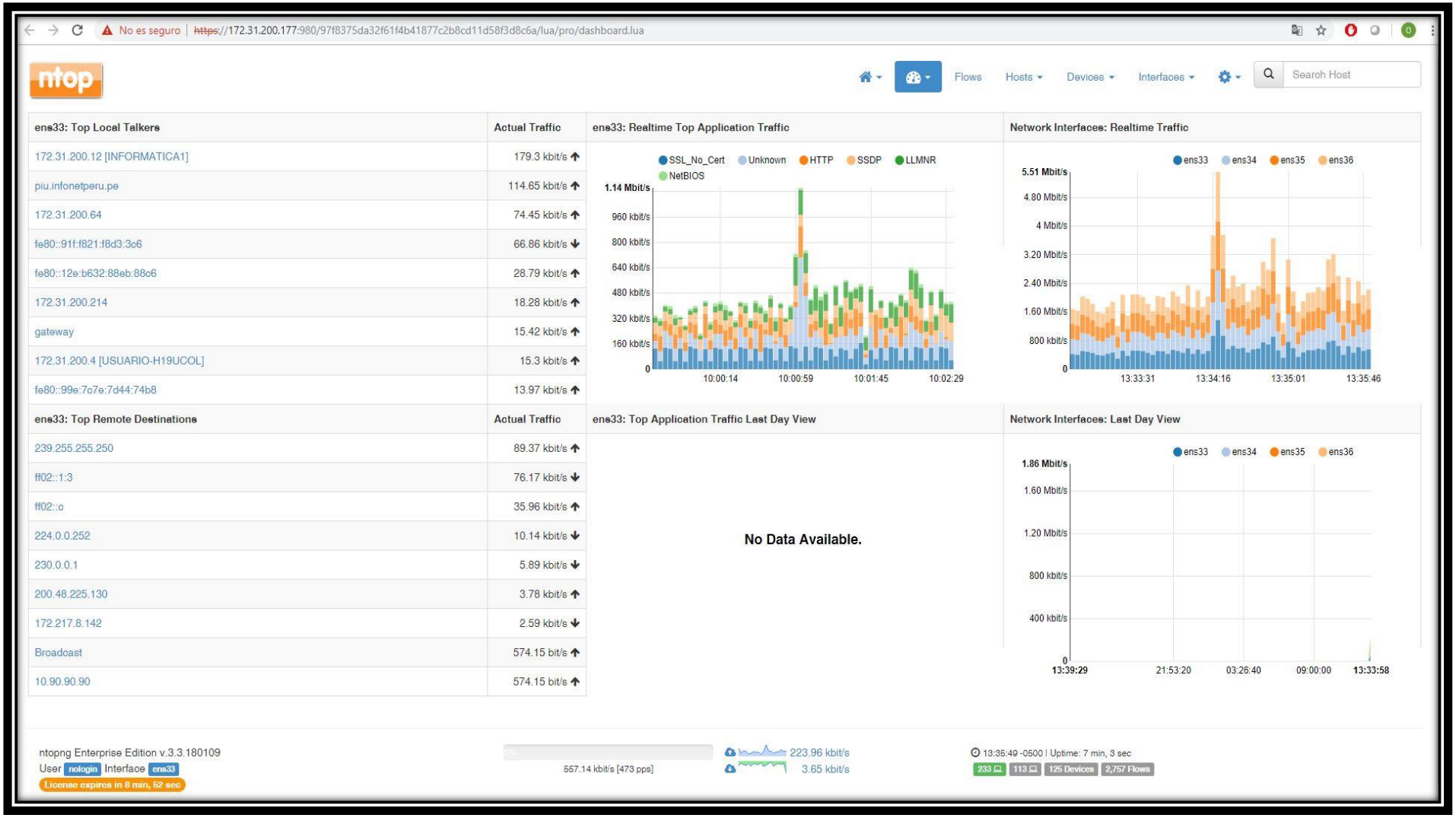


Figura N° 39. Interfaz web de la herramienta NTOPNG

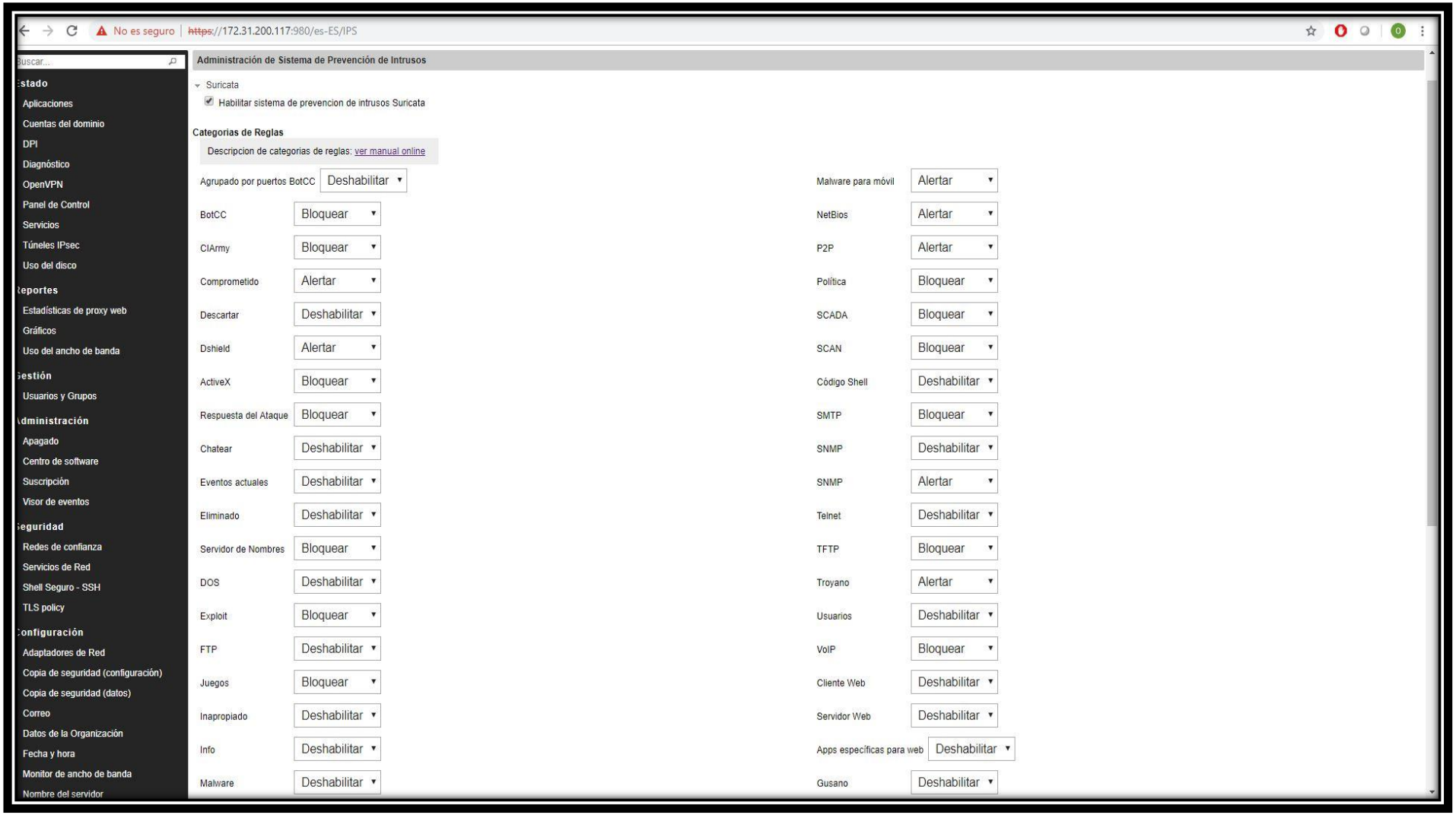


Figura N° 40. Habilitar Sistema de Prevención de Intrusos Suricata

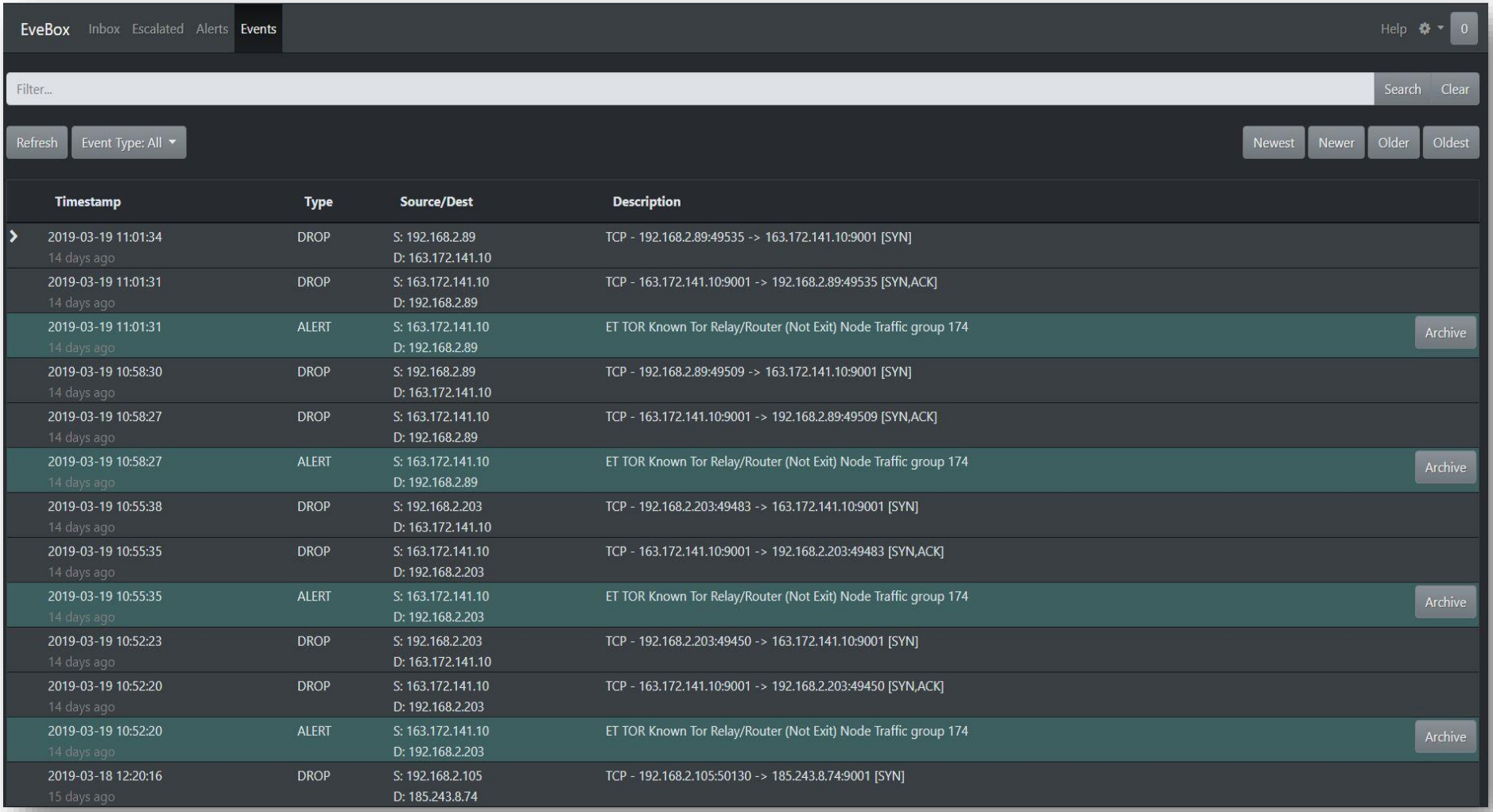


Figura N° 41. Interfaz de la Plataforma web EVEBOX herramienta de análisis de intrusos SURICATA

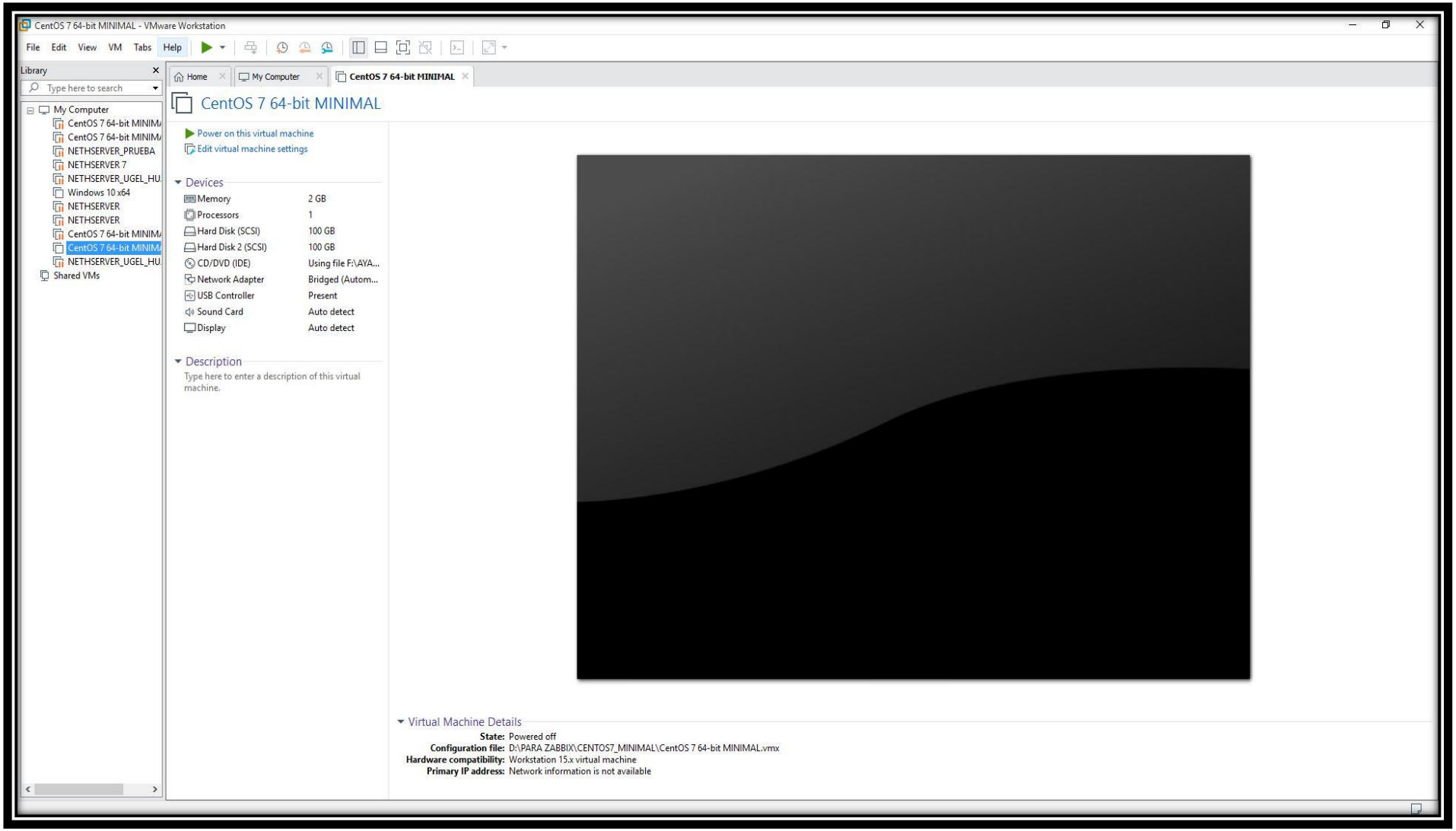


Figura N° 42. Creación de la máquina virtual del Sistema Operativo CentOS 7

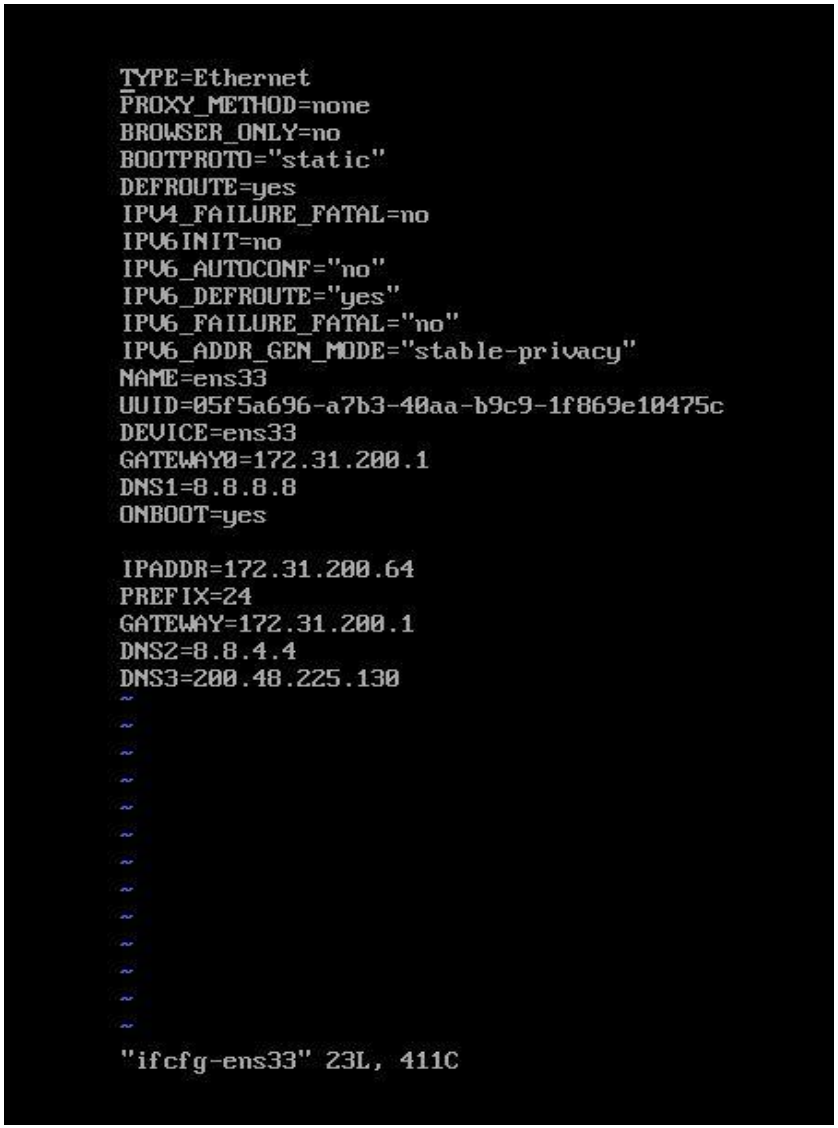


Figura N° 43. Configuración de la tarjeta de red en CentOS 7

```
[root@localhost ~]# hostnamectl
   Static hostname: ugelhga.ugelhuamanga.pe
   Pretty hostname: UGELHGA.ugelhuamanga.pe
         Icon name: computer-vm
           Chassis: vm
        Machine ID: 1faecbbf26264e1d95e3b8f38ec08e7e
           Boot ID: 08f2b477a847467ab91008aedfb3d36f
    Virtualization: vmware
  Operating System: CentOS Linux 7 (Core)
       CPE OS Name: cpe:/o:centos:centos:7
            Kernel: Linux 3.10.0-957.1.3.el7.x86_64
      Architecture: x86-64
```

Figura N° 44. Configuración del Hostname en CentOS

```
[root@localhost ~]# rpm --import http://repo.zabbix.com/RPM-GPG-KEY-ZABBIX
[root@localhost ~]# rpm -ivh https://repo.zabbix.com/zabbix/4.0/rhel/7/x86_64/zabbix-release-4.0-1.el7.noarch.rpm
Recuperando https://repo.zabbix.com/zabbix/4.0/rhel/7/x86_64/zabbix-release-4.0-1.el7.noarch.rpm
advertencia:/var/tmp/rpm-tmp.8ZHqdc: EncabezadoV4 RSA/SHA512 Signature, ID de clave a14fe591: NOKEY
Preparando...                          ################################# [100%]
Actualizando / instalando...
   1:zabbix-release-4.0-1.el7          ################################# [100%]
```

Figura N° 45. Instalación de la herramienta Zabbix

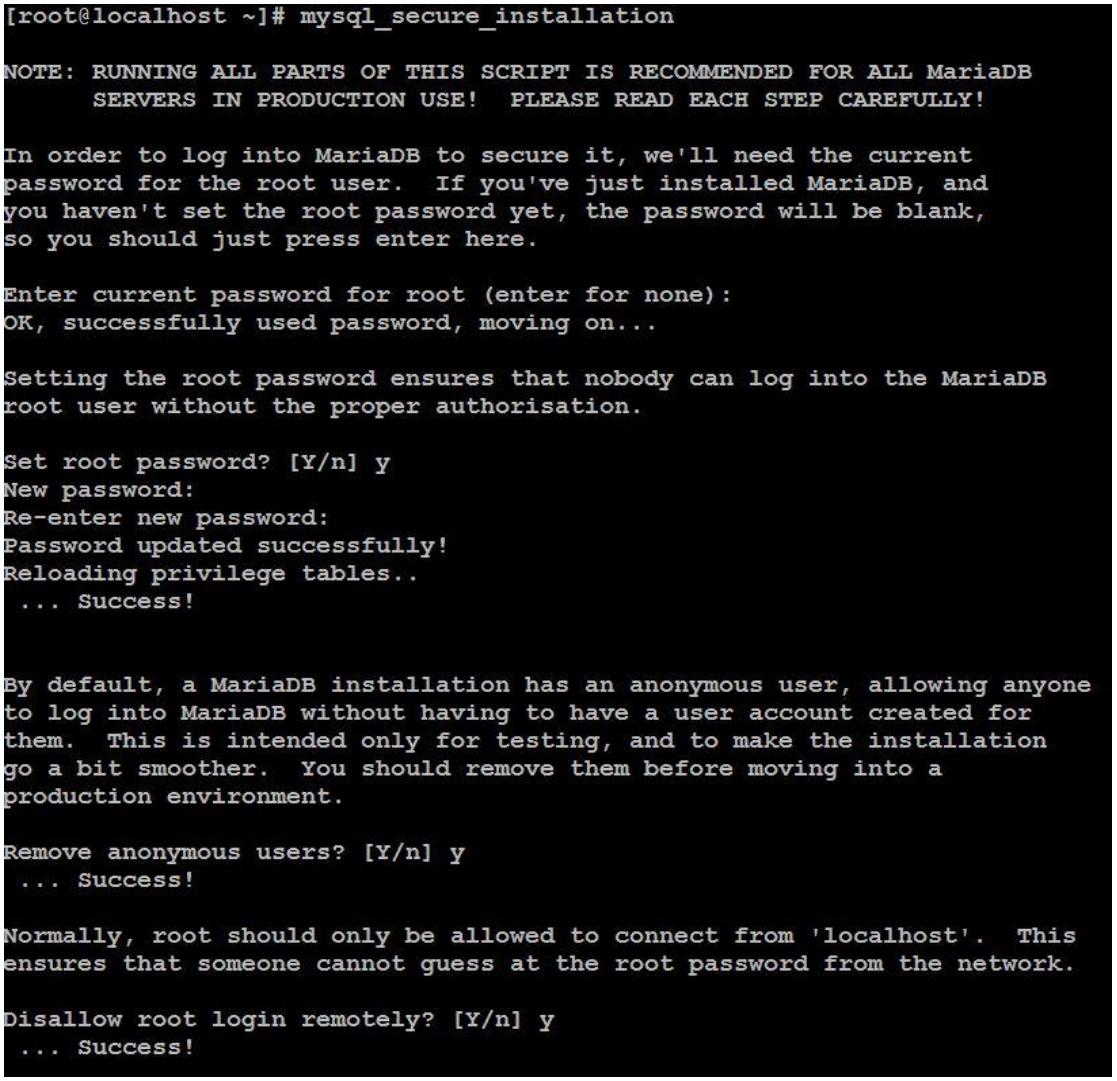


Figura N° 46. Script de creación de usuario y contraseña en MariaDB

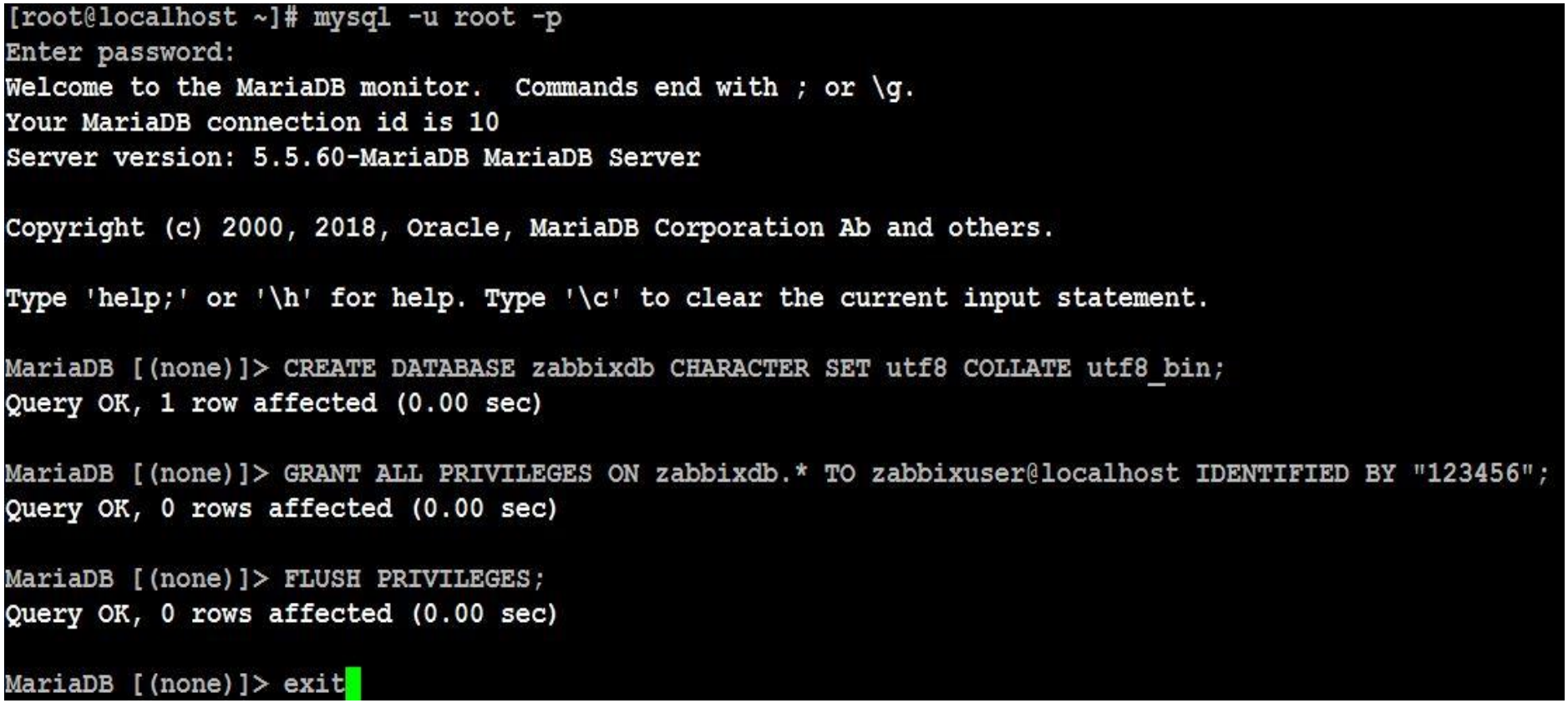


Figura N° 47. Creación de la Base de Datos y dar Privilegios en MariaDB

```
Alias /zabbix /usr/share/zabbix

<Directory "/usr/share/zabbix">
    Options FollowSymLinks
    AllowOverride None
    Require all granted

    <IfModule mod_php5.c>
        php_value max_execution_time 300
        php_value memory_limit 128M
        php_value post_max_size 16M
        php_value upload_max_filesize 2M
        php_value max_input_time 300
        php_value max_input_vars 10000
        php_value always_populate_raw_post_data -1
        php_value date.timezone America/Lima
    </IfModule>
</Directory>
```

Figura N° 48. Edición del archivo .conf en Zabbix en Apache

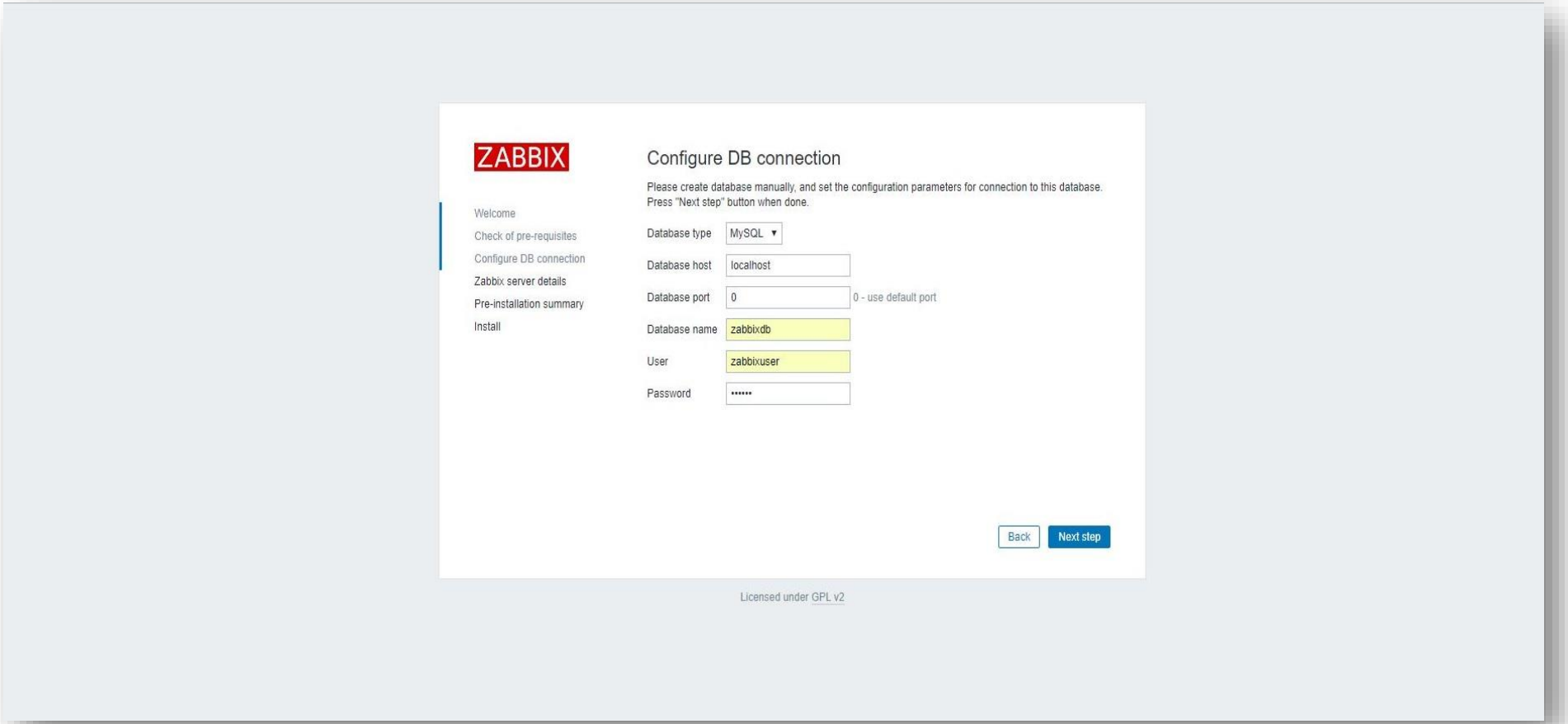


Figura N° 49. Configuración de la Base de datos en la Plataforma web de Zabbix

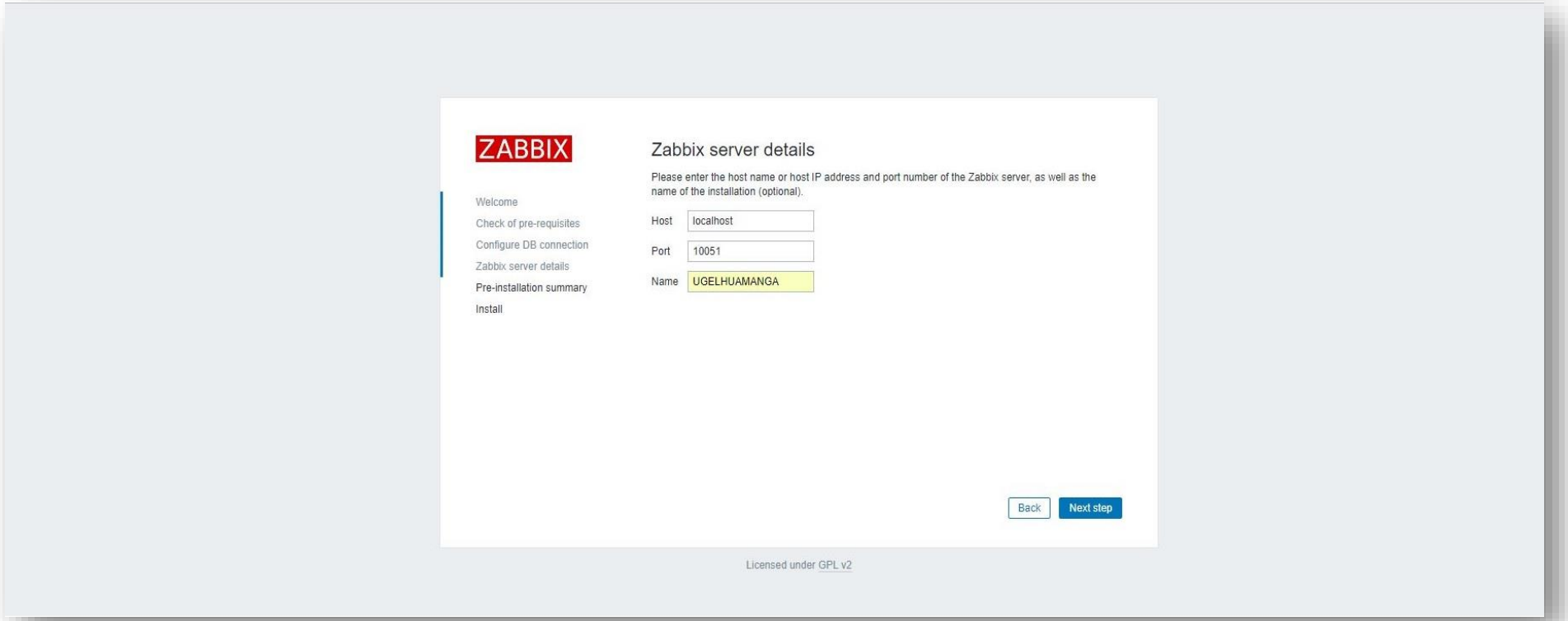


Figura N° 50. Configuración del nombre del host y numero de puerto

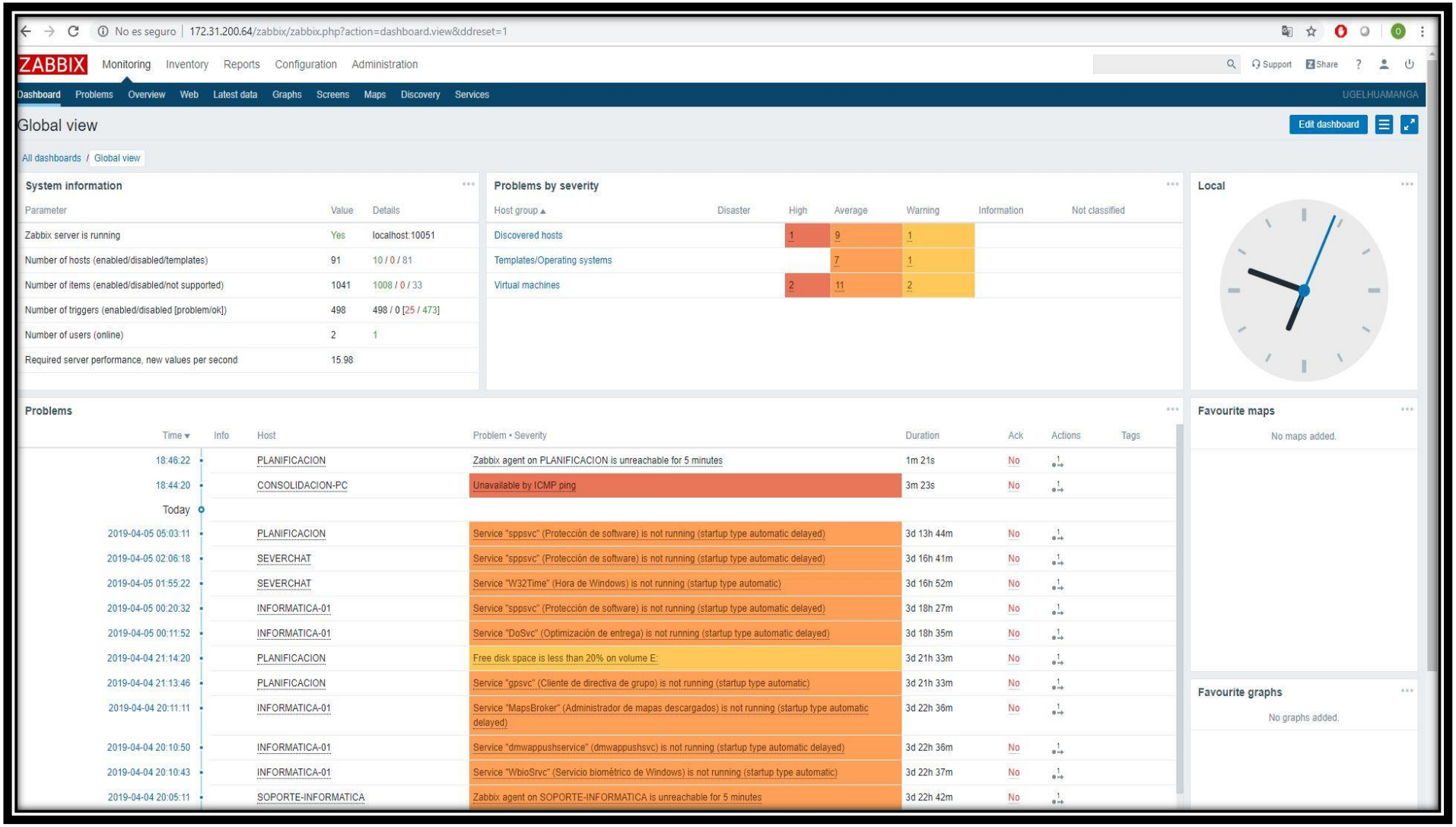


Figura N° 51. Dashboard (Panel de Control) de la Plataforma web de Zabbix

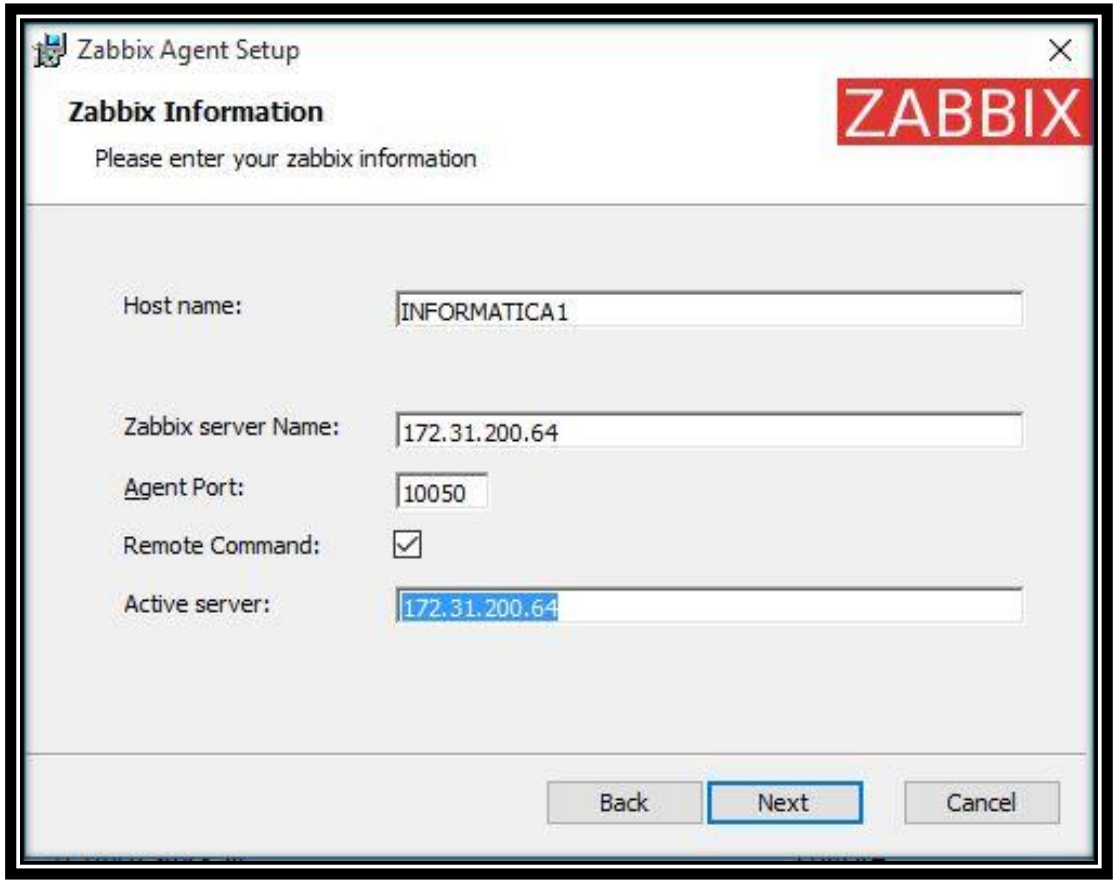


Figura N° 52. Configuración del Agente Zabbix en Windows

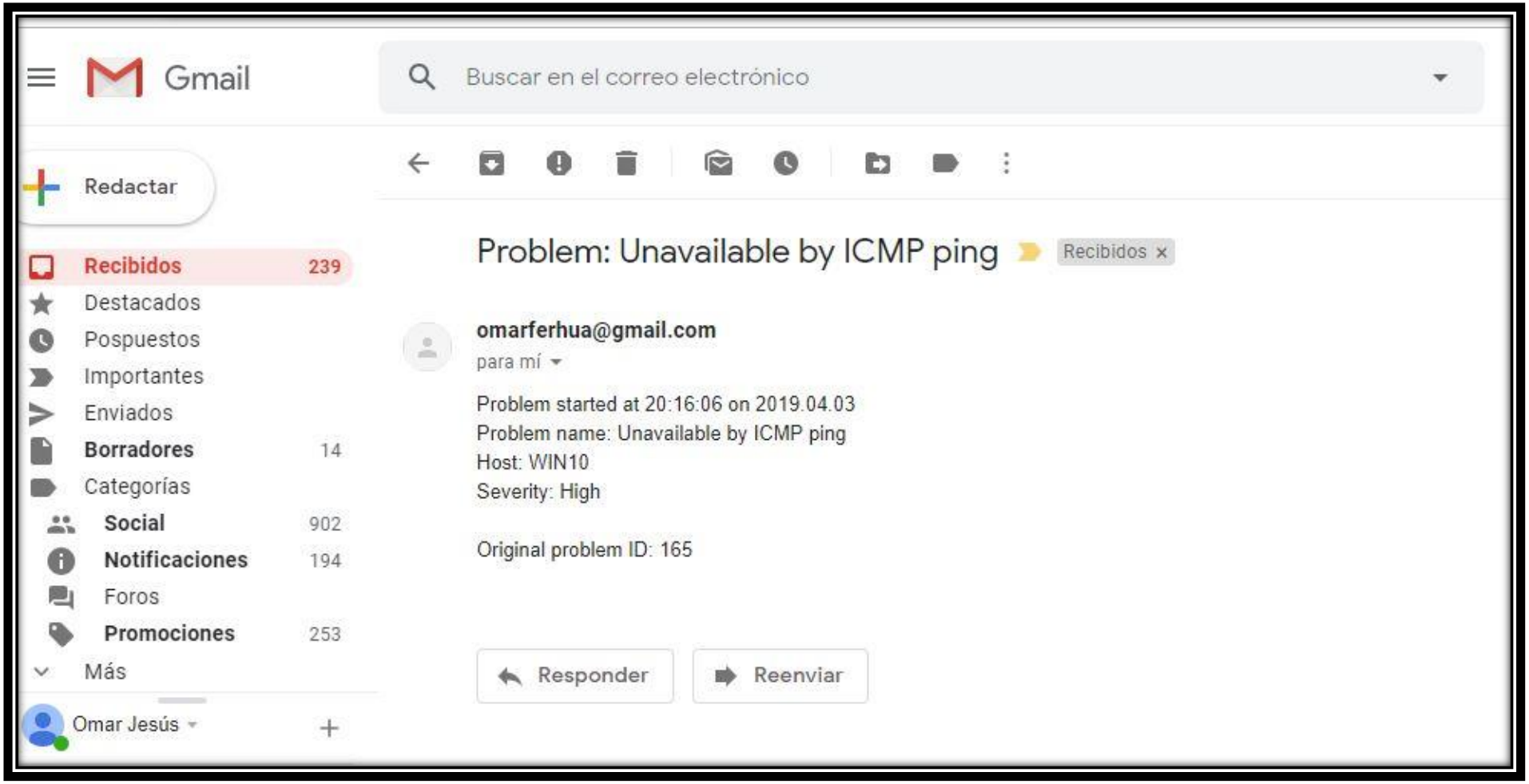


Figura N° 53. Envío de alertas y notificaciones al correo electrónico